CHAPTER 1
The Foundations: Logic and Proofs

SECTION 1.1 Propositional Logic

2. Propositions must have clearly defined truth values, so a proposition must be a declarative sentence with no free variables.

a) This is not a proposition; it's a command.

b) This is not a proposition; it's a question.

c) This is a proposition that is false, as anyone who has been to Maine knows.

d) This is not a proposition; its truth value depends on the value of x.

e) This is a proposition that is false.

f) This is not a proposition; its truth value depends on the value of n.

4. **a)** Jennifer and Teja are not friends.

b) There are not 13 items in a baker's dozen. (Alternatively: The number of items in a baker's dozen is not equal to 13.)

c) Abby sent fewer than 101 text messages yesterday. Alternatively, Abby sent at most 100 text messages yesterday. Note: The first printing of this edition incorrectly rendered this exercise with "every day" in place of "yesterday." That makes it a much harder problem, because the days are quantified, and quantified propositions are not dealt with until a later section. It would be incorrect to say that the negation in that case is "Abby sent at most 100 text messages every day." Rather, a correct negation would be "There exists a day on which Abby sent at most 100 text messages." Saying "Abby did not send more than 100 text messages every day" is somewhat ambiguous—do we mean $\neg\forall$ or do we mean $\forall\neg$?

d) 121 is not a perfect square.

6. **a)** True, because $288 > 256$ and $288 > 128$.

b) True, because C has 5 MP resolution compared to B's 4 MP resolution. Note that only one of these conditions needs to be met because of the word *or*.

c) False, because its resolution is not higher (all of the statements would have to be true for the conjunction to be true).

d) False, because the hypothesis of this conditional statement is true and the conclusion is false.

e) False, because the first part of this biconditional statement is false and the second part is true.

8. **a)** I did not buy a lottery ticket this week.

b) Either I bought a lottery ticket this week or [in the inclusive sense] I won the million dollar jackpot on Friday.

c) If I bought a lottery ticket this week, then I won the million dollar jackpot on Friday.

d) I bought a lottery ticket this week and I won the million dollar jackpot on Friday.

e) I bought a lottery ticket this week if and only if I won the million dollar jackpot on Friday.

f) If I did not buy a lottery ticket this week, then I did not win the million dollar jackpot on Friday.

g) I did not buy a lottery ticket this week, and I did not win the million dollar jackpot on Friday.

h) Either I did not buy a lottery ticket this week, or else I did buy one and won the million dollar jackpot on Friday.

10. **a)** The election is not decided.

b) The election is decided, or the votes have been counted.

c) The election is not decided, and the votes have been counted.

d) If the votes have been counted, then the election is decided.

e) If the votes have not been counted, then the election is not decided.

f) If the election is not decided, then the votes have not been counted.

g) The election is decided if and only if the votes have been counted.

h) Either the votes have not been counted, or else the election is not decided and the votes have been counted. Note that we were able to incorporate the parentheses by using the words *either* and *else*.

12. **a)** If you have the flu, then you miss the final exam.

b) You do not miss the final exam if and only if you pass the course.

c) If you miss the final exam, then you do not pass the course.

d) You have the flu, or miss the final exam, or pass the course.

e) It is either the case that if you have the flu then you do not pass the course or the case that if you miss the final exam then you do not pass the course (or both, it is understood).

f) Either you have the flu and miss the final exam, or you do not miss the final exam and do pass the course.

14. **a)** $r \wedge \neg q$ **b)** $p \wedge q \wedge r$ **c)** $r \rightarrow p$ **d)** $p \wedge \neg q \wedge r$ **e)** $(p \wedge q) \rightarrow r$ **f)** $r \leftrightarrow (q \vee p)$

16. **a)** This is $\mathbf{T} \leftrightarrow \mathbf{T}$, which is true.

b) This is $\mathbf{T} \leftrightarrow \mathbf{F}$, which is false.

c) This is $\mathbf{F} \leftrightarrow \mathbf{F}$, which is true.

d) This is $\mathbf{F} \leftrightarrow \mathbf{T}$, which is false.

18. **a)** This is $\mathbf{F} \rightarrow \mathbf{F}$, which is true.

b) This is $\mathbf{F} \rightarrow \mathbf{F}$, which is true.

c) This is $\mathbf{T} \rightarrow \mathbf{F}$, which is false.

d) This is $\mathbf{T} \rightarrow \mathbf{T}$, which is true.

20. **a)** The employer making this request would be happy if the applicant knew both of these languages, so this is clearly an inclusive *or*.

b) The restaurant would probably charge extra if the diner wanted both of these items, so this is an exclusive *or*.

c) If a person happened to have both forms of identification, so much the better, so this is clearly an inclusive *or*.

d) This could be argued either way, but the inclusive interpretation seems more appropriate. This phrase means that faculty members who do not publish papers in research journals are likely to be fired from their jobs during the probationary period. On the other hand, it may happen that they will be fired even if they do publish (for example, if their teaching is poor).

22. **a)** The necessary condition is the conclusion: If you get promoted, then you wash the boss's car.

b) If the winds are from the south, then there will be a spring thaw.

c) The sufficient condition is the hypothesis: If you bought the computer less than a year ago, then the warranty is good.

d) If Willy cheats, then he gets caught.

e) The "only if" condition is the conclusion: If you access the website, then you must pay a subscription fee.

f) If you know the right people, then you will be elected.

g) If Carol is on a boat, then she gets seasick.

24. **a)** If I am to remember to send you the address, then you will have to send me an e-mail message. (This has been slightly reworded so that the tenses make more sense.)

b) If you were born in the United States, then you are a citizen of this country.

c) If you keep your textbook, then it will be a useful reference in your future courses. (The word "then" is understood in English, even if omitted.)

d) If their goaltender plays well, then the Red Wings will win the Stanley Cup.

e) If you get the job, then you had the best credentials.

f) If there is a storm, then the beach erodes.

g) If you log on to the server, then you have a valid password.

h) If you do not begin your climb too late, then you will reach the summit.

26. **a)** You will get an A in this course if and only if you learn how to solve discrete mathematics problems.

b) You will be informed if and only if you read the newspaper every day. (It sounds better in this order; it would be logically equivalent to state this as "You read the newspaper every day if and only if you will be informed.")

c) It rains if and only if it is a weekend day.

d) You can see the wizard if and only if he is not in.

28. **a)** Converse: If I stay home, then it will snow tonight. Contrapositive: If I do not stay at home, then it will not snow tonight. Inverse: If it does not snow tonight, then I will not stay home.

b) Converse: Whenever I go to the beach, it is a sunny summer day. Contrapositive: Whenever I do not go to the beach, it is not a sunny summer day. Inverse: Whenever it is not a sunny day, I do not go to the beach.

c) Converse: If I sleep until noon, then I stayed up late. Contrapositive: If I do not sleep until noon, then I did not stay up late. Inverse: If I don't stay up late, then I don't sleep until noon.

30. A truth table will need 2^n rows if there are n variables.

a) $2^2 = 4$ **b)** $2^3 = 8$ **c)** $2^6 = 64$ **d)** $2^5 = 32$

32. To construct the truth table for a compound proposition, we work from the inside out. In each case, we will show the intermediate steps. In part **(d)**, for example, we first construct the truth tables for $p \wedge q$ and for $p \vee q$ and combine them to get the truth table for $(p \wedge q) \to (p \vee q)$. For parts **(a)** and **(b)** we have the following table (column three for part **(a)**, column four for part **(b)**).

p	$\neg p$	$p \to \neg p$	$p \leftrightarrow \neg p$
T	F	F	F
F	T	T	F

For parts **(c)** and **(d)** we have the following table.

p	q	$p \vee q$	$p \wedge q$	$p \oplus (p \vee q)$	$(p \wedge q) \to (p \vee q)$
T	T	T	T	F	T
T	F	T	F	F	T
F	T	T	F	T	T
F	F	F	F	F	T

For part **(e)** we have the following table.

p	q	$\neg p$	$q \to \neg p$	$p \leftrightarrow q$	$(q \to \neg p) \leftrightarrow (p \leftrightarrow q)$
T	T	F	F	T	F
T	F	F	T	F	F
F	T	T	T	F	F
F	F	T	T	T	T

For part **(f)** we have the following table.

p	q	$\neg q$	$p \leftrightarrow q$	$p \leftrightarrow \neg q$	$(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$
T	T	F	T	F	T
T	F	T	F	T	T
F	T	F	F	T	T
F	F	T	T	F	T

34. For parts **(a)** and **(b)** we have the following table (column two for part **(a)**, column four for part **(b)**).

p	$p \oplus p$	$\neg p$	$p \oplus \neg p$
T	F	F	T
F	F	T	T

For parts **(c)** and **(d)** we have the following table (columns five and six).

p	q	$\neg p$	$\neg q$	$p \oplus \neg q$	$\neg p \oplus \neg q$
T	T	F	F	T	F
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

For parts **(e)** and **(f)** we have the following table (columns five and six). This time we have omitted the column explicitly showing the negation of q. Note that the first is a tautology and the second is a contradiction (see definitions in Section 1.3).

p	q	$p \oplus q$	$p \oplus \neg q$	$(p \oplus q) \vee (p \oplus \neg q)$	$(p \oplus q) \wedge (p \oplus \neg q)$
T	T	F	T	T	F
T	F	T	F	T	F
F	T	T	F	T	F
F	F	F	T	T	F

36. For parts **(a)** and **(b)**, we have

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$(p \vee q) \wedge r$
T	T	T	T	T	T
T	T	F	T	T	F
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	T	T	T
F	T	F	T	T	F
F	F	T	F	T	F
F	F	F	F	F	F

For parts **(c)** and **(d)**, we have

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$	$(p \wedge q) \wedge r$
T	T	T	T	T	T
T	T	F	T	T	F
T	F	T	F	T	F
T	F	F	F	F	F
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	F	T	F
F	F	F	F	F	F

Finally, for parts **(e)** and **(f)** we have

p	q	r	$\neg r$	$p \vee q$	$(p \vee q) \wedge \neg r$	$p \wedge q$	$(p \wedge q) \vee \neg r$
T	T	T	F	T	F	T	T
T	T	F	T	T	T	T	T
T	F	T	F	T	F	F	F
T	F	F	T	T	T	F	T
F	T	T	F	T	F	F	F
F	T	F	T	T	T	F	T
F	F	T	F	F	F	F	F
F	F	F	T	F	F	F	T

38. This time the truth table needs $2^4 = 16$ rows.

p	q	r	s	$p \to q$	$(p \to q) \to r$	$((p \to q) \to r) \to s$
T	T	T	T	T	T	T
T	T	T	F	T	T	F
T	T	F	T	T	F	T
T	T	F	F	T	F	T
T	F	T	T	F	T	T
T	F	T	F	F	T	F
T	F	F	T	F	T	T
T	F	F	F	F	T	F
F	T	T	T	T	T	T
F	T	T	F	T	T	F
F	T	F	T	T	F	T
F	T	F	F	T	F	T
F	F	T	T	T	T	T
F	F	T	F	T	T	F
F	F	F	T	T	F	T
F	F	F	F	T	F	T

40. This statement is true if and only if all three clauses, $p \vee \neg q$, $q \vee \neg r$, and $r \vee \neg p$ are true. Suppose p, q, and r are all true. Because each clause has an unnegated variable, each clause is true. Similarly, if p, q, and r are all false, then because each clause has a negated variable, each clause is true. On the other hand, if one of the variables is true and the other two false, then the clause containing the negation of that variable will be false, making the entire conjunction false; and similarly, if one of the variables is false and the other two true, then the clause containing that variable unnegated will be false, again making the entire conjunction false.

42. **a)** Since the condition is true, the statement is executed, so x is incremented and now has the value 2.

b) Since the condition is false, the statement is not executed, so x is not incremented and now still has the value 1.

c) Since the condition is true, the statement is executed, so x is incremented and now has the value 2.

d) Since the condition is false, the statement is not executed, so x is not incremented and now still has the value 1.

e) Since the condition is true when it is encountered (since $x = 1$), the statement is executed, so x is incremented and now has the value 2. (It is irrelevant that the condition is now false.)

44. a) $1\ 1000 \wedge (0\ 1011 \vee 1\ 1011) = 1\ 1000 \wedge 1\ 1011 = 1\ 1000$
b) $(0\ 1111 \wedge 1\ 0101) \vee 0\ 1000 = 0\ 0101 \vee 0\ 1000 = 0\ 1101$
c) $(0\ 1010 \oplus 1\ 1011) \oplus 0\ 1000 = 1\ 0001 \oplus 0\ 1000 = 1\ 1001$
d) $(1\ 1011 \vee 0\ 1010) \wedge (1\ 0001 \vee 1\ 1011) = 1\ 1011 \wedge 1\ 1011 = 1\ 1011$

46. The truth value of "Fred and John are happy" is $\min(0.8, 0.4) = 0.4$. The truth value of "Neither Fred nor John is happy" is $\min(0.2, 0.6) = 0.2$, since this statement means "Fred is not happy, and John is not happy," and we computed the truth values of the two propositions in this conjunction in Exercise 45.

48. This cannot be a proposition, because it cannot have a truth value. Indeed, if it were true, then it would be truly asserting that it is false, a contradiction; on the other hand if it were false, then its assertion that it is false must be false, so that it would be true—again a contradiction. Thus this string of letters, while appearing to be a proposition, is in fact meaningless.

50. No. This is a classical paradox. (We will use the male pronoun in what follows, assuming that we are talking about males shaving their beards here, and assuming that all men have facial hair. If we restrict ourselves to beards and allow female barbers, then the barber could be female with no contradiction.) If such a barber existed, who would shave the barber? If the barber shaved himself, then he would be violating the rule that he shaves only those people who do not shave themselves. On the other hand, if he does not shave himself, then the rule says that he must shave himself. Neither is possible, so there can be no such barber.

SECTION 1.2 Applications of Propositional Logic

2. Recall that p only if q means $p \to q$. In this case, if you can see the movie then you must have fulfilled one of the two requirements. Therefore the statement is $m \to (e \vee p)$. Notice that in everyday life one might actually say "You can see the movie *if* you meet one of these conditions," but logically that is not what the rules really say.

4. The condition stated here is that if you use the network, then either you pay the fee or you are a subscriber. Therefore the proposition in symbols is $w \to (d \vee s)$.

6. This is similar to Exercise 2: $u \to (b_{32} \wedge g_1 \wedge r_1 \wedge h_{16}) \vee (b_{64} \wedge g_2 \wedge r_2 \wedge h_{32})$.

8. a) "But" means "and": $r \wedge \neg p$.
b) "Whenever" means "if": $(r \wedge p) \to q$.
c) Access being denied is the negation of q, so we have $\neg r \to \neg q$.
d) The hypothesis is a conjunction: $(\neg p \wedge r) \to q$.

10. We write these symbolically: $u \to \neg a$, $a \to s$, $\neg s \to \neg u$. Note that we can make all the conclusion true by making a false, s true, and u false. Therefore if the users cannot access the file system, they can save new files, and the system is not being upgraded, then all the conditional statements are true. Thus the system is consistent.

12. This system is consistent. We use L, Q, N, and B to stand for the basic propositions here, "The file system is locked," "New messages will be queued," "The system is functioning normally," and "New messages will be sent to the message buffer," respectively. Then the given specifications are $\neg L \to Q$, $\neg L \leftrightarrow N$, $\neg Q \to B$, $\neg L \to B$, and $\neg B$. If we want consistency, then we had better have B false in order that $\neg B$ be true. This requires that both L and Q be true, by the two conditional statements that have B as their consequence. The first conditional statement therefore is of the form $\mathrm{F} \to \mathrm{T}$, which is true. Finally, the biconditional $\neg L \leftrightarrow N$ can be satisfied by taking N to be false. Thus this set of specifications is consistent. Note that there is just this one satisfying truth assignment.

14. This is similar to Example 6, about universities in New Mexico. To search for hiking in West Virginia, we could enter WEST **AND** VIRGINIA **AND** HIKING. If we enter (VIRGINIA **AND** HIKING) **NOT** WEST, then we'll get websites about hiking in Virginia but not in West Virginia, except for sites that happen to use the word "west" in a different context (e.g., "Follow the stream west until you come to a clearing").

16. a) If the explorer (a woman, so that our pronouns will not get confused here—the cannibals will be male) encounters a truth-teller, then he will honestly answer "no" to her question. If she encounters a liar, then the honest answer to her question is "yes," so he will lie and answer "no." Thus everybody will answer "no" to the question, and the explorer will have no way to determine which type of cannibal she is speaking to.

b) There are several possible correct answers. One is the following question: "If I were to ask you if you always told the truth, would you say that you did?" Then if the cannibal is a truth teller, he will answer yes (truthfully), while if he is a liar, then, since in fact he would have said that he did tell the truth if questioned, he will now lie and answer no.

18. We will translate these conditions into statements in symbolic logic, using j, s, and k for the propositions that Jasmine, Samir, and Kanti attend, respectively. The first statement is $j \to \neg s$. The second statement is $s \to k$. The last statement is $\neg k \vee j$, because"unless" means "or." (We could also translate this as $k \to j$. From the comments following Definition 5 in the text, we know that $p \to q$ is equivalent to "q unless $\neg p$. In this case p is $\neg j$ and q is $\neg k$.) First, suppose that s is true. Then the second statement tells us that k is also true, and then the last statement forces j to be true. But now the first statement forces s to be false. So we conclude that s must be false; Samir cannot attend. On the other hand, if s is false, then the first two statements are automatically true, not matter what the truth values of k and j are. If we look at the last statement, we see that it will be true as long as it is not the case that k is true and j is false. So the only combinations of friends that make everybody happy are Jasmine and Kanti, or Jasmine alone (or no one!).

20. If A is a knight, then his statement that both of them are knights is true, and both will be telling the truth. But that is impossible, because B is asserting otherwise (that A is a knave). If A is a knave, then B's assertion is true, so he must be a knight, and A's assertion is false, as it should be. Thus we conclude that A is a knave and B is a knight.

22. We can draw no conclusions. A knight will declare himself to be a knight, telling the truth. A knave will lie and assert that he is a knight. Since everyone will say "I am a knight," we can determine nothing.

24. Suppose that A is the knight. Then because he told the truth, C is the knave and therefore B is the spy. In this case both B and C are lying, which is consistent with their identities. To see that this is the only solution, first note that B cannot be the knight, because of his claim that A is the knight (which would then have to be a lie). Similarly, C cannot be the knight, because he would be lying when stating that he is the spy.

26. There is no solution, because neither a knight nor a knave would ever claim to be the knave.

28. Suppose that A is the knight. Then B's statement is true, so he must be the spy, which means that C's statement is also true, but that is impossible because C would have to be the knave. Therefore A is not the knight. Next suppose that B is the knight. His true statement forces A to be the spy, which in turn forces C to be the knave; once more that is impossible because C said something true. The only other possibility is that C is the knight, which then forces B to be the spy and A the knave. This works out fine, because A is lying and B is telling the truth.

30. Neither A nor B can be the knave, because the knave cannot make the truthful statement that he is not the spy. Therefore C is the knave, and consequently A is not the spy. It follows that A is the knight and B is the spy. This works out fine, because A and B are then both telling the truth and C is lying.

32. **a)** We look at the three possibilities of who the innocent men might be. If Smith and Jones are innocent (and therefore telling the truth), then we get an immediate contradiction, since Smith said that Jones was a friend of Cooper, but Jones said that he did not even know Cooper. If Jones and Williams are the innocent truth-tellers, then we again get a contradiction, since Jones says that he did not know Cooper and was out of town, but Williams says he saw Jones with Cooper (presumably in town, and presumably if we was with him, then he knew him). Therefore it must be the case that Smith and Williams are telling the truth. Their statements do not contradict each other. Based on Williams' statement, we know that Jones is lying, since he said that he did not know Cooper when in fact he was with him. Therefore Jones is the murderer.

b) This is just like part **(a)**, except that we are not told ahead of time that one of the men is guilty. Can none of them be guilty? If so, then they are all telling the truth, but this is impossible, because as we just saw, some of the statements are contradictory. Can more than one of them be guilty? If, for example, they are all guilty, then their statements give us no information. So that is certainly possible.

34. This information is enough to determine the entire system. Let each letter stand for the statement that the person whose name begins with that letter is chatting. Then the given information can be expressed symbolically as follows: $\neg K \to H$, $R \to \neg V$, $\neg R \to V$, $A \to R$, $V \to K$, $K \to V$, $H \to A$, $H \to K$. Note that we were able to convert all of these statements into conditional statements. In what follows we will sometimes make use of the contrapositives of these conditional statements as well. First suppose that H is true. Then it follows that A and K are true, whence it follows that R and V are true. But R implies that V is false, so we get a contradiction. Therefore H must be false. From this it follows that K is true; whence V is true, and therefore R is false, as is A. We can now check that this assignment leads to a true value for each conditional statement. So we conclude that Kevin and Vijay are chatting but Heather, Randy, and Abby are not.

36. Note that Diana's statement is merely that she didn't do it.

a) John did it. There are four cases to consider. If Alice is the sole truth-teller, then Carlos did it; but this means that John is telling the truth, a contradiction. If John is the sole truth-teller, then Diana must be lying, so she did it, but then Carlos is telling the truth, a contradiction. If Carlos is the sole truth-teller, then Diana did it, but that makes John truthful, again a contradiction. So the only possibility is that Diana is the sole truth-teller. This means that John is lying when he denied it, so he did it. Note that in this case both Alice and Carlos are indeed lying.

b) Again there are four cases to consider. Since Carlos and Diana are making contradictory statements, the liar must be one of them (we could have used this approach in part **(a)** as well). Therefore Alice is telling the truth, so Carlos did it. Note that John and Diana are telling the truth as well here, and it is Carlos who is lying.

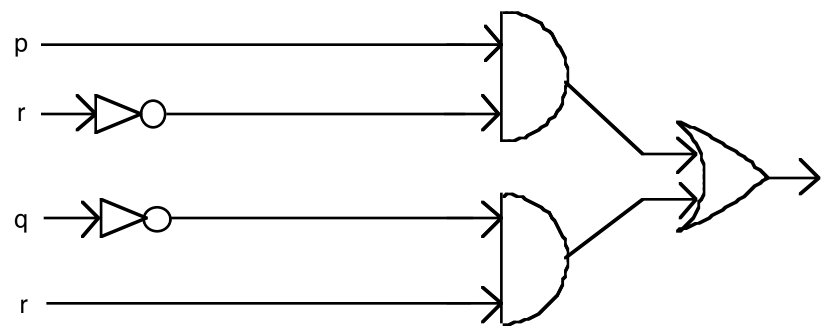
38. This is often given as an exercise in constraint programming, and it is difficult to solve by hand. The following table shows a solution consistent with all the clues, with the houses listed from left to right. Reportedly the solution is unique.

NATIONALITY	Norwegian	Italian	Englishman	Spaniard	Japanese
COLOR	Yellow	Blue	Red	White	Green
PET	Fox	Horse	Snail	Dog	Zebra
JOB	Diplomat	Physician	Photographer	Violinist	Painter
DRINK	Water	Tea	Milk	Juice	Coffee

In this solution the Japanese man owns the zebra, and the Norwegian drinks water. The logical reasoning needed to solve the problem is rather extensive, and the reader is referred to the following website containing the solution to a similar problem: `mathforum.org/library/drmath/view/55627.html`.

40. **a)** Each of p and q is negated and fed to the OR gate. Therefore the output is $(\neg p) \vee (\neg q)$.
b) $\neg(p \vee ((\neg p) \wedge q)))$

42. We have the inputs come in from the left, in some cases passing through an inverter to form their negations. Certain pairs of them enter AND gates, and the outputs of these enter the final OR gate.



SECTION 1.3 Propositional Equivalences

2. There are two cases. If p is true, then $\neg(\neg p)$ is the negation of a false proposition, hence true. Similarly, if p is false, then $\neg(\neg p)$ is also false. Therefore the two propositions are logically equivalent.

4. **a)** We construct the relevant truth table and note that the fifth and seventh columns are identical.

p	q	r	$p \vee q$	$(p \vee q) \vee r$	$q \vee r$	$p \vee (q \vee r)$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

b) Again we construct the relevant truth table and note that the fifth and seventh columns are identical.

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

6. We see that the fourth and seventh columns are identical.

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

8. We need to negate each part and swap "and" with "or."

a) Kwame will not take a job in industry and will not go to graduate school.

b) Yoshiko does not know Java or does not know calculus.

c) James is not young, or he is not strong.

d) Rita will not move to Oregon and will not move to Washington.

10. We construct a truth table for each conditional statement and note that the relevant column contains only T's. For part **(a)** we have the following table.

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$[\neg p \wedge (p \vee q)] \to q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

For part **(b)** we have the following table. We omit the columns showing $p \to q$ and $q \to r$ so that the table will fit on the page.

p	q	r	$(p \to q) \to (q \to r)$	$q \to r$	$[(p \to q) \to (q \to r)] \to (p \to r)$
T	T	T	T	T	T
T	T	F	F	T	T
T	F	T	T	T	F
T	F	F	F	F	T
F	T	T	T	T	T
F	T	F	F	T	F
F	F	T	T	T	F
F	F	F	T	T	T

For part **(c)** we have the following table.

p	q	$p \to q$	$p \wedge (p \to q)$	$[p \wedge (p \to q)] \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

For part **(d)** we have the following table. We have omitted some of the intermediate steps to make the table fit.

p	q	r	$(p \lor q) \land (p \to r) \land (p \to r)$	$[(p \lor q) \land (p \to r) \land (p \to r)] \to r$
T	T	T	T	T
T	T	F	F	T
T	F	T	T	T
T	F	F	F	T
F	T	T	T	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

12. We argue directly by showing that if the hypothesis is true, then so is the conclusion. An alternative approach, which we show only for part **(a)**, is to use the equivalences listed in the section and work symbolically.

a) Assume the hypothesis is true. Then p is false. Since $p \lor q$ is true, we conclude that q must be true. Here is a more "algebraic" solution: $[\neg p \land (p \lor q)] \to q \equiv \neg[\neg p \land (p \lor q)] \lor q \equiv \neg\neg p \lor \neg(p \lor q)] \lor q \equiv p \lor \neg(p \lor q) \lor q \equiv (p \lor q) \lor \neg(p \lor q) \equiv \mathbf{T}$. The reasons for these logical equivalences are, respectively, Table 7, line 1; De Morgan's law; double negation; commutative and associative laws; negation law.

b) We want to show that if the entire hypothesis is true, then the conclusion $p \to r$ is true. To do this, we need only show that if p is true, then r is true. Suppose p is true. Then by the first part of the hypothesis, we conclude that q is true. It now follows from the second part of the hypothesis that r is true, as desired.

c) Assume the hypothesis is true. Then p is true, and since the second part of the hypothesis is true, we conclude that q is also true, as desired.

d) Assume the hypothesis is true. Since the first part of the hypothesis is true, we know that either p or q is true. If p is true, then the second part of the hypothesis tells us that r is true; similarly, if q is true, then the third part of the hypothesis tells us that r is true. Thus in either case we conclude that r is true.

14. This is not a tautology. It is saying that knowing that the hypothesis of an conditional statement is false allows us to conclude that the conclusion is also false, and we know that this is not valid reasoning. To show that it is not a tautology, we need to find truth assignments for p and q that make the entire proposition false. Since this is possible only if the conclusion if false, we want to let q be true; and since we want the hypothesis to be true, we must also let p be false. It is easy to check that if, indeed, p is false and q is true, then the conditional statement is false. Therefore it is not a tautology.

16. The first of these propositions is true if and only if p and q have the same truth value. The second is true if and only if either p and q are both true, or p and q are both false. Clearly these two conditions are saying the same thing.

18. It is easy to see from the definitions of conditional statement and negation that each of these propositions is false in the case in which p is true and q is false, and true in the other three cases. Therefore the two propositions are logically equivalent.

20. It is easy to see from the definitions of the logical operations involved here that each of these propositions is true in the cases in which p and q have the same truth value, and false in the cases in which p and q have opposite truth values. Therefore the two propositions are logically equivalent.

22. Suppose that $(p \to q) \land (p \to r)$ is true. We want to show that $p \to (q \land r)$ is true, which means that we want to show that $q \land r$ is true whenever p is true. If p is true, since we know that both $p \to q$ and $p \to r$ are true from our assumption, we can conclude that q is true and that r is true. Therefore $q \land r$ is true, as desired. Conversely, suppose that $p \to (q \land r)$ is true. We need to show that $p \to q$ is true and that $p \to r$ is true, which means that if p is true, then so are q and r. But this follows from $p \to (q \land r)$.

24. We determine exactly which rows of the truth table will have T as their entries. Now $(p \to q) \vee (p \to r)$ will be true when either of the conditional statements is true. The conditional statement will be true if p is false, or if q in one case or r in the other case is true, i.e., when $q \vee r$ is true, which is precisely when $p \to (q \vee r)$ is true. Since the two propositions are true in exactly the same situations, they are logically equivalent.

26. Applying the third and first equivalences in Table 7, we have $\neg p \to (q \to r) \equiv p \vee (q \to r) \equiv p \vee \neg q \vee r$. Applying the first equivalence in Table 7 to $q \to (p \vee r)$ shows that $\neg q \vee p \vee r$ is equivalent to it. But these are equivalent by the commutative and associative laws.

28. We know that $p \leftrightarrow q$ is true precisely when p and q have the same truth value. But this happens precisely when $\neg p$ and $\neg q$ have the same truth value, that is, $\neg p \leftrightarrow \neg q$.

30. The conclusion $q \vee r$ will be true in every case except when q and r are both false. But if q and r are both false, then one of $p \vee q$ or $\neg p \vee r$ is false, because one of p or $\neg p$ is false. Thus in this case the hypothesis $(p \vee q) \wedge (\neg p \vee r)$ is false. An conditional statement in which the conclusion is true or the hypothesis is false is true, and that completes the argument.

32. We just need to find an assignment of truth values that makes one of these propositions true and the other false. We can let p be true and the other two variables be false. Then the first statement will be $\mathbf{F} \to \mathbf{F}$, which is true, but the second will be $\mathbf{F} \wedge \mathbf{T}$, which is false.

34. We apply the rules stated in the preamble.
a) $p \wedge \neg q$ **b)** $p \vee (q \wedge (r \vee \mathbf{F}))$ **c)** $(p \vee \neg q) \wedge (q \vee \mathbf{T})$

36. If s has any occurrences of $\wedge$, $\vee$, $\mathbf{T}$, or $\mathbf{F}$, then the process of forming the dual will change it. Therefore $s^* = s$ if and only if s is simply one propositional variable (like p). A more difficult question is to determine when s^* will be logically equivalent to s. For example, $p \vee \mathbf{F}$ is logically equivalent to its dual $p \wedge \mathbf{T}$, because both are logically equivalent to p.

38. The table is in fact displayed so as to exhibit the duality. The two identity laws are duals of each other, the two domination laws are duals of each other, etc. The only law not listed with another, the double negation law, is its own dual, since there are no occurrences of $\wedge$, $\vee$, $\mathbf{T}$, or $\mathbf{F}$ to replace.

40. Following the hint, we easily see that the answer is $p \wedge q \wedge \neg r$.

42. The statement of the problem is really the solution. Each line of the truth table corresponds to exactly one combination of truth values for the n atomic propositions involved. We can write down a conjunction that is true precisely in this case, namely the conjunction of all the atomic propositions that are true and the negations of all the atomic propositions that are false. If we do this for *each* line of the truth table for which the value of the compound proposition is to be true, and take the disjunction of the resulting propositions, then we have the desired proposition in its disjunctive normal form.

44. Given a compound proposition p, we can, by Exercise 43, write down a proposition q that is logically equivalent to p and uses only $\neg$, $\wedge$, and $\vee$. Now by De Morgan's law we can get rid of all the $\vee$'s by replacing each occurrence of $p_1 \vee p_2 \vee \cdots \vee p_n$ with $\neg(\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n)$.

46. We write down the truth table corresponding to the definition.

p	q	$p \mid q$
T	T	F
T	F	T
F	T	T
F	F	T

48. We write down the truth table corresponding to the definition.

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

50. **a)** From the definition (or as seen in the truth table constructed in Exercise 48), $p \downarrow p$ is false when p is true and true when p is false, exactly as $\neg p$ is; thus the two are logically equivalent.

b) The proposition $(p \downarrow q) \downarrow (p \downarrow q)$ is equivalent, by part **(a)**, to $\neg(p \downarrow q)$, which from the definition (or truth table or Exercise 49) is clearly equivalent to $p \vee q$.

c) By Exercise 45, every compound proposition is logically equivalent to one that uses only $\neg$ and $\vee$. But by parts **(a)** and **(b)** of the present exercise, we can get rid of all the negations and disjunctions by using *NOR*'s. Thus every compound proposition can be converted into a logically equivalent compound proposition involving only *NOR*'s.

52. This exercise is similar to Exercise 50. First we can see from the truth tables that $(p \mid p) \equiv (\neg p)$ and that $((p \mid p) \mid (q \mid q)) \equiv (p \vee q)$. Then we argue exactly as in part **(c)** of Exercise 50: by Exercise 45, every compound proposition is logically equivalent to one that uses only $\neg$ and $\vee$. But by our observations at the beginning of the present exercise, we can get rid of all the negations and disjunctions by using *NAND*'s. Thus every compound proposition can be converted into a logically equivalent compound proposition involving only *NAND*'s.

54. To show that these are *not* logically equivalent, we need only find one assignment of truth values to p, q, and r for which the truth values of $p \mid (q \mid r)$ and $(p \mid q) \mid r$ differ. One such assignment is T for p and F for q and r. Then computing from the truth tables (or definitions), we see that $p \mid (q \mid r)$ is false and $(p \mid q) \mid r$ is true.

56. To say that p and q are logically equivalent is to say that the truth tables for p and q are identical; similarly, to say that q and r are logically equivalent is to say that the truth tables for q and r are identical. Clearly if the truth tables for p and q are identical, and the truth tables for q and r are identical, then the truth tables for p and r are identical (this is a fundamental axiom of the notion of equality). Therefore p and r are logically equivalent. (We are assuming—and there is no loss of generality in doing so—that the same atomic variables appear in all three propositions.)

58. If we want the first two of these to be true, then p and q must have the same truth value. If q is true, then the third and fourth expressions will be true, and if r is false, the last expression will be true. So all five of these disjunctions will be true if we set p and q to be true, and r to be false.

60. These follow directly from the definitions. An unsatisfiable compound proposition is one that is true for no assignment of truth values to its variables, which is the same as saying that it is false for every assignment of truth values, which is the same same saying that its negation is true for every assignment of truth values. That is the definition of a tautology. Conversely, the negation of a tautology (i.e., a proposition that is true for every assignment of truth values to its variables) will be false for every assignment of truth values, and therefore will be unsatisfiable.

62. In each case we hunt for truth assignments that make all the disjunctions true.

a) Since p occurs in four of the five disjunctions, we can make p true, and then make q false (and make r and s anything we please). Thus this proposition is satisfiable.

b) This is satisfiable by, for example, setting p to be false (that takes care of the first, second, and fourth disjunctions), s to be false (for the third and sixth disjunctions), q to be true (for the fifth disjunction), and r to be anything.

c) It is not hard to find a satisfying truth assignment, such as p, q, and s true, and r false.

64. Recall that $p(i,j,n)$ asserts that the cell in row i, column j contains the number n. Thus $\bigvee_{n=1}^{9} p(i,j,n)$ asserts that this cell contains at least one number. To assert that every cell contains at least one number, we take the conjunction of these statements over all cells: $\bigwedge_{i=1}^{9} \bigwedge_{j=1}^{9} \bigvee_{n=1}^{9} p(i,j,n)$.

66. There are nine blocks, in three rows and three columns. Let r and s index the row and column of the block, respectively, where we start counting at 0, so that $0 \le r \le 2$ and $0 \le s \le 2$. (For example, $r = 0, s = 1$ corresponds to the block in the first row of blocks and second column of blocks.) The key point is to notice that the block corresponding to the pair (r,s) contains the cells that are in rows $3r+1$, $3r+2$, and $3r+3$ and columns $3s+1$, $3s+2$, and $3s+3$. Therefore $p(3r+i, 3s+j, n)$ asserts that a particular cell in this block contains the number n, where $1 \le i \le 3$ and $1 \le j \le 3$. If we take the disjunction over all these values of i and j, then we obtain $\bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r+i, 3s+j, n)$, asserting that some cell in this block contains the number n. Because we want this to be true for every number and for every block, we form the triply-indexed conjunction given in the text.

SECTION 1.4 Predicates and Quantifiers

2. a) This is true, since there is an a in *orange*. **b)** This is false, since there is no a in *lemon*.
c) This is false, since there is no a in *true*. **d)** This is true, since there is an a in *false*.

4. a) Here x is still equal to 0, since the condition is false.
b) Here x is still equal to 1, since the condition is false.
c) This time x is equal to 1 at the end, since the condition is true, so the statement $x := 1$ is executed.

6. The answers given here are not unique, but care must be taken not to confuse nonequivalent sentences. Parts **(c)** and **(f)** are equivalent; and parts **(d)** and **(e)** are equivalent. But these two pairs are not equivalent to each other.

a) Some student in the school has visited North Dakota. (Alternatively, there exists a student in the school who has visited North Dakota.)

b) Every student in the school has visited North Dakota. (Alternatively, all students in the school have visited North Dakota.)

c) This is the negation of part **(a)**: No student in the school has visited North Dakota. (Alternatively, there does not exist a student in the school who has visited North Dakota.)

d) Some student in the school has not visited North Dakota. (Alternatively, there exists a student in the school who has not visited North Dakota.)

e) This is the negation of part **(b)**: It is not true that every student in the school has visited North Dakota. (Alternatively, not all students in the school have visited North Dakota.)

f) All students in the school have not visited North Dakota. (This is technically the correct answer, although common English usage takes this sentence to mean—incorrectly—the answer to part **(e)**. To be perfectly clear, one could say that every student in this school has failed to visit North Dakota, or simply that no student has visited North Dakota.)

8. Note that part **(b)** and part **(c)** are not the sorts of things one would normally say.

a) If an animal is a rabbit, then that animal hops. (Alternatively, every rabbit hops.)

b) Every animal is a rabbit and hops.

c) There exists an animal such that if it is a rabbit, then it hops. (Note that this is trivially true, satisfied, for example, by lions, so it is not the sort of thing one would say.)

d) There exists an animal that is a rabbit and hops. (Alternatively, some rabbits hop. Alternatively, some hopping animals are rabbits.)

10. a) We assume that this means that one student has all three animals: $\exists x(C(x) \wedge D(x) \wedge F(x))$.

b) $\forall x(C(x) \vee D(x) \vee F(x))$ **c)** $\exists x(C(x) \wedge F(x) \wedge \neg D(x))$

d) This is the negation of part **(a)**: $\neg\exists x(C(x) \wedge D(x) \wedge F(x))$.

e) Here the owners of these pets can be different: $(\exists x\, C(x)) \wedge (\exists x\, D(x)) \wedge (\exists x\, F(x))$. There is no harm in using the same dummy variable, but this could also be written, for example, as $(\exists x\, C(x)) \wedge (\exists y\, D(y)) \wedge (\exists z\, F(z))$.

12. a) Since $0 + 1 > 2 \cdot 0$, we know that $Q(0)$ is true.

b) Since $(-1) + 1 > 2 \cdot (-1)$, we know that $Q(-1)$ is true.

c) Since $1 + 1 \not> 2 \cdot 1$, we know that $Q(1)$ is false.

d) From part **(a)** we know that there is at least one x that makes $Q(x)$ true, so $\exists x\, Q(x)$ is true.

e) From part **(c)** we know that there is at least one x that makes $Q(x)$ false, so $\forall x\, Q(x)$ is false.

f) From part **(c)** we know that there is at least one x that makes $Q(x)$ false, so $\exists x\, \neg Q(x)$ is true.

g) From part **(a)** we know that there is at least one x that makes $Q(x)$ true, so $\forall x\, \neg Q(x)$ is false.

14. a) Since $(-1)^3 = -1$, this is true.

b) Since $(\frac{1}{2})^4 < (\frac{1}{2})^2$, this is true.

c) Since $(-x)^2 = ((-1)x)^2 = (-1)^2 x^2 = x^2$, we know that $\forall x((-x)^2 = x^2)$ is true.

d) Twice a positive number is larger than the number, but this inequality is not true for negative numbers or 0. Therefore $\forall x(2x > x)$ is false.

16. a) true ($x = \sqrt{2}$) **b)** false ($\sqrt{-1}$ is not a real number)

c) true (the left-hand side is always at least 2) **d)** false (not true for $x = 1$ or $x = 0$)

18. Existential quantifiers are like disjunctions, and universal quantifiers are like conjunctions. See Examples 11 and 16.

a) We want to assert that $P(x)$ is true for some x in the domain, so either $P(-2)$ is true or $P(-1)$ is true or $P(0)$ is true or $P(1)$ is true or $P(2)$ is true. Thus the answer is $P(-2) \vee P(-1) \vee P(0) \vee P(1) \vee P(2)$. The other parts of this exercise are similar. Note that by De Morgan's laws, the expression in part **(c)** is logically equivalent to the expression in part **(f)**, and the expression in part **(d)** is logically equivalent to the expression in part **(e)**.

b) $P(-2) \wedge P(-1) \wedge P(0) \wedge P(1) \wedge P(2)$

c) $\neg P(-2) \vee \neg P(-1) \vee \neg P(0) \vee \neg P(1) \vee \neg P(2)$

d) $\neg P(-2) \wedge \neg P(-1) \wedge \neg P(0) \wedge \neg P(1) \wedge \neg P(2)$

e) This is just the negation of part **(a)**: $\neg(P(-2) \vee P(-1) \vee P(0) \vee P(1) \vee P(2))$

f) This is just the negation of part **(b)**: $\neg(P(-2) \wedge P(-1) \wedge P(0) \wedge P(1) \wedge P(2))$

20. Existential quantifiers are like disjunctions, and universal quantifiers are like conjunctions. See Examples 11 and 16.

a) We want to assert that $P(x)$ is true for some x in the domain, so either $P(-5)$ is true or $P(-3)$ is true or $P(-1)$ is true or $P(1)$ is true or $P(3)$ is true or $P(5)$ is true. Thus the answer is $P(-5) \vee P(-3) \vee P(-1) \vee P(1) \vee P(3) \vee P(5)$.

b) $P(-5) \wedge P(-3) \wedge P(-1) \wedge P(1) \wedge P(3) \wedge P(5)$

c) The formal translation is as follows: $((-5 \neq 1) \rightarrow P(-5)) \wedge ((-3 \neq 1) \rightarrow P(-3)) \wedge ((-1 \neq 1) \rightarrow P(-1)) \wedge ((1 \neq 1) \rightarrow P(1)) \wedge ((3 \neq 1) \rightarrow P(3)) \wedge ((5 \neq 1) \rightarrow P(5))$. However, since the hypothesis $x \neq 1$ is false when x is 1 and true when x is anything other than 1, we have more simply $P(-5) \wedge P(-3) \wedge P(-1) \wedge P(3) \wedge P(5)$.

d) The formal translation is as follows: $((-5 \geq 0) \wedge P(-5)) \vee ((-3 \geq 0) \wedge P(-3)) \vee ((-1 \geq 0) \wedge P(-1)) \vee ((1 \geq 0) \wedge P(1)) \vee ((3 \geq 0) \wedge P(3)) \vee ((5 \geq 0) \wedge P(5))$. Since only three of the x's in the domain meet the condition, the answer is equivalent to $P(1) \vee P(3) \vee P(5)$.

e) For the second part we again restrict the domain: $(\neg P(-5) \vee \neg P(-3) \vee \neg P(-1) \vee \neg P(1) \vee \neg P(3) \vee \neg P(5)) \wedge (P(-1) \wedge P(-3) \wedge P(-5))$. This is equivalent to $(\neg P(1) \vee \neg P(3) \vee \neg P(5)) \wedge (P(-1) \wedge P(-3) \wedge P(-5))$.

22. Many answer are possible in each case.

a) A domain consisting of a few adults in certain parts of India would make this true. If the domain were all residents of the United States, then this is certainly false.

b) If the domain is all residents of the United States, then this is true. If the domain is the set of pupils in a first grade class, it is false.

c) If the domain consists of all the United States Presidents whose last name is Bush, then the statement is true. If the domain consists of all United States Presidents, then the statement is false.

d) If the domain were all residents of the United States, then this is certainly true. If the domain consists of all babies born in the last five minutes, one would expect the statement to be false (it's not even clear that these babies "know" their mothers yet).

24. In order to do the translation the second way, we let $C(x)$ be the propositional function "x is in your class." Note that for the second way, we always want to use conditional statements with universal quantifiers and conjunctions with existential quantifiers.

a) Let $P(x)$ be "x has a cellular phone." Then we have $\forall x\, P(x)$ the first way, or $\forall x(C(x) \rightarrow P(x))$ the second way.

b) Let $F(x)$ be "x has seen a foreign movie." Then we have $\exists x\, F(x)$ the first way, or $\exists x(C(x) \wedge F(x))$ the second way.

c) Let $S(x)$ be "x can swim." Then we have $\exists x\, \neg S(x)$ the first way, or $\exists x(C(x) \wedge \neg S(x))$ the second way.

d) Let $Q(x)$ be "x can solve quadratic equations." Then we have $\forall x\, Q(x)$ the first way, or $\forall x(C(x) \rightarrow Q(x))$ the second way.

e) Let $R(x)$ be "x wants to be rich." Then we have $\exists x\, \neg R(x)$ the first way, or $\exists x(C(x) \wedge \neg R(x))$ the second way.

26. In all of these, we will let $Y(x)$ be the propositional function that x is in your school or class, as appropriate.

a) If we let $U(x)$ be "x has visited Uzbekistan," then we have $\exists x\, U(x)$ if the domain is just your schoolmates, or $\exists x(Y(x) \wedge U(x))$ if the domain is all people. If we let $V(x, y)$ mean that person x has visited country y, then we can rewrite this last one as $\exists x(Y(x) \wedge V(x, \text{Uzbekistan}))$.

b) If we let $C(x)$ and $P(x)$ be the propositional functions asserting that x has studied calculus and C++, respectively, then we have $\forall x(C(x) \wedge P(x))$ if the domain is just your schoolmates, or $\forall x(Y(x) \rightarrow (C(x) \wedge P(x)))$ if the domain is all people. If we let $S(x, y)$ mean that person x has studied subject y, then we can rewrite this last one as $\forall x(Y(x) \rightarrow (S(x, \text{calculus}) \wedge S(x, \text{C++})))$.

c) If we let $B(x)$ and $M(x)$ be the propositional functions asserting that x owns a bicycle and a motorcycle, respectively, then we have $\forall x(\neg(B(x) \wedge M(x)))$ if the domain is just your schoolmates, or $\forall x(Y(x) \rightarrow \neg(B(x) \wedge$

$M(x)))$ if the domain is all people. Note that "no one" became "for all ... not." If we let $O(x,y)$ mean that person x owns item y, then we can rewrite this last one as $\forall x(Y(x) \to \neg(O(x,\text{bicycle}) \wedge O(x,\text{motorcycle})))$.

d) If we let $H(x)$ be "x is happy," then we have $\exists x\, \neg H(x)$ if the domain is just your schoolmates, or $\exists x(Y(x) \wedge \neg H(x))$ if the domain is all people. If we let $E(x,y)$ mean that person x is in mental state y, then we can rewrite this last one as $\exists x(Y(x) \wedge \neg E(x,\text{happy}))$.

e) If we let $T(x)$ be "x was born in the twentieth century," then we have $\forall x\, T(x)$ if the domain is just your schoolmates, or $\forall x(Y(x) \to T(x))$ if the domain is all people. If we let $B(x,y)$ mean that person x was born in the y^{th} century, then we can rewrite this last one as $\forall x(Y(x) \to B(x,20))$.

28. Let $R(x)$ be "x is in the correct place"; let $E(x)$ be "x is in excellent condition"; let $T(x)$ be "x is a [or your] tool"; and let the domain of discourse be all things.

a) There exists something not in the correct place: $\exists x\, \neg R(x)$.

b) If something is a tool, then it is in the correct place place and in excellent condition: $\forall x\,(T(x) \to (R(x) \wedge E(x)))$.

c) $\forall x\,(R(x) \wedge E(x))$

d) This is saying that everything fails to satisfy the condition: $\forall x\, \neg(R(x) \wedge E(x))$.

e) There exists a tool with this property: $\exists x\,(T(x) \wedge \neg R(x) \wedge E(x))$.

30. **a)** $P(1,3) \vee P(2,3) \vee P(3,3)$ **b)** $P(1,1) \wedge P(1,2) \wedge P(1,3)$
c) $\neg P(2,1) \vee \neg P(2,2) \vee \neg P(2,3)$ **d)** $\neg P(1,2) \wedge \neg P(2,2) \wedge \neg P(3,2)$

32. In each case we need to specify some propositional functions (predicates) and identify the domain of discourse.

a) Let $F(x)$ be "x has fleas," and let the domain of discourse be dogs. Our original statement is $\forall x\, F(x)$. Its negation is $\exists x\, \neg F(x)$. In English this reads "There is a dog that does not have fleas."

b) Let $H(x)$ be "x can add," where the domain of discourse is horses. Then our original statement is $\exists x\, H(x)$. Its negation is $\forall x\, \neg H(x)$. In English this is rendered most simply as "No horse can add."

c) Let $C(x)$ be "x can climb," and let the domain of discourse be koalas. Our original statement is $\forall x\, C(x)$. Its negation is $\exists x\, \neg C(x)$. In English this reads "There is a koala that cannot climb."

d) Let $F(x)$ be "x can speak French," and let the domain of discourse be monkeys. Our original statement is $\neg \exists x\, F(x)$ or $\forall x\, \neg F(x)$. Its negation is $\exists x\, F(x)$. In English this reads "There is a monkey that can speak French."

e) Let $S(x)$ be "x can swim" and let $C(x)$ be "x can catch fish," where the domain of discourse is pigs. Then our original statement is $\exists x\,(S(x) \wedge C(x))$. Its negation is $\forall x\, \neg(S(x) \wedge C(x))$, which could also be written $\forall x\,(\neg S(x) \vee \neg C(x))$ by De Morgan's law. In English this is "No pig can both swim and catch fish," or "Every pig either is unable to swim or is unable to catch fish."

34. **a)** Let $S(x)$ be "x obeys the speed limit," where the domain of discourse is drivers. The original statement is $\exists x\, \neg S(x)$, the negation is $\forall x\, S(x)$, "All drivers obey the speed limit."

b) Let $S(x)$ be "x is serious," where the domain of discourse is Swedish movies. The original statement is $\forall x\, S(x)$, the negation is $\exists x\, \neg S(x)$, "Some Swedish movies are not serious."

c) Let $S(x)$ be "x can keep a secret," where the domain of discourse is people. The original statement is $\neg \exists x\, S(x)$, the negation is $\exists x\, S(x)$, "Some people can keep a secret."

d) Let $A(x)$ be "x has a good attitude," where the domain of discourse is people in this class. The original statement is $\exists x\, \neg A(x)$, the negation is $\forall x\, A(x)$, "Everyone in this class has a good attitude."

36. **a)** Since $1^2 = 1$, this statement is false; $x = 1$ is a counterexample. So is $x = 0$ (these are the only two counterexamples).

b) There are two counterexamples: $x = \sqrt{2}$ and $x = -\sqrt{2}$.

c) There is one counterexample: $x = 0$.

38. a) Some system is open. **b)** Every system is either malfunctioning or in a diagnostic state.
c) Some system is open, or some system is in a diagnostic state. **d)** Some system is unavailable.
e) No system is working. (We could also say "Every system is not working," as long as we understood that this is different from "Not every system is working.")

40. There are many ways to write these, depending on what we use for predicates.
a) Let $F(x)$ be "There is less than x megabytes free on the hard disk," with the domain of discourse being positive numbers, and let $W(x)$ be "User x is sent a warning message." Then we have $F(30) \to \forall x\, W(x)$.
b) Let $O(x)$ be "Directory x can be opened," let $C(x)$ be "File x can be closed," and let E be the proposition "System errors have been detected." Then we have $E \to ((\forall x\, \neg O(x)) \wedge (\forall x\, \neg C(x)))$.
c) Let B be the proposition "The file system can be backed up," and let $L(x)$ be "User x is currently logged on." Then we have $(\exists x\, L(x)) \to \neg B$.
d) Let $D(x)$ be "Product x can be delivered," and let $M(x)$ be "There are at least x megabytes of memory available" and $S(x)$ be "The connection speed is at least x kilobits per second," where the domain of discourse for the last two propositional functions are positive numbers. Then we have $(M(8) \wedge S(56)) \to D(\text{video on demand})$.

42. There are many ways to write these, depending on what we use for predicates.
a) Let $A(x)$ be "User x has access to an electronic mailbox." Then we have $\forall x\, A(x)$.
b) Let $A(x,y)$ be "Group member x can access resource y," and let $S(x,y)$ be "System x is in state y." Then we have $S(\text{file system, locked}) \to \forall x\, A(x, \text{system mailbox})$.
c) Let $S(x,y)$ be "System x is in state y." Recalling that "only if" indicates a necessary condition, we have $S(\text{firewall, diagnostic}) \to S(\text{proxy server, diagnostic})$.
d) Let $T(x)$ be "The throughput is at least x kbps," where the domain of discourse is positive numbers, let $M(x,y)$ be "Resource x is in mode y," and let $S(x,y)$ be "Router x is in state y." Then we have $(T(100) \wedge \neg T(500) \wedge \neg M(\text{proxy server, diagnostic})) \to \exists x\, S(x, \text{normal})$.

44. We want propositional functions P and Q that are sometimes, but not always, true (so that the second biconditional is $\mathbf{F} \leftrightarrow \mathbf{F}$ and hence true), but such that there is an x making one true and the other false. For example, we can take $P(x)$ to mean that x is an even number (a multiple of 2) and $Q(x)$ to mean that x is a multiple of 3. Then an example like $x = 4$ or $x = 9$ shows that $\forall x(P(x) \leftrightarrow Q(x))$ is false.

46. a) There are two cases. If A is true, then $(\forall x P(x)) \vee A$ is true, and since $P(x) \vee A$ is true for all x, $\forall x(P(x) \vee A)$ is also true. Thus both sides of the logical equivalence are true (hence equivalent). Now suppose that A is false. If $P(x)$ is true for all x, then the left-hand side is true. Furthermore, the right-hand side is also true (since $P(x) \vee A$ is true for all x). On the other hand, if $P(x)$ is false for some x, then both sides are false. Therefore again the two sides are logically equivalent.
b) There are two cases. If A is true, then $(\exists x P(x)) \vee A$ is true, and since $P(x) \vee A$ is true for some (really all) x, $\exists x(P(x) \vee A)$ is also true. Thus both sides of the logical equivalence are true (hence equivalent). Now suppose that A is false. If $P(x)$ is true for at least one x, then the left-hand side is true. Furthermore, the right-hand side is also true (since $P(x) \vee A$ is true for that x). On the other hand, if $P(x)$ is false for all x, then both sides are false. Therefore again the two sides are logically equivalent.

48. a) There are two cases. If A is false, then both sides of the equivalence are true, because a conditional statement with a false hypothesis is true. If A is true, then $A \to P(x)$ is equivalent to $P(x)$ for each x, so the left-hand side is equivalent to $\forall x\, P(x)$, which is equivalent to the right-hand side.

b) There are two cases. If A is false, then both sides of the equivalence are true, because a conditional statement with a false hypothesis is true (and we are assuming that the domain is nonempty). If A is true, then $A \to P(x)$ is equivalent to $P(x)$ for each x, so the left-hand side is equivalent to $\exists x\, P(x)$, which is equivalent to the right-hand side.

50. It is enough to find a counterexample. It is intuitively clear that the first proposition is asserting much more than the second. It is saying that one of the two predicates, P or Q, is universally true; whereas the second proposition is simply saying that for every x either $P(x)$ or $Q(x)$ holds, but which it is may well depend on x. As a simple counterexample, let $P(x)$ be the statement that x is odd, and let $Q(x)$ be the statement that x is even. Let the domain of discourse be the positive integers. The second proposition is true, since every positive integer is either odd or even. But the first proposition is false, since it is neither the case that all positive integers are odd nor the case that all of them are even.

52. **a)** This is false, since there are many values of x that make $x > 1$ true.
b) This is false, since there are two values of x that make $x^2 = 1$ true.
c) This is true, since by algebra we see that the unique solution to the equation is $x = 3$.
d) This is false, since there are no values of x that make $x = x + 1$ true.

54. There are only three cases in which $\exists x! P(x)$ is true, so we form the disjunction of these three cases. The answer is thus $(P(1) \wedge \neg P(2) \wedge \neg P(3)) \vee (\neg P(1) \wedge P(2) \wedge \neg P(3)) \vee (\neg P(1) \wedge \neg P(2) \wedge P(3))$.

56. A Prolog query returns a yes/no answer if there are no variables in the query, and it returns the values that make the query true if there are.
a) None of the facts was that Kevin was enrolled in EE 222. So the response is `no`.
b) One of the facts was that Kiko was enrolled in Math 273. So the response is `yes`.
c) Prolog returns the names of the courses for which Grossman is the instructor, namely just `cs301`.
d) Prolog returns the names of the instructor for CS 301, namely `grossman`.
e) Prolog returns the names of the instructors teaching any course that Kevin is enrolled in, namely `chan`, since Chan is the instructor in Math 273, the only course Kevin is enrolled in.

58. Following the idea and syntax of Example 28, we have the following rule:
`grandfather(X,Y) :- father(X,Z), father(Z,Y); father(X,Z), mother(Z,Y).`
Note that we used the comma to mean "and" and the semicolon to mean "or." For `X` to be the grandfather of `Y`, `X` must be either `Y`'s father's father or `Y`'s mother's father.

60. **a)** $\forall x(P(x) \to Q(x))$ **b)** $\exists x(R(x) \wedge \neg Q(x))$ **c)** $\exists x(R(x) \wedge \neg P(x))$
d) Yes. The unsatisfactory excuse guaranteed by part **(b)** cannot be a clear explanation by part **(a)**.

62. **a)** $\forall x(P(x) \to \neg S(x))$ **b)** $\forall x(R(x) \to S(x))$ **c)** $\forall x(Q(x) \to P(x))$ **d)** $\forall x(Q(x) \to \neg R(x))$
e) Yes. If x is one of my poultry, then he is a duck (by part **(c)**), hence not willing to waltz (part **(a)**). Since officers are always willing to waltz (part **(b)**), x is not an officer.

SECTION 1.5 Nested Quantifiers

2. **a)** There exists a real number x such that for every real number y, $xy = y$. This is asserting the existence of a multiplicative identity for the real numbers, and the statement is true, since we can take $x = 1$.

b) For every real number x and real number y, if x is nonnegative and y is negative, then the difference $x - y$ is positive. Or, more simply, a nonnegative number minus a negative number is positive (which is true).

c) For every real number x and real number y, there exists a real number z such that $x = y + z$. This is a true statement, since we can take $z = x - y$ in each case.

4. **a)** Some student in your class has taken some computer science course.

b) There is a student in your class who has taken every computer science course.

c) Every student in your class has taken at least one computer science course.

d) There is a computer science course that every student in your class has taken.

e) Every computer science course has been taken by at least one student in your class.

f) Every student in your class has taken every computer science course.

6. **a)** Randy Goldberg is enrolled in CS 252.

b) Someone is enrolled in Math 695.

c) Carol Sitea is enrolled in some course.

d) Some student is enrolled simultaneously in Math 222 and CS 252.

e) There exist two distinct people, the second of whom is enrolled in every course that the first is enrolled in.

f) There exist two distinct people enrolled in exactly the same courses.

8. **a)** $\exists x \exists y Q(x, y)$

b) This is the negation of part **(a)**, and so could be written either $\neg\exists x \exists y Q(x, y)$ or $\forall x \forall y \neg Q(x, y)$.

c) We assume from the wording that the statement means that the same person appeared on both shows: $\exists x(Q(x, \text{Jeopardy}) \wedge Q(x, \text{Wheel of Fortune}))$

d) $\forall y \exists x Q(x, y)$ **e)** $\exists x_1 \exists x_2 (Q(x_1, \text{Jeopardy}) \wedge Q(x_2, \text{Jeopardy}) \wedge x_1 \neq x_2)$

10. **a)** $\forall x F(x, \text{Fred})$ **b)** $\forall y F(\text{Evelyn}, y)$ **c)** $\forall x \exists y F(x, y)$ **d)** $\neg\exists x \forall y F(x, y)$ **e)** $\forall y \exists x F(x, y)$

f) $\neg\exists x(F(x, \text{Fred}) \wedge F(x, \text{Jerry}))$

g) $\exists y_1 \exists y_2 (F(\text{Nancy}, y_1) \wedge F(\text{Nancy}, y_2) \wedge y_1 \neq y_2 \wedge \forall y(F(\text{Nancy}, y) \rightarrow (y = y_1 \vee y = y_2)))$

h) $\exists y(\forall x F(x, y) \wedge \forall z(\forall x F(x, z) \rightarrow z = y))$ **i)** $\neg\exists x F(x, x)$

j) $\exists x \exists y(x \neq y \wedge F(x, y) \wedge \forall z((F(x, z) \wedge z \neq x) \rightarrow z = y))$ (We do not assume that this sentence is asserting that this person can or cannot fool her/himself.)

12. The answers to this exercise are not unique; there are many ways of expressing the same propositions symbolically. Note that $C(x, y)$ and $C(y, x)$ say the same thing.

a) $\neg I(\text{Jerry})$ **b)** $\neg C(\text{Rachel}, \text{Chelsea})$ **c)** $\neg C(\text{Jan}, \text{Sharon})$ **d)** $\neg\exists x\, C(x, \text{Bob})$

e) $\forall x(x \neq \text{Joseph} \leftrightarrow C(x, \text{Sanjay}))$ **f)** $\exists x\, \neg I(x)$ **g)** $\neg\forall x\, I(x)$ (same as **(f)**)

h) $\exists x \forall y(x = y \leftrightarrow I(y))$ **i)** $\exists x \forall y(x \neq y \leftrightarrow I(y))$ **j)** $\forall x(I(x) \rightarrow \exists y(x \neq y \wedge C(x, y)))$

k) $\exists x(I(x) \wedge \forall y(x \neq y \rightarrow \neg C(x, y)))$ **l)** $\exists x \exists y(x \neq y \wedge \neg C(x, y))$ **m)** $\exists x \forall y\, C(x, y)$

n) $\exists x \exists y(x \neq y \wedge \forall z\, \neg(C(x, z) \wedge C(y, z)))$ **o)** $\exists x \exists y(x \neq y \wedge \forall z(C(x, z) \vee C(y, z)))$

14. The answers to this exercise are not unique; there are many ways of expressing the same propositions symbolically. Our domain of discourse for persons here consists of people in this class. We need to make up a predicate in each case.

a) Let $S(x,y)$ mean that person x can speak language y. Then our statement is $\exists x\, S(x, \text{Hindi})$.

b) Let $P(x,y)$ mean that person x plays sport y. Then our statement is $\forall x \exists y\, P(x,y)$.

c) Let $V(x,y)$ mean that person x has visited state y. Then our statement is $\exists x(V(x, \text{Alaska}) \wedge \neg V(x, \text{Hawaii}))$.

d) Let $L(x,y)$ mean that person x has learned programming language y. Then our statement is $\forall x \exists y\, L(x,y)$.

e) Let $T(x,y)$ mean that person x has taken course y, and let $O(y,z)$ mean that course y is offered by department z. Then our statement is $\exists x \exists z \forall y (O(y,z) \to T(x,y))$.

f) Let $G(x,y)$ mean that persons x and y grew up in the same town. Then our statement is $\exists x \exists y (x \neq y \wedge G(x,y) \wedge \forall z (G(x,z) \to (x = y \vee x = z)))$.

g) Let $C(x,y,z)$ mean that persons x and y have chatted with each other in chat group z. Then our statement is $\forall x \exists y \exists z (x \neq y \wedge C(x,y,z))$.

16. We let $P(s,c,m)$ be the statement that student s has class standing c and is majoring in m. The variable s ranges over students in the class, the variable c ranges over the four class standings, and the variable m ranges over all possible majors.

a) The proposition is $\exists s \exists m P(s, \text{junior}, m)$. It is true from the given information.

b) The proposition is $\forall s \exists c P(s, c, \text{computer science})$. This is false, since there are some mathematics majors.

c) The proposition is $\exists s \exists c \exists m \big(P(s,c,m) \wedge (c \neq \text{junior}) \wedge (m \neq \text{mathematics})\big)$. This is true, since there is a sophomore majoring in computer science.

d) The proposition is $\forall s \big(\exists c P(s, c, \text{computer science}) \vee \exists m P(s, \text{sophomore}, m)\big)$. This is false, since there is a freshman mathematics major.

e) The proposition is $\exists m \forall c \exists s P(s,c,m)$. This is false. It cannot be that m is mathematics, since there is no senior mathematics major, and it cannot be that m is computer science, since there is no freshman computer science major. Nor, of course, can m be any other major.

18. **a)** $\forall f\, (H(f) \to \exists c\, A(c))$, where $A(x)$ means that console x is accessible, and $H(x)$ means that fault condition x is happening

b) $(\forall u \exists m\, (A(m) \wedge S(u,m))) \to \forall u\, R(u)$, where $A(x)$ means that the archive contains message x, $S(x,y)$ means that user x sent message y, and $R(x)$ means that the e-mail address of user x can be retrieved

c) $(\forall b \exists m\, D(m,b)) \leftrightarrow \exists p \neg C(p)$, where $D(x,y)$ means that mechanism x can detect breach y, and $C(x)$ means that process x has been compromised

d) $\forall x \forall y\, (x \neq y \to \exists p \exists q\, (p \neq q \wedge C(p,x,y) \wedge C(q,x,y)))$, where $C(p,x,y)$ means that path p connects endpoint x to endpoint y

e) $\forall x\, ((\forall u\, K(x,u)) \leftrightarrow x = \text{SysAdm})$, where $K(x,y)$ means that person x knows the password of user y

20. **a)** $\forall x \forall y ((x < 0) \wedge (y < 0) \to (xy > 0))$ **b)** $\forall x \forall y ((x > 0) \wedge (y > 0) \to ((x+y)/2 > 0))$

c) What does "necessarily" mean in this context? The best explanation is to assert that a certain universal conditional statement is not true. So we have $\neg \forall x \forall y ((x < 0) \wedge (y < 0) \to (x - y < 0))$. Note that we do not want to put the negation symbol inside (it is not true that the difference of two negative integers is never negative), nor do we want to negate just the conclusion (it is not true that the sum is always nonnegative). We could rewrite our solution by passing the negation inside, obtaining $\exists x \exists y ((x < 0) \wedge (y < 0) \wedge (x - y \geq 0))$.

d) $\forall x \forall y\, (|x + y| \leq |x| + |y|)$

22. $\exists x \forall a \forall b \forall c\, ((x > 0) \wedge x \neq a^2 + b^2 + c^2)$, where the domain of discourse consists of all integers

24. **a)** There exists an additive identity for the real numbers—a number that when added to every number does not change its value.

b) A nonnegative number minus a negative number is positive.
c) The difference of two nonpositive numbers is not necessarily nonpositive.
d) The product of two numbers is nonzero if and only if both factors are nonzero.

26. **a)** This is false, since $1+1 \neq 1-1$. **b)** This is true, since $2+0=2-0$.
c) This is false, since there are many values of y for which $1+y \neq 1-y$.
d) This is false, since the equation $x+2=x-2$ has no solution.
e) This is true, since we can take $x=y=0$. **f)** This is true, since we can take $y=0$ for each x.
g) This is true, since we can take $y=0$. **h)** This is false, since part **(d)** was false.
i) This is certainly false.

28. **a)** true (let $y=x^2$) **b)** false (no such y exists if x is negative) **c)** true (let $x=0$)
d) false (the commutative law for addition always holds) **e)** true (let $y=1/x$)
f) false (the reciprocal of y depends on y—there is not one x that works for all y) **g)** true (let $y=1-x$)
h) false (this system of equations is inconsistent)
i) false (this system has only one solution; if $x=0$, for example, then no y satisfies $y=2 \wedge -y=1$)
j) true (let $z=(x+y)/2$)

30. We need to use the transformations shown in Table 2 of Section 1.4, replacing $\neg\forall$ by $\exists\neg$, and replacing $\neg\exists$ by $\forall\neg$. In other words, we push all the negation symbols inside the quantifiers, changing the sense of the quantifiers as we do so, because of the equivalences in Table 2 of Section 1.4. In addition, we need to use De Morgan's laws (Section 1.3) to change the negation of a conjunction to the disjunction of the negations and to change the negation of a disjunction to the conjunction of the negations. We also use the fact that $\neg\neg p \equiv p$.
a) $\forall y \forall x\, \neg P(x,y)$ **b)** $\exists x \forall y\, \neg P(x,y)$ **c)** $\forall y(\neg Q(y) \vee \exists x\, R(x,y))$
d) $\forall y(\forall x\, \neg R(x,y) \wedge \exists x\, \neg S(x,y))$ **e)** $\forall y(\exists x \forall z\, \neg T(x,y,z) \wedge \forall x \exists z\, \neg U(x,y,z))$

32. As we push the negation symbol toward the inside, each quantifier it passes must change its type. For logical connectives we either use De Morgan's laws or recall that $\neg(p \to q) \equiv p \wedge \neg q$ (Table 7 in Section 1.3) and that $\neg(p \leftrightarrow q) \equiv \neg p \leftrightarrow q$ (Exercise 21 in Section 1.3).

a)
$$\begin{aligned} \neg\exists z \forall y \forall x\, T(x,y,z) &\equiv \forall z \neg \forall y \forall x\, T(x,y,z) \\ &\equiv \forall z \exists y \neg \forall x\, T(x,y,z) \\ &\equiv \forall z \exists y \exists x\, \neg T(x,y,z) \end{aligned}$$

b)
$$\begin{aligned} \neg(\exists x \exists y\, P(x,y) \wedge \forall x \forall y\, Q(x,y)) &\equiv \neg\exists x \exists y\, P(x,y) \vee \neg\forall x \forall y\, Q(x,y) \\ &\equiv \forall x \neg\exists y\, P(x,y) \vee \exists x \neg \forall y\, Q(x,y) \\ &\equiv \forall x \forall y\, \neg P(x,y) \vee \exists x \exists y\, \neg Q(x,y) \end{aligned}$$

c)
$$\begin{aligned} \neg\exists x \exists y (Q(x,y) \leftrightarrow Q(y,x)) &\equiv \forall x \neg \exists y (Q(x,y) \leftrightarrow Q(y,x)) \\ &\equiv \forall x \forall y \neg (Q(x,y) \leftrightarrow Q(y,x)) \\ &\equiv \forall x \forall y (\neg Q(x,y) \leftrightarrow Q(y,x)) \end{aligned}$$

d)
$$\begin{aligned} \neg\forall y \exists x \exists z\, (T(x,y,z) \vee Q(x,y)) &\equiv \exists y \neg \exists x \exists z\, (T(x,y,z) \vee Q(x,y)) \\ &\equiv \exists y \forall x \neg \exists z\, (T(x,y,z) \vee Q(x,y)) \\ &\equiv \exists y \forall x \forall z\, \neg (T(x,y,z) \vee Q(x,y)) \\ &\equiv \exists y \forall x \forall z\, (\neg T(x,y,z) \wedge \neg Q(x,y)) \end{aligned}$$

34. The logical expression is asserting that the domain consists of at most two members. (It is saying that whenever you have two unequal objects, any object has to be one of those two. Note that this is vacuously true for domains with one element.) Therefore any domain having one or two members will make it true (such as the female members of the United States Supreme Court in 2005), and any domain with more than two members will make it false (such as all members of the United States Supreme Court in 2005).

36. In each case we need to specify some predicates and identify the domain of discourse.

a) Let $L(x,y)$ mean that person x has lost y dollars playing the lottery. The original statement is then $\neg\exists x\exists y(y > 1000 \wedge L(x,y))$. Its negation of course is $\exists x\exists y(y > 1000 \wedge L(x,y))$; someone has lost more than \$1000 playing the lottery.

b) Let $C(x,y)$ mean that person x has chatted with person y. The given statement is $\exists x\exists y(y \neq x \wedge \forall z(z \neq x \rightarrow (z = y \leftrightarrow C(x,z))))$. The negation is therefore $\forall x\forall y(y \neq x \rightarrow \exists z(z \neq x \wedge \neg(z = y \leftrightarrow C(x,z))))$. In English, everybody in this class has either chatted with no one else or has chatted with two or more others.

c) Let $E(x,y)$ mean that person x has sent e-mail to person y. The given statement is $\neg\exists x\exists y\exists z(y \neq z \wedge x \neq y \wedge x \neq z \wedge \forall w(w \neq x \rightarrow (E(x,w) \leftrightarrow (w = y \vee w = z))))$. The negation is obviously $\exists x\exists y\exists z(y \neq z \wedge x \neq y \wedge x \neq z \wedge \forall w(w \neq x \rightarrow (E(x,w) \leftrightarrow (w = y \vee w = z))))$. In English, some student in this class has sent e-mail to exactly two other students in this class.

d) Let $S(x,y)$ mean that student x has solved exercise y. The statement is $\exists x\forall y\, S(x,y)$. The negation is $\forall x\exists y\, \neg S(x,y)$. In English, for every student in this class, there is some exercise that he or she has not solved. (One could also interpret the given statement as asserting that for every exercise, there exists a student—perhaps a different one for each exercise—who has solved it. In that case the order of the quantifiers would be reversed. Word order in English sometimes makes for a little ambiguity.)

e) Let $S(x,y)$ mean that student x has solved exercise y, and let $B(y,z)$ mean that exercise y is in section z of the book. The statement is $\neg\exists x\forall z\exists y(B(y,z) \wedge S(x,y))$. The negation is of course $\exists x\forall z\exists y(B(y,z) \wedge S(x,y))$. In English, some student has solved at least one exercise in every section of this book.

38. a) In English, the negation is "Some student in this class does not like mathematics." With the obvious propositional function, this is $\exists x \neg L(x)$.

b) In English, the negation is "Every student in this class has seen a computer." With the obvious propositional function, this is $\forall x S(x)$.

c) In English, the negation is "For every student in this class, there is a mathematics course that this student has not taken." With the obvious propositional function, this is $\forall x\exists c \neg T(x,c)$.

d) As in Exercise 15f, let $P(z,y)$ be "Room z is in building y," and let $Q(x,z)$ be "Student x has been in room z." Then the original statement is $\exists x\forall y\exists z\big(P(z,y) \wedge Q(x,z)\big)$. To form the negation, we change all the quantifiers and put the negation on the inside, then apply De Morgan's law. The negation is therefore $\forall x\exists y\forall z\big(\neg P(z,y) \vee \neg Q(x,z)\big)$, which is also equivalent to $\forall x\exists y\forall z\big(P(z,y) \rightarrow \neg Q(x,z)\big)$. In English, this could be read, "For every student there is a building such that for every room in that building, the student has not been in that room."

40. a) There are many counterexamples. If $x = 2$, then there is no y among the integers such that $2 = 1/y$, since the only solution of this equation is $y = 1/2$. Even if we were working in the domain of real numbers, $x = 0$ would provide a counterexample, since $0 = 1/y$ for no real number y.

b) We can rewrite $y^2 - x < 100$ as $y^2 < 100 + x$. Since squares can never be negative, no such y exists if x is, say, -200. This x provides a counterexample.

c) This is not true, since sixth powers are both squares and cubes. Trivial counterexamples would include $x = y = 0$ and $x = y = 1$, but we can also take something like $x = 27$ and $y = 9$, since $27^2 = 3^6 = 9^3$.

42. The distributive law is just the statement that $x(y+z) = xy+xz$ for all real numbers. Therefore the expression we want is $\forall x \forall y \forall z\,(x(y+z) = xy + xz)$, where the quantifiers are assumed to range over (i.e., the domain of discourse is) the real numbers.

44. We want to say that for each triple of coefficients (the a, b, and c in the expression ax^2+bx+c, where we insist that $a \neq 0$ so that this actually is quadratic), there are at most two values of x making that expression equal to 0. The domain here is all real numbers. We write $\forall a \forall b \forall c(a \neq 0 \to \forall x_1 \forall x_2 \forall x_3 (ax_1^2 + bx_1 + c = 0 \wedge ax_2^2 + bx_2 + c = 0 \wedge ax_3^2 + bx_3 + c = 0) \to (x_1 = x_2 \vee x_1 = x_3 \vee x_2 = x_3))$.

46. This statement says that there is a number that is less than or equal to all squares.

a) This is false, since no matter how small a positive number x we might choose, if we let $y = \sqrt{x/2}$, then $x = 2y^2$, and it will not be true that $x \le y^2$.

b) This is true, since we can take $x = -1$, for example.

c) This is true, since we can take $x = -1$, for example.

48. We need to show that each of these propositions implies the other. Suppose that $\forall x P(x) \vee \forall x Q(x)$ is true. We want to show that $\forall x \forall y (P(x) \vee Q(y))$ is true. By our hypothesis, one of two things must be true. Either P is universally true, or Q is universally true. In the first case, $\forall x \forall y (P(x) \vee Q(y))$ is true, since the first expression in the disjunction is true, no matter what x and y are; and in the second case, $\forall x \forall y (P(x) \vee Q(y))$ is also true, since now the second expression in the disjunction is true, no matter what x and y are. Next we need to prove the converse. So suppose that $\forall x \forall y (P(x) \vee Q(y))$ is true. We want to show that $\forall x P(x) \vee \forall x Q(x)$ is true. If $\forall x P(x)$ is true, then we are done. Otherwise, $P(x_0)$ must be false for some x_0 in the domain of discourse. For this x_0, then, the hypothesis tells us that $P(x_0) \vee Q(y)$ is true, no matter what y is. Since $P(x_0)$ is false, it must be the case that $Q(y)$ is true for each y. In other words, $\forall y Q(y)$ is true, or, to change the name of the meaningless quantified variable, $\forall x Q(x)$ is true. This certainly implies that $\forall x P(x) \vee \forall x Q(x)$ is true, as desired.

50. **a)** By Exercises 45 and 46b in Section 1.4, we can simply bring the existential quantifier outside: $\exists x (P(x) \vee Q(x) \vee A)$.

b) By Exercise 48 of the current section, the expression inside the parentheses is logically equivalent to $\forall x \forall y (P(x) \vee Q(y))$. Applying the negation operation, we obtain $\exists x \exists y \neg (P(x) \vee Q(y))$.

c) First we rewrite this using Table 7 in Section 1.3 as $\exists x Q(x) \vee \neg \exists x P(x)$, which is equivalent to $\exists x Q(x) \vee \forall x \neg P(x)$. To combine the existential and universal statements we use Exercise 49b of the current section, obtaining $\forall x \exists y (\neg P(x) \vee Q(y))$, which is in prenex normal form.

52. We simply want to say that there exists an x such that $P(x)$ holds, and that every y such that $P(y)$ holds must be this same x. Thus we write $\exists x \big(P(x) \wedge \forall y (P(y) \to y = x)\big)$. Even more compactly, we can write $\exists x \forall y (P(y) \leftrightarrow y = x)$.

SECTION 1.6 Rules of Inference

2. This is modus tollens. The first statement is $p \to q$, where p is "George does not have eight legs" and q is "George is not a spider." The second statement is $\neg q$. The third is $\neg p$. Modus tollens is valid. We can therefore conclude that the conclusion of the argument (third statement) is true, given that the hypotheses (the first two statements) are true.

4. **a)** We have taken the conjunction of two propositions and asserted one of them. This is, according to Table 1, simplification.

b) We have taken the disjunction of two propositions and the negation of one of them, and asserted the other. This is, according to Table 1, disjunctive syllogism. See Table 1 for the other parts of this exercise as well.

c) modus ponens **d)** addition **e)** hypothetical syllogism

6. Let r be the proposition "It rains," let f be the proposition "It is foggy," let s be the proposition "The sailing race will be held," let l be the proposition "The life saving demonstration will go on," and let t be the proposition "The trophy will be awarded." We are given premises $(\neg r \vee \neg f) \to (s \wedge l)$, $s \to t$, and $\neg t$. We want to conclude r. We set up the proof in two columns, with reasons, as in Example 6. Note that it is valid to replace subexpressions by other expressions logically equivalent to them.

Step	**Reason**
1. $\neg t$	Hypothesis
2. $s \to t$	Hypothesis
3. $\neg s$	Modus tollens using (1) and (2)
4. $(\neg r \vee \neg f) \to (s \wedge l)$	Hypothesis
5. $(\neg(s \wedge l)) \to \neg(\neg r \vee \neg f)$	Contrapositive of (4)
6. $(\neg s \vee \neg l) \to (r \wedge f)$	De Morgan's law and double negative
7. $\neg s \vee \neg l$	Addition, using (3)
8. $r \wedge f$	Modus ponens using (6) and (7)
9. r	Simplification using (8)

8. First we use universal instantiation to conclude from "For all x, if x is a man, then x is not an island" the special case of interest, "If Manhattan is a man, then Manhattan is not an island." Then we form the contrapositive (using also double negative): "If Manhattan is an island, then Manhattan is not a man." Finally we use modus ponens to conclude that Manhattan is not a man. Alternatively, we could apply modus tollens.

10. **a)** If we use modus tollens starting from the back, then we conclude that I am not sore. Another application of modus tollens then tells us that I did not play hockey.

b) We really can't conclude anything specific here.

c) By universal instantiation, we conclude from the first conditional statement by modus ponens that dragonflies have six legs, and we conclude by modus tollens that spiders are not insects. We could say using existential generalization that, for example, there exists a non-six-legged creature that eats a six-legged creature, and that there exists a non-insect that eats an insect.

d) We can apply universal instantiation to the conditional statement and conclude that if Homer (respectively, Maggie) is a student, then he (she) has an Internet account. Now modus tollens tells us that Homer is not a student. There are no conclusions to be drawn about Maggie.

e) The first conditional statement is that if x is healthy to eat, then x does not taste good. Universal instantiation and modus ponens therefore tell us that tofu does not taste good. The third sentence says that if you eat x, then x tastes good. Therefore the fourth hypothesis already follows (by modus tollens) from the first three. No conclusions can be drawn about cheeseburgers from these statements.

f) By disjunctive syllogism, the first two hypotheses allow us to conclude that I am hallucinating. Therefore by modus ponens we know that I see elephants running down the road.

12. Applying Exercise 11, we want to show that the conclusion r follows from the five premises $(p \wedge t) \rightarrow (r \vee s)$, $q \rightarrow (u \wedge t)$, $u \rightarrow p$, $\neg s$, and q. From q and $q \rightarrow (u \wedge t)$ we get $u \wedge t$ by modus ponens. From there we get both u and t by simplification (and the commutative law). From u and $u \rightarrow p$ we get p by modus ponens. From p and t we get $p \wedge t$ by conjunction. From that and $(p \wedge t) \rightarrow (r \vee s)$ we get $r \vee s$ by modus ponens. From that and $\neg s$ we finally get r by disjunctive syllogism.

14. In each case we set up the proof in two columns, with reasons, as in Example 6.

a) Let $c(x)$ be "x is in this class," let $r(x)$ be "x owns a red convertible," and let $t(x)$ be "x has gotten a speeding ticket." We are given premises $c(\text{Linda})$, $r(\text{Linda})$, $\forall x(r(x) \rightarrow t(x))$, and we want to conclude $\exists x(c(x) \wedge t(x))$.

Step	**Reason**
1. $\forall x(r(x) \rightarrow t(x))$	Hypothesis
2. $r(\text{Linda}) \rightarrow t(\text{Linda})$	Universal instantiation using (1)
3. $r(\text{Linda})$	Hypothesis
4. $t(\text{Linda})$	Modus ponens using (2) and (3)
5. $c(\text{Linda})$	Hypothesis
6. $c(\text{Linda}) \wedge t(\text{Linda})$	Conjunction using (4) and (5)
7. $\exists x(c(x) \wedge t(x))$	Existential generalization using (6)

b) Let $r(x)$ be "r is one of the five roommates listed," let $d(x)$ be "x has taken a course in discrete mathematics," and let $a(x)$ be "x can take a course in algorithms." We are given premises $\forall x(r(x) \rightarrow d(x))$ and $\forall x(d(x) \rightarrow a(x))$, and we want to conclude $\forall x(r(x) \rightarrow a(x))$. In what follows y represents an arbitrary person.

Step	**Reason**
1. $\forall x(r(x) \rightarrow d(x))$	Hypothesis
2. $r(y) \rightarrow d(y)$	Universal instantiation using (1)
3. $\forall x(d(x) \rightarrow a(x))$	Hypothesis
4. $d(y) \rightarrow a(y)$	Universal instantiation using (3)
5. $r(y) \rightarrow a(y)$	Hypothetical syllogism using (2) and (4)
6. $\forall x(r(x) \rightarrow a(x))$	Universal generalization using (5)

c) Let $s(x)$ be "x is a movie produced by Sayles," let $c(x)$ be "x is a movie about coal miners," and let $w(x)$ be "movie x is wonderful." We are given premises $\forall x(s(x) \rightarrow w(x))$ and $\exists x(s(x) \wedge c(x))$, and we want to conclude $\exists x(c(x) \wedge w(x))$. In our proof, y represents an unspecified particular movie.

Step	**Reason**
1. $\exists x(s(x) \wedge c(x))$	Hypothesis
2. $s(y) \wedge c(y)$	Existential instantiation using (1)
3. $s(y)$	Simplification using (2)
4. $\forall x(s(x) \rightarrow w(x))$	Hypothesis
5. $s(y) \rightarrow w(y)$	Universal instantiation using (4)
6. $w(y)$	Modus ponens using (3) and (5)
7. $c(y)$	Simplification using (2)
8. $w(y) \wedge c(y)$	Conjunction using (6) and (7)
9. $\exists x(c(x) \wedge w(x))$	Existential generalization using (8)

d) Let $c(x)$ be "x is in this class," let $f(x)$ be "x has been to France," and let $l(x)$ be "x has visited the Louvre." We are given premises $\exists x(c(x) \wedge f(x))$, $\forall x(f(x) \rightarrow l(x))$, and we want to conclude $\exists x(c(x) \wedge l(x))$.

In our proof, y represents an unspecified particular person.

Step	**Reason**
1. $\exists x(c(x) \wedge f(x))$	Hypothesis
2. $c(y) \wedge f(y)$	Existential instantiation using (1)
3. $f(y)$	Simplification using (2)
4. $c(y)$	Simplification using (2)
5. $\forall x(f(x) \to l(x))$	Hypothesis
6. $f(y) \to l(y)$	Universal instantiation using (5)
7. $l(y)$	Modus ponens using (3) and (6)
8. $c(y) \wedge l(y)$	Conjunction using (4) and (7)
9. $\exists x(c(x) \wedge l(x))$	Existential generalization using (8)

16. **a)** This is correct, using universal instantiation and modus tollens.
b) This is not correct. After applying universal instantiation, it contains the fallacy of denying the hypothesis.
c) After applying universal instantiation, it contains the fallacy of affirming the conclusion.
d) This is correct, using universal instantiation and modus ponens.

18. We know that *some* s exists that makes $S(s, \text{Max})$ true, but we cannot conclude that Max is one such s. Therefore this first step is invalid.

20. **a)** This is invalid. It is the fallacy of affirming the conclusion. Letting $a = -2$ provides a counterexample.
b) This is valid; it is modus ponens.

22. We will give an argument establishing the conclusion. We want to show that all hummingbirds are small. Let Tweety be an arbitrary hummingbird. We must show that Tweety is small. The first premise implies that if Tweety is a hummingbird, then Tweety is richly colored. Therefore by (universal) modus ponens we can conclude that Tweety is richly colored. The third premise implies that if Tweety does not live on honey, then Tweety is not richly colored. Therefore by (universal) modus tollens we can now conclude that Tweety does live on honey. Finally, the second premise implies that if Tweety is a large bird, then Tweety does not live on honey. Therefore again by (universal) modus tollens we can now conclude that Tweety is not a large bird, i.e., that Tweety is small, as desired. Notice that we invoke universal generalization as the last step.

24. Steps 3 and 5 are incorrect; simplification applies to conjunctions, not disjunctions.

26. We want to show that the conditional statement $P(a) \to R(a)$ is true for all a in the domain; the desired conclusion then follows by universal generalization. Thus we want to show that if $P(a)$ is true for a particular a, then $R(a)$ is also true. For such an a, by universal modus ponens from the first premise we have $Q(a)$, and then by universal modus ponens from the second premise we have $R(a)$, as desired.

28. We want to show that the conditional statement $\neg R(a) \to P(a)$ is true for all a in the domain; the desired conclusion then follows by universal generalization. Thus we want to show that if $\neg R(a)$ is true for a particular a, then $P(a)$ is also true. For such an a, universal modus tollens applied to the second premise gives us $\neg(\neg P(a) \wedge Q(a))$. By rules from propositional logic, this gives us $P(a) \vee \neg Q(a)$. By universal generalization from the first premise, we have $P(a) \vee Q(a)$. Now by resolution we can conclude $P(a) \vee P(a)$, which is logically equivalent to $P(a)$, as desired.

30. Let a be "Allen is a good boy"; let h be "Hillary is a good girl"; let d be "David is happy." Then our assumptions are $\neg a \vee h$ and $a \vee d$. Using resolution gives us $h \vee d$, as desired.

32. We apply resolution to give the tautology $(p \vee \mathbf{F}) \wedge (\neg p \vee \mathbf{F}) \to (\mathbf{F} \vee \mathbf{F})$. The left-hand side is equivalent to $p \wedge \neg p$, since $p \vee \mathbf{F}$ is equivalent to p, and $\neg p \vee \mathbf{F}$ is equivalent to $\neg p$. The right-hand side is equivalent to $\mathbf{F}$. Since the conditional statement is true, and the conclusion is false, it follows that the hypothesis, $p \wedge \neg p$, is false, as desired.

34. Let us use the following letters to stand for the relevant propositions: d for "logic is difficult"; s for "many students like logic"; and e for "mathematics is easy." Then the assumptions are $d \vee \neg s$ and $e \to \neg d$. Note that the first of these is equivalent to $s \to d$, since both forms are false if and only if s is true and d is false. In addition, let us note that the second assumption is equivalent to its contrapositive, $d \to \neg e$. And finally, by combining these two conditional statements, we see that $s \to \neg e$ also follows from our assumptions.

a) Here we are asked whether we can conclude that $s \to \neg e$. As we noted above, the answer is yes, this conclusion is valid.

b) The question concerns $\neg e \to \neg s$. This is equivalent to its contrapositive, $s \to e$. That doesn't seem to follow from our assumptions, so let's find a case in which the assumptions hold but this conditional statement does not. This conditional statement fails in the case in which s is true and e is false. If we take d to be true as well, then both of our assumptions are true. Therefore this conclusion is not valid.

c) The issue is $\neg e \vee d$, which is equivalent to the conditional statement $e \to d$. This does *not* follow from our assumptions. If we take d to be false, e to be true, and s to be false, then this proposition is false but our assumptions are true.

d) The issue is $\neg d \vee \neg e$, which is equivalent to the conditional statement $d \to \neg e$. We noted above that this validly follows from our assumptions.

e) This sentence says $\neg s \to (\neg e \vee \neg d)$. The only case in which this is false is when s is false and both e and d are true. But in this case, our assumption $e \to \neg d$ is also violated. Therefore, in all cases in which the assumptions hold, this statement holds as well, so it *is* a valid conclusion.

SECTION 1.7 Introduction to Proofs

2. We must show that whenever we have two even integers, their sum is even. Suppose that a and b are two even integers. Then there exist integers s and t such that $a = 2s$ and $b = 2t$. Adding, we obtain $a + b = 2s + 2t = 2(s + t)$. Since this represents $a + b$ as 2 times the integer $s + t$, we conclude that $a + b$ is even, as desired.

4. We must show that whenever we have an even integer, its negative is even. Suppose that a is an even integer. Then there exists an integer s such that $a = 2s$. Its additive inverse is $-2s$, which by rules of arithmetic and algebra (see Appendix 1) equals $2(-s)$. Since this is 2 times the integer $-s$, it is even, as desired.

6. An odd number is one of the form $2n + 1$, where n is an integer. We are given two odd numbers, say $2a + 1$ and $2b + 1$. Their product is $(2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$. This last expression shows that the product is odd, since it is of the form $2n + 1$, with $n = 2ab + a + b$.

8. Let $n = m^2$. If $m = 0$, then $n + 2 = 2$, which is not a perfect square, so we can assume that $m \geq 1$. The smallest perfect square greater than n is $(m + 1)^2$, and we have $(m + 1)^2 = m^2 + 2m + 1 = n + 2m + 1 > n + 2 \cdot 1 + 1 > n + 2$. Therefore $n + 2$ cannot be a perfect square.

10. A rational number is a number that can be written in the form x/y where x and y are integers and $y \neq 0$. Suppose that we have two rational numbers, say a/b and c/d. Then their product is, by the usual rules for multiplication of fractions, $(ac)/(bd)$. Note that both the numerator and the denominator are integers, and that $bd \neq 0$ since b and d were both nonzero. Therefore the product is, by definition, a rational number.

12. This is true. Suppose that a/b is a nonzero rational number and that x is an irrational number. We must prove that the product xa/b is also irrational. We give a proof by contradiction. Suppose that xa/b were rational. Since $a/b \neq 0$, we know that $a \neq 0$, so b/a is also a rational number. Let us multiply this rational number b/a by the assumed rational number xa/b. By Exercise 26, the product is rational. But the product is $(b/a)(xa/b) = x$, which is irrational by hypothesis. This is a contradiction, so in fact xa/b must be irrational, as desired.

14. If x is rational and not zero, then by definition we can write $x = p/q$, where p and q are nonzero integers. Since $1/x$ is then q/p and $p \neq 0$, we can conclude that $1/x$ is rational.

16. We give a proof by contraposition. If it is not true than m is even or n is even, then m and n are both odd. By Exercise 6, this tells us that mn is odd, and our proof is complete.

18. **a)** We must prove the contrapositive: If n is odd, then $3n+2$ is odd. Assume that n is odd. Then we can write $n = 2k+1$ for some integer k. Then $3n+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1$. Thus $3n+2$ is two times some integer plus 1, so it is odd.

b) Suppose that $3n+2$ is even and that n is odd. Since $3n+2$ is even, so is $3n$. If we add subtract an odd number from an even number, we get an odd number, so $3n - n = 2n$ is odd. But this is obviously not true. Therefore our supposition was wrong, and the proof by contradiction is complete.

20. We need to prove the proposition "If 1 is a positive integer, then $1^2 \geq 1$." The conclusion is the true statement $1 \geq 1$. Therefore the conditional statement is true. This is an example of a trivial proof, since we merely showed that the conclusion was true.

22. We give a proof by contradiction. Suppose that we don't get a pair of blue socks or a pair of black socks. Then we drew at most one of each color. This accounts for only two socks. But we are drawing three socks. Therefore our supposition that we did not get a pair of blue socks or a pair of black socks is incorrect, and our proof is complete.

24. We give a proof by contradiction. If there were at most two days falling in the same month, then we could have at most $2 \cdot 12 = 24$ days, since there are 12 months. Since we have chosen 25 days, at least three of them must fall in the same month.

26. We need to prove two things, since this is an "if and only if" statement. First let us prove directly that if n is even then $7n+4$ is even. Since n is even, it can be written as $2k$ for some integer k. Then $7n+4 = 14k+4 = 2(7k+2)$. This is 2 times an integer, so it is even, as desired. Next we give a proof by contraposition that if $7n+4$ is even then n is even. So suppose that n is not even, i.e., that n is odd. Then n can be written as $2k+1$ for some integer k. Thus $7n+4 = 14k+11 = 2(7k+5)+1$. This is 1 more than 2 times an integer, so it is odd. That completes the proof by contraposition.

28. There are two things to prove. For the "if" part, there are two cases. If $m = n$, then of course $m^2 = n^2$; if $m = -n$, then $m^2 = (-n)^2 = (-1)^2 n^2 = n^2$. For the "only if" part, we suppose that $m^2 = n^2$. Putting everything on the left and factoring, we have $(m+n)(m-n) = 0$. Now the only way that a product of two numbers can be zero is if one of them is zero. Therefore we conclude that either $m+n = 0$ (in which case $m = -n$), or else $m - n = 0$ (in which case $m = n$), and our proof is complete.

30. We write these in symbols: $a < b$, $(a+b)/2 > a$, and $(a+b)/2 < b$. The latter two are equivalent to $a+b > 2a$ and $a+b < 2b$, respectively, and these are in turn equivalent to $b > a$ and $a < b$, respectively. It is now clear that all three statements are equivalent.

32. We give direct proofs that (i) implies (ii), that (ii) implies (iii), and that (iii) implies (i). That will suffice. For the first, suppose that $x = p/q$ where p and q are integers with $q \neq 0$. Then $x/2 = p/(2q)$, and this is rational, since p and $2q$ are integers with $2q \neq 0$. For the second, suppose that $x/2 = p/q$ where p and q are integers with $q \neq 0$. Then $x = (2p)/q$, so $3x - 1 = (6p)/q - 1 = (6p - q)/q$ and this is rational, since $6p - q$ and q are integers with $q \neq 0$. For the last, suppose that $3x - 1 = p/q$ where p and q are integers with $q \neq 0$. Then $x = (p/q + 1)/3 = (p + q)/(3q)$, and this is rational, since $p + q$ and $3q$ are integers with $3q \neq 0$.

34. No. This line of reasoning shows that *if* $\sqrt{2x^2 - 1} = x$, then we must have $x = 1$ or $x = -1$. These are therefore the only possible solutions, but we have no guarantee that they *are* solutions, since not all of our steps were reversible (in particular, squaring both sides). Therefore we *must* substitute these values back into the original equation to determine whether they do indeed satisfy it.

36. The only conditional statements not shown directly are $p_1 \leftrightarrow p_2$, $p_2 \leftrightarrow p_4$, and $p_3 \leftrightarrow p_4$. But these each follow with one or more intermediate steps: $p_1 \leftrightarrow p_2$, since $p_1 \leftrightarrow p_3$ and $p_3 \leftrightarrow p_2$; $p_2 \leftrightarrow p_4$, since $p_2 \leftrightarrow p_1$ (just established) and $p_1 \leftrightarrow p_4$; and $p_3 \leftrightarrow p_4$, since $p_3 \leftrightarrow p_1$ and $p_1 \leftrightarrow p_4$.

38. We must find a number that cannot be written as the sum of the squares of three integers. We claim that 7 is such a number (in fact, it is the smallest such number). The only squares that can be used to contribute to the sum are 0, 1, and 4. We cannot use two 4's, because their sum exceeds 7. Therefore we can use at most one 4, which means that we must get 3 using just 0's and 1's. Clearly three 1's are required for this, bringing the total number of squares used to four. Thus 7 cannot be written as the sum of three squares.

40. Suppose that we look at the ten groups of integers in three consecutive locations around the circle (first-second-third, second-third-fourth, $\ldots$, eighth-ninth-tenth, ninth-tenth-first, and tenth-first-second). Since each number from 1 to 10 gets used three times in these groups, the sum of the sums of the ten groups must equal three times the sum of the numbers from 1 to 10, namely $3 \cdot 55 = 165$. Therefore the average sum is $165/10 = 16.5$. By Exercise 39, at least one of the sums must be greater than or equal to 16.5, and since the sums are whole numbers, this means that at least one of the sums must be greater than or equal to 17.

42. We show that each of these is equivalent to the statement (v) n is odd, say $n = 2k+1$. Example 1 showed that (v) implies (i), and Example 8 showed that (i) implies (v). For $(v) \rightarrow (ii)$ we see that $1 - n = 1 - (2k+1) = 2(-k)$ is even. Conversely, if n were even, say $n = 2m$, then we would have $1 - n = 1 - 2m = 2(-m) + 1$, so $1 - n$ would be odd, and this completes the proof by contraposition that $(ii) \rightarrow (v)$. For $(v) \rightarrow (iii)$, we see that $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$ is odd. Conversely, if n were even, say $n = 2m$, then we would have $n^3 = 2(4m^3)$, so n^3 would be even, and this completes the proof by contraposition that $(iii) \rightarrow (v)$. Finally, for $(v) \rightarrow (iv)$, we see that $n^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2 = 2(2k^2 + 2k + 1)$ is even. Conversely, if n were even, say $n = 2m$, then we would have $n^2 + 1 = 2(2m^2) + 1$, so $n^2 + 1$ would be odd, and this completes the proof by contraposition that $(iv) \rightarrow (v)$.

SECTION 1.8 Proof Methods and Strategy

2. The cubes that might go into the sum are 1, 8, 27, 64, 125, 216, 343, 512, and 729. We must show that no two of these sum to a number on this list. If we try the 45 combinations ($1+1$, $1+8$, $\ldots$, $1+729$, $8+8$, $8+27$, $\ldots$ $8+729$, $\ldots$, $729+729$), we see that none of them works. Having exhausted the possibilities, we conclude that no cube less than 1000 is the sum of two cubes.

4. There are three main cases, depending on which of the three numbers is smallest. If a is smallest (or tied for smallest), then clearly $a \le \min(b,c)$, and so the left-hand side equals a. On the other hand, for the right-hand side we have $\min(a,c) = a$ as well. In the second case, b is smallest (or tied for smallest). The same reasoning shows us that the right-hand side equals b; and the left-hand side is $\min(a,b) = b$ as well. In the final case, in which c is smallest (or tied for smallest), the left-hand side is $\min(a,c) = c$, whereas the right-hand side is clearly also c. Since one of the three has to be smallest we have taken care of all the cases.

6. Because x and y are of opposite parities, we can assume, without loss of generality, that x is even and y is odd. This tells us that $x = 2m$ for some integer m and $y = 2n+1$ for some integer n. Then $5x+5y = 5(2m)+5(2n+1) = 10m+10n+1 = 10(m+n)+1 = 2\cdot 5(m+n)+1$, which satisfies the definition of being an odd number.

8. The number 1 has this property, since the only positive integer not exceeding 1 is 1 itself, and therefore the sum is 1. This is a constructive proof.

10. The only perfect squares that differ by 1 are 0 and 1. Therefore these two consecutive integers cannot both be perfect squares. This is a nonconstructive proof—we do not know which of them meets the requirement. (In fact, a computer algebra system will tell us that neither of them is a perfect square.)

12. Of these three numbers, at least two must have the same sign (both positive or both negative), since there are only two signs. (It is conceivable that some of them are zero, but we view zero as positive for the purposes of this problem.) The product of two with the same sign is nonnegative. This was a nonconstructive proof, since we have not identified which product is nonnegative. (In fact, a computer algebra system will tell us that all three are positive, so all three products are positive.)

14. An assertion like this one is implicitly universally quantified—it means that *for all* rational numbers a and b, a^b is rational. To disprove such a statement it suffices to provide one counterexample. Take $a = 2$ and $b = 1/2$. Then $a^b = 2^{1/2} = \sqrt{2}$, and we know from Example 10 in Section 1.7 that $\sqrt{2}$ is not rational.

16. We know from algebra that the following equations are equivalent: $ax+b=c$, $ax = c-b$. $x = (c-b)/a$. This shows, constructively, what the unique solution of the given equation is.

18. Given r, let a be the closest integer to r less than r, and let b be the closest integer to r greater than r. In the notation to be introduced in Section 2.3, $a = \lfloor r \rfloor$ and $b = \lceil r \rceil$. In fact, $b = a+1$. Clearly the distance between r and any integer other than a or b is greater than 1 so cannot be less than $1/2$. Furthermore, since r is irrational, it cannot be exactly half-way between a and b, so exactly one of $r-a < 1/2$ and $b-r < 1/2$ holds.

20. Given x, let n be the greatest integer less than or equal to x, and let $\epsilon = x - n$. In the notation to be introduced in Section 2.3, $n = \lfloor x \rfloor$. Clearly $0 \le \epsilon < 1$, and ϵ is unique for this n. Any other choice of n would cause the required ϵ to be less than 0 or greater than or equal to 1, so n is unique as well.

22. We follow the hint. The square of every real number is nonnegative, so $(x-1/x)^2 \ge 0$. Multiplying this out and simplifying, we obtain $x^2 - 2 + 1/x^2 \ge 0$, so $x^2 + 1/x^2 \ge 2$, as desired.

24. Let $x = 1$ and $y = 10$. Then their arithmetic is 5.5 and their quadratic mean is $\sqrt{50.5} \approx 7.11$. Similarly, if $x = 5$ and $y = 8$, then the arithmetic mean is $(5+8)/2 = 6.5$ and the quadratic mean is $\sqrt{(5^2+8^2)/2} \approx 6.67$. So we conjecture that the quadratic mean is always greater than or equal to the arithmetic mean. Thus we want to prove that

$$\sqrt{\frac{x^2+y^2}{2}} \ge \frac{x+y}{2}$$

for all positive real numbers x and y.Doing some algebra, we find that this inequality is equivalent to the true statement that $(x-y)^2 \ge 0$:

$$\begin{aligned} \sqrt{\frac{x^2+y^2}{2}} &\ge \frac{x+y}{2} \\ 2x^2+2y^2 &\ge x^2+2xy+y^2 \\ x^2-2xy+y^2 &\ge 0 \\ (x-y)^2 &\ge 0 \end{aligned}$$

In fact, our argument also shows that equality holds if and only if $x = y$.

26. If we were to end up with nine 0's, then in the step before this we must have had either nine 0's or nine 1's, since each adjacent pair of bits must have been equal and therefore all the bits must have been the same. Thus if we are to start with something other than nine 0's and yet end up with nine 0's, we must have had nine 1's at some point. But in the step before that each adjacent pair of bits must have been different; in other words, they must have alternated 0, 1, 0, 1, and so on. This is impossible with an odd number of bits. This contradiction shows that we can never get nine 0's.

28. Clearly only the last two digits of n contribute to the last two digits of n^2. So we can compute 0^2, 1^2, 2^2, 3^2, ..., 99^2, and record the last two digits, omitting repetitions. We obtain 00, 01, 04, 09, 16, 25, 36, 49, 64, 81, 21, 44, 69, 96, 56, 89, 24, 61, 41, 84, 29, 76. From that point on, the list repeats in reverse order (as we take the squares from 25^2 to 49^2, and then it all repeats again as we take the squares from 50^2 to 99^2). The reason for these last two statements are that $(50-n)^2 = 2500 - 100n + n^2$, so $(50-n)^2$ and n^2 have the same two final digits, and $(50+n)^2 = 2500 + 100n + n^2$, so $(50+n)^2$ and n^2 have the same two final digits. Thus our list (which contains 22 numbers) is complete.

30. If $|y| \ge 2$, then $2x^2 + 5y^2 \ge 2x^2 + 20 \ge 20$, so the only possible values of y to try are 0 and ± 1. In the former case we would be looking for solutions to $2x^2 = 14$ and in the latter case to $2x^2 = 9$. Clearly there are no integer solutions to these equations, so there are no solutions to the original equation.

32. Following the hint, we let $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$. Then $x^2 + y^2 = (m^2-n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2+n^2)^2 = z^2$. Thus we have found infinitely many solutions, since m and n can be arbitrarily large.

34. One proof that $\sqrt[3]{2}$ is irrational is similar to the proof that $\sqrt{2}$ is irrational, given in Example 10 in Section 1.7. It is a proof by contradiction. Suppose that $2^{1/3}$ (or $\sqrt[3]{2}$, which is the same thing) is the rational number p/q, where p and q are positive integers with no common factors (the fraction is in lowest terms). Cubing, we see that $2 = p^3/q^3$, or, equivalently, $p^3 = 2q^3$. Thus p^3 is even. Since the product of odd numbers is odd, this means that p is even, so we can write $p = 2s$. Substituting into the equation $p^3 = 2q^3$, we obtain $8s^3 = 2q^3$, which simplifies to $4s^3 = q^3$.

Now we play the same game with q. Since q^3 is even, q must be even. We have now concluded that p and q are both even, that is, that 2 is a common divisor of p and q. This contradicts the choice of p/q to be in lowest terms. Therefore our original assumption—that $\sqrt[3]{2}$ is rational—is in error, so we have proved that $\sqrt[3]{2}$ is irrational.

36. The average of two different numbers is certainly always between the two numbers. Furthermore, the average a of rational number x and irrational number y must be irrational, because the equation $a = (x+y)/2$ leads to $y = 2a - x$, which would be rational if a were rational.

38. The solution is not unique, but here is one way to measure out four gallons. Fill the 5-gallon jug from the 8-gallon jug, leaving the contents $(3, 5, 0)$, where we are using the ordered triple to record the amount of water in the 8-gallon jug, the 5-gallon jug, and the 3-gallon jug, respectively. Next fill the 3-gallon jug from the 5-gallon jug, leaving $(3, 2, 3)$. Pour the contents of the 3-gallon jug back into the 8-gallon jug, leaving $(6, 2, 0)$. Empty the 5-gallon jug's contents into the 3-gallon jug, leaving $(6, 0, 2)$, and then fill the 5-gallon jug from the 8-gallon jug, producing $(1, 5, 2)$. Finally, top off the 3-gallon jug from the 5-gallon jug, and we'll have $(1, 4, 3)$, with four gallons in the 5-gallon jug.

40. **a)** $16 \to 8 \to 4 \to 2 \to 1$

b) $11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$

c) $35 \to 106 \to 53 \to 160 \to 80 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$

d) $113 \to 340 \to 170 \to 85 \to 256 \to 128 \to 64 \to 32 \to 16 \to 8 \to 4 \to 2 \to 1$

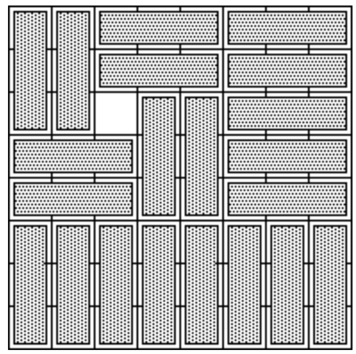
42. This is easily done, by laying the dominoes horizontally, three in the first and last rows and four in each of the other six rows.

44. Without loss of generality, we number the squares from 1 to 25, starting in the top row and proceeding left to right in each row; and we assume that squares 5 (upper right corner), 21 (lower left corner), and 25 (lower right corner) are the missing ones. We argue that there is no way to cover the remaining squares with dominoes.

By symmetry we can assume that there is a domino placed in 1-2 (using the obvious notation). If square 3 is covered by 3-8, then the following dominoes are forced in turn: 4-9, 10-15, 19-20, 23-24, 17-22, and 13-18, and now no domino can cover square 14. Therefore we must use 3-4 along with 1-2. If we use all of 17-22, 18-23, and 19-24, then we are again quickly forced into a sequence of placements that lead to a contradiction. Therefore without loss of generality, we can assume that we use 22-23, which then forces 19-24, 15-20, 9-10, 13-14, 7-8, 6-11, and 12-17, and we are stuck once again. This completes the proof by contradiction that no placement is possible.

46. The barriers shown in the diagram split the board into one continuous closed path of 64 squares, each adjacent to the next (for example, start at the upper left corner, go all the way to the right, then all the way down, then all the way to the left, and then weave your way back up to the starting point). Because each square in the path is adjacent to its neighbors, the colors alternate. Therefore, if we remove one black square and one white square, this closed path decomposes into two paths, each of which starts in one color and ends in the other color (and therefore has even length). Clearly each such path can be covered by dominoes by starting at one end. This completes the proof.

48. If we study Figure 7, we see that by rotating or reflecting the board, we can make any square we wish nonwhite, with the exception of the squares with coordinates $(3, 3)$, $(3, 6)$, $(6, 3)$, and $(6, 6)$. Therefore the same argument as was used in Example 22 shows that we cannot tile the board using straight triominoes if any one of those other 60 squares is removed. The following drawing (rotated as necessary) shows that we can tile the board using straight triominoes if one of those four squares is removed.



50. We will use a coloring of the 10×10 board with four colors as the basis for a proof by contradiction showing that no such tiling exists. Assume that 25 straight tetrominoes can cover the board. Some will be placed horizontally and some vertically. Because there is an odd number of tiles, the number placed horizontally and the number placed vertically cannot both be odd, so assume without loss of generality that an even number of tiles are placed horizontally. Color the squares in order using the colors red, blue, green, yellow in that order repeatedly, starting in the upper left corner and proceeding row by row, from left to right in each row. Then it is clear that every horizontally placed tile covers one square of each color and each vertically placed tile covers either zero or two squares of each color. It follows that in this tiling an even number of squares of each color are covered. But this contradicts the fact that there are 25 squares of each color. Therefore no such coloring exists.

SUPPLEMENTARY EXERCISES FOR CHAPTER 1

2. The truth table is as follows.

p	q	r	$p \vee q$	$p \wedge \neg r$	$(p \vee q) \to (p \wedge \neg r)$
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	F	F
F	F	T	F	F	T
F	F	F	F	F	T

4. **a)** The converse is "If I drive to work today, then it will rain." The contrapositive is "If I do not drive to work today, then it will not rain." The inverse is "If it does not rain today, then I will not drive to work."

b) The converse is "If $x \geq 0$ then $|x| = x$." The contrapositive is "If $x < 0$ then $|x| \neq x$." The inverse is "If $|x| \neq x$, then $x < 0$."

c) The converse is "If n^2 is greater than 9, then n is greater than 3." The contrapositive is "If n^2 is not greater than 9, then n is not greater than 3." The inverse is "If n is not greater than 3, then n^2 is not greater than 9."

6. The inverse of $p \to q$ is $\neg p \to \neg q$. Therefore the inverse of the inverse is $\neg\neg p \to \neg\neg q$, which is equivalent to $p \to q$ (the original proposition). The converse of $p \to q$ is $q \to p$. Therefore the inverse of the converse is $\neg q \to \neg p$, which is the contrapositive of the original proposition. The inverse of the contrapositive is $q \to p$, which is the same as the converse of the original statement.

8. Let t be "Sergei takes the job offer"; let b be "Sergei gets a signing bonus"; and let h be "Sergei will receive a higher salary." The given statements are $t \to b$, $t \to h$, $b \to \neg h$, and t. By modus ponens we can conclude b and h from the first two conditional statements, and therefore we can conclude $\neg h$ from the third conditional statement. We now have the contradiction $h \wedge \neg h$, so these statements are inconsistent.

10. We make a table of the eight possibilities for p, q, and r, showing the truth values of the three propositions.

p	q	r	$p \to q$	$\neg(p \vee r) \vee q$	q
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	F	F	T
T	F	F	F	F	T
F	T	T	T	T	F
F	T	F	T	T	F
F	F	T	T	F	F
F	F	F	T	T	F

If we look at the first row of the table, we see that if the student accepts all three propositions, then the resulting commitments are consistent, because the propositions are all true in this case in which p, q, and r are all true. Similarly, looking at the sixth row of the table, where p and r are false but q is true, we see that a student who accepts the first two propositions and rejects the third also wins. Scanning the entire table, we see that the winning answers are accept-accept-accept, reject-reject-accept, accept-accept-reject, and accept-reject-reject.

12. As we saw from the examples in the previous exercises, one winning strategy is just to assume that all the variables are true and answer "accept" or "reject" according to whether the given proposition is true or false.

14. A knight would never claim that she is a knave, so we know that Anita is a knave. Because she is lying and the first part of her conjunction is true, it must be the second part that is false, and so Bohan must be a knave. If Carmen were a knight, then Bohan's statement would be true; because Bohan is a knave, we know that that cannot be, so we conclude that Carmen is also a knave.

16. If S is a proposition, then it is either true or false. If S is false, then the statement "If S is true, then unicorns live" is vacuously true; but this statement *is* S, so we would have a contradiction. Therefore S is true, so the statement "If S is true, then unicorns live" is true and has a true hypothesis. Hence it has a true conclusion (modus ponens), and so unicorns live. But we know that unicorns do not live. It follows that S cannot be a proposition.

18. From the given information we know that p_1, p_3, p_5, ... are true and p_2, p_4, p_6, ... are false. Therefore $p_i \wedge p_{i+1}$ is always false, and so the disjunction $\bigvee_{i=1}^{100}(p_i \wedge p_{i+1})$ is also false. On the other hand, $p_i \vee p_{i+1}$ is always true, and so the conjunction $\bigwedge_{i=1}^{100}(p_i \vee p_{i+1})$ is also true.

20. **a)** The answer is $\exists x P(x)$ if we do not read any significance into the use of the plural, and $\exists x \exists y (P(x) \wedge P(y) \wedge x \neq y)$ if we do.
b) $\neg \forall x P(x)$, or, equivalently, $\exists x \neg P(x)$ **c)** $\forall y Q(y)$
d) $\forall x P(x)$ (the class has nothing to do with it) **e)** $\exists y \neg Q(y)$

22. The given statement tells us that there are exactly two elements in the domain. Therefore the statement will be true as long as we choose the domain to be anything with size 2, such as the United States presidents named Bush.

24. We want to say that for every y, there do not exist four different people each of whom is the grandmother of y. Thus we have $\forall x \neg\exists a \exists b \exists c \exists d(a \neq b \wedge a \neq c \wedge a \neq d \wedge b \neq c \wedge b \neq d \wedge c \neq d \wedge G(a,y) \wedge G(b,y) \wedge G(c,y) \wedge G(d,y))$.

26. **a)** Since there is no real number whose square is -1, it is true that there exist exactly 0 values of x such that $x^2 = -1$.

b) This is true, because 0 is the one and only value of x such that $|x| = 0$.

c) This is true, because $\sqrt{2}$ and $-\sqrt{2}$ are the only values of x such that $x^2 = 2$.

d) This is false, because there are more than three values of x such that $x = |x|$, namely all positive real numbers.

28. Let us assume the hypothesis. This means that there is some x_0 such that $P(x_0, y)$ holds for all y. Then it is certainly true that for all y there exists an x such that $P(x,y)$ is true, since in each case we can take $x = x_0$. Note that the converse is not always a tautology, since the x in $\forall y \exists x P(x,y)$ can depend on y.

30. No. Here is an example. Let $P(x,y)$ be $x > y$, where we are talking about integers. Then for every y there does exist an x such that $x > y$; we could take $x = y + 1$, for example. However, there does not exist an x such that for *every* y, $x > y$; in other words, there is no superlarge integer (if for no other reason than that no integer can be larger than itself).

32. **a)** It will snow today, but I will not go skiing tomorrow.

b) Some person in this class does not understand mathematical induction.

c) All students in this class like discrete mathematics.

d) There is some mathematics class in which all the students stay awake during lectures.

34. Let $W(r)$ means that room r is painted white. Let $I(r,b)$ mean that room r is in building b. Let $L(b,u)$ mean that building b is on the campus of United States university u. Then the statement is that there is some university u and some building on the campus of u such that every room in b is painted white. In symbols this is $\exists u \exists b(L(b,u) \wedge \forall r(I(r,b) \rightarrow W(r)))$.

36. To say that there are exactly two elements that make the statement true is to say that two elements exist that make the statement true, and that every element that makes the statement true is one of these two elements. More compactly, we can phrase the last part by saying that an element makes the statement true if and only if it is one of these two elements. In symbols this is $\exists x \exists y(x \neq y \wedge \forall z(P(z) \leftrightarrow (z = x \vee z = y)))$. In English we might express the rule as follows. The hypotheses are that $P(x)$ and $P(y)$ are both true, that $x \neq y$, and that every z that satisfies $P(z)$ must be either x or y. The conclusion is that there are exactly two elements that make P true.

38. We give a proof by contraposition. If x is rational, then $x = p/q$ for some integers p and q with $q \neq 0$. Then $x^3 = p^3/q^3$, and we have expressed x^3 as the quotient of two integers, the second of which is not zero. This by definition means that x^3 is rational, and that completes the proof of the contrapositive of the original statement.

40. Let m be the square root of n, rounded down if it is not a whole number. (In the notation to be introduced in Section 2.3, we are letting $m = \lfloor\sqrt{n}\rfloor$.) We can see that this is the unique solution in a couple of ways. First, clearly the different choices of m correspond to a partition of $\mathbf{N}$, namely into $\{0\}$, $\{1,2,3\}$, $\{4,5,6,7,8\}$, $\{9,10,11,12,13,14,15\}$, $\ldots$. So every n is in exactly one of these sets. Alternatively, take the square root of the given inequalities to give $m \leq \sqrt{n} < m+1$. That m is then the floor of $\sqrt{n}$ (and that m is unique) follows from statement (1a) of Table 1 in Section 2.3.

42. A constructive proof seems indicated. We can look for examples by hand or with a computer program. The smallest ones to be found are $50 = 5^2 + 5^2 = 1^2 + 7^2$ and $65 = 4^2 + 7^2 = 1^2 + 8^2$.

44. We claim that the number 7 is not the sum of at most two squares and a cube. The first two positive squares are 1 and 4, and the first positive cube is 1, and these are the only numbers that could be used in forming the sum. Clearly no sum of three or fewer of these is 7. This counterexample disproves the statement.

46. We give a proof by contradiction. If $\sqrt{2} + \sqrt{3}$ were rational, then so would be its square, which is $5 + 2\sqrt{6}$. Subtracting 5 and dividing by 2 then shows that $\sqrt{6}$ is rational, but this contradicts the theorem we are told to assume.

CHAPTER 2
Basic Structures: Sets, Functions, Sequences, Sums, and Matrices

SECTION 2.1 Sets

2. There are of course an infinite number of correct answers.

a) $\{\,3n \mid n = 0,1,2,3,4\,\}$ or $\{\,x \mid x$ is a multiple of $3 \wedge 0 \le x \le 12\,\}$.

b) $\{\,x \mid -3 \le x \le 3\,\}$, where we are assuming that the domain (universe of discourse) is the set of integers.

c) $\{x \mid x$ is a letter of the word *monopoly* other than l or $y\,\}$.

4. Recall that one set is a subset of another set if every element of the first set is also an element of the second.

a) The second condition imposes an extra requirement, so clearly the second set is a subset of the first, but not vice versa.

b) Again the second condition imposes an extra requirement, so the second set is a subset of the first, but not vice versa.

c) There could well be students studying discrete mathematics but not data structures (for example, pure math majors) and students studying data structure but not discrete mathematics (at least not this semester—one could argue that the knowing the latter is necessary to really understand the former!), so neither set is a subset of the other.

6. Each of the sets is a subset of itself. Aside from that, the only relations are $B \subseteq A$, $C \subseteq A$, and $C \subseteq D$.

8. a) Since the set contains only integers and $\{2\}$ is a set, not an integer, $\{2\}$ is not an element.

b) Since the set contains only integers and $\{2\}$ is a set, not an integer, $\{2\}$ is not an element.

c) The set has two elements. One of them is patently $\{2\}$.

d) The set has two elements. One of them is patently $\{2\}$.

e) The set has two elements. One of them is patently $\{2\}$.

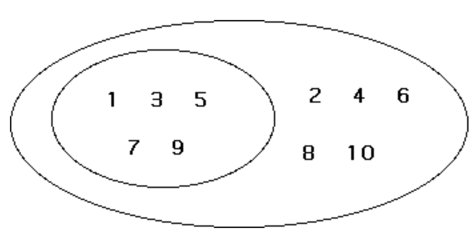
f) The set has only one element, $\{\{2\}\}$; since this is not the same as $\{2\}$ (the former is a set containing a set, whereas the latter is a set containing a number), $\{2\}$ is not an element of $\{\{\{2\}\}\}$.

10. a) true **b)** true **c)** false—see part **(a)** **d)** true

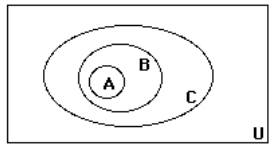
e) true—the one element in the set on the left is an element of the set on the right, and the sets are not equal

f) true—similar to part **(e)** **g)** false—the two sets are equal

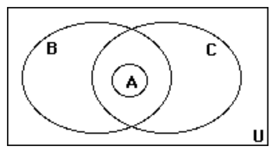
12. The numbers 1, 3, 5, 7, and 9 form a subset of the set of all ten positive integers under discussion, as shown here.



14. We put the subsets inside the supersets. Thus the answer is as shown.



16. We allow B and C to overlap, because we are told nothing about their relationship. The set A must be a subset of each of them, and that forces it to be positioned as shown. We cannot actually show the properness of the subset relationships in the diagram, because we don't know where the elements in B and C that are not in A are located—there might be only one (which is in both B and C), or they might be located in portions of B and/or C outside the other. Thus the answer is as shown, but with the added condition that there must be at least one element of B not in A and one element of C not in A.



18. Since the empty set is a subset of every set, we just need to take a set B that contains $\emptyset$ as an element. Thus we can let $A = \emptyset$ and $B = \{\emptyset\}$ as the simplest example.

20. The cardinality of a set is the number of elements it has.

a) The empty set has no elements, so its cardinality is 0.

b) This set has one element (the empty set), so its cardinality is 1.

c) This set has two elements, so its cardinality is 2.

d) This set has three elements, so its cardinality is 3.

22. The union of all the sets in the power set of a set X must be exactly X. In other words, we can recover X from its power set, uniquely. Therefore the answer is yes.

24. **a)** The power set of every set includes at least the empty set, so the power set cannot be empty. Thus $\emptyset$ is not the power set of any set.

b) This is the power set of $\{a\}$.

c) This set has three elements. Since 3 is not a power of 2, this set cannot be the power set of any set.

d) This is the power set of $\{a, b\}$.

26. We need to show that every element of $A \times B$ is also an element of $C \times D$. By definition, a typical element of $A \times B$ is a pair (a, b) where $a \in A$ and $b \in B$. Because $A \subseteq C$, we know that $a \in C$; similarly, $b \in D$. Therefore $(a, b) \in C \times D$.

28. By definition it is the set of all ordered pairs (c, p) such that c is a course and p is a professor. The elements of this set are the possible teaching assignments for the mathematics department.

30. We can conclude that $A = \emptyset$ or $B = \emptyset$. To prove this, suppose that neither A nor B were empty. Then there would be elements $a \in A$ and $b \in B$. This would give at last one element, namely (a, b), in $A \times B$, so $A \times B$ would not be the empty set. This contradiction shows that either A or B (or both, it goes without saying) is empty.

32. In each case the answer is a set of 3-tuples.

a) $\{(a,x,0),(a,x,1),(a,y,0),(a,y,1),(b,x,0),(b,x,1),(b,y,0),(b,y,1),(c,x,0),(c,x,1),(c,y,0),(c,y,1)\}$

b) $\{(0,x,a),(0,x,b),(0,x,c),(0,y,a),(0,y,b),(0,y,c),(1,x,a),(1,x,b),(1,x,c),(1,y,a),(1,y,b),(1,y,c)\}$

c) $\{(0,a,x),(0,a,y),(0,b,x),(0,b,y),(0,c,x),(0,c,y),(1,a,x),(1,a,y),(1,b,x),(1,b,y),(1,c,x),(1,c,y)\}$

d) $\{(x,x,x),(x,x,y),(x,y,x),(x,y,y),(y,x,x),(y,x,y),(y,y,x),(y,y,y)\}$

34. Recall that A^3 consists of all the ordered triples (x,y,z) of elements of A.

a) $\{(a,a,a)\}$ **b)** $\{(0,0,0),(0,0,a),(0,a,0),(0,a,a),(a,0,0),(a,0,a),(a,a,0),(a,a,a)\}$

36. The set $A\times B\times C$ consists of ordered triples (a,b,c) with $a\in A$, $b\in B$, and $c\in C$. There are m choices for the first coordinate. For each of these, there n choices for the second coordinate, giving us mn choices for the first two coordinates. For each of these, there p choices for the third coordinate, giving us mnp choices in all. Therefore $A\times B\times C$ has mnp elements. This is an application of the product rule (see Chapter 6).

38. Suppose $A\neq B$ and neither A nor B is empty. We must prove that $A\times B\neq B\times A$. Since $A\neq B$, either we can find an element x that is in A but not B, or vice versa. The two cases are similar, so without loss of generality, let us assume that x is in A but not B. Also, since B is not empty, there is some element $y\in B$. Then (x,y) is in $A\times B$ by definition, but it is not in $B\times A$ since $x\notin B$. Therefore $A\times B\neq B\times A$.

40. The only difference between $(A\times B)\times(C\times D)$ and $A\times(B\times C)\times D$ is parentheses, so for all practical purposes one can think of them as essentially the same thing. By Definition 8, the elements of $(A\times B)\times(C\times D)$ consist of ordered pairs (x,y), where $x\in A\times B$ and $y\in C\times D$, so the typical element of $(A\times B)\times(C\times D)$ looks like $((a,b),(c,d))$. By Definition 9, the elements of $A\times(B\times C)\times D$ consist of 3-tuples (a,x,d), where $a\in A$, $d\in D$, and $x\in B\times C$, so the typical element of $A\times(B\times C)\times D$ looks like $(a,(b,c),d)$. The structures $((a,b),(c,d))$ and $(a,(b,c),d)$ are different, even if they convey exactly the same information (the first is a pair, and the second is a 3-tuple). To be more precise, there is a natural one-to-one correspondence between $(A\times B)\times(C\times D)$ and $A\times(B\times C)\times D$ given by $((a,b),(c,d))\leftrightarrow(a,(b,c),d)$.

42. a) There is a real number whose cube is -1. This is true, since $x=-1$ is a solution.

b) There is an integer such that the number obtained by adding 1 to it is greater than the integer. This is true—in fact, every integer satisfies this statement.

c) For every integer, the number obtained by subtracting 1 is again an integer. This is true.

d) The square of every integer is an integer. This is true.

44. In each case we want the set of all values of x in the domain (the set of integers) that satisfy the given equation or inequality.

a) It is exactly the positive integers that satisfy this inequality. Therefore the truth set is $\{x\in\mathbf{Z}\mid x^3\geq 1\}=\{x\in\mathbf{Z}\mid x\geq 1\}=\{1,2,3,\ldots\}$.

b) The square roots of 2 are not integers, so the truth set is the empty set, $\emptyset$.

c) Negative integers certainly satisfy this inequality, as do all positive integers greater than 1. However, $0\not<0^2$ and $1\not<1^2$. Thus the truth set is $\{x\in\mathbf{Z}\mid x<x^2\}=\{x\in\mathbf{Z}\mid x\neq 0\wedge x\neq 1\}=\{\ldots,-3,-2,-1,2,3,\ldots\}$.

46. a) If $S\in S$, then by the defining condition for S we conclude that $S\notin S$, a contradiction.

b) If $S\notin S$, then by the defining condition for S we conclude that it is not the case that $S\notin S$ (otherwise S would be an element of S), again a contradiction.

SECTION 2.2 Set Operations

2. **a)** $A \cap B$ **b)** $A \cap \overline{B}$, which is the same as $A - B$ **c)** $A \cup B$ **d)** $\overline{A} \cup \overline{B}$

4. Note that $A \subseteq B$.
a) $\{a, b, c, d, e, f, g, h\} = B$ **b)** $\{a, b, c, d, e\} = A$
c) There are no elements in A that are not in B, so the answer is $\emptyset$. **d)** $\{f, g, h\}$

6. **a)** $A \cup \emptyset = \{\, x \mid x \in A \vee x \in \emptyset \,\} = \{\, x \mid x \in A \vee \mathbf{F} \,\} = \{\, x \mid x \in A \,\} = A$
b) $A \cap U = \{\, x \mid x \in A \wedge x \in U \,\} = \{\, x \mid x \in A \wedge \mathbf{T} \,\} = \{\, x \mid x \in A \,\} = A$

8. **a)** $A \cup A = \{\, x \mid x \in A \vee x \in A \,\} = \{\, x \mid x \in A \,\} = A$
b) $A \cap A = \{\, x \mid x \in A \wedge x \in A \,\} = \{\, x \mid x \in A \,\} = A$

10. **a)** $A - \emptyset = \{\, x \mid x \in A \wedge x \notin \emptyset \,\} = \{\, x \mid x \in A \wedge \mathbf{T} \,\} = \{\, x \mid x \in A \,\} = A$
b) $\emptyset - A = \{\, x \mid x \in \emptyset \wedge x \notin A \,\} = \{\, x \mid \mathbf{F} \wedge x \notin A \,\} = \{\, x \mid \mathbf{F} \,\} = \emptyset$

12. We will show that these two sets are equal by showing that each is a subset of the other. Suppose $x \in A \cup (A \cap B)$. Then $x \in A$ or $x \in A \cap B$ by the definition of union. In the former case, we have $x \in A$, and in the latter case we have $x \in A$ and $x \in B$ by the definition of intersection; thus in any event, $x \in A$, so we have proved that the left-hand side is a subset of the right-hand side. Conversely, let $x \in A$. Then by the definition of union, $x \in A \cup (A \cap B)$ as well. Thus we have shown that the right-hand side is a subset of the left-hand side.

14. Since $A = (A - B) \cup (A \cap B)$, we conclude that $A = \{1, 5, 7, 8\} \cup \{3, 6, 9\} = \{1, 3, 5, 6, 7, 8, 9\}$. Similarly $B = (B - A) \cup (A \cap B) = \{2, 10\} \cup \{3, 6, 9\} = \{2, 3, 6, 9, 10\}$.

16. **a)** If x is in $A \cap B$, then perforce it is in A (by definition of intersection).
b) If x is in A, then perforce it is in $A \cup B$ (by definition of union).
c) If x is in $A - B$, then perforce it is in A (by definition of difference).
d) If $x \in A$ then $x \notin B - A$. Therefore there can be no elements in $A \cap (B - A)$, so $A \cap (B - A) = \emptyset$.
e) The left-hand side consists precisely of those things that are either elements of A or else elements of B but not A, in other words, things that are elements of either A or B (or, of course, both). This is precisely the definition of the right-hand side.

18. **a)** Suppose that $x \in A \cup B$. Then either $x \in A$ or $x \in B$. In either case, certainly $x \in A \cup B \cup C$. This establishes the desired inclusion.
b) Suppose that $x \in A \cap B \cap C$. Then x is in all three of these sets. In particular, it is in both A and B and therefore in $A \cap B$, as desired.
c) Suppose that $x \in (A - B) - C$. Then x is in $A - B$ but not in C. Since $x \in A - B$, we know that $x \in A$ (we also know that $x \notin B$, but that won't be used here). Since we have established that $x \in A$ but $x \notin C$, we have proved that $x \in A - C$.
d) To show that the set given on the left-hand side is empty, it suffices to assume that x is some element in that set and derive a contradiction, thereby showing that no such x exists. So suppose that $x \in (A - C) \cap (C - B)$. Then $x \in A - C$ and $x \in C - B$. The first of these statements implies by definition that $x \notin C$, while the second implies that $x \in C$. This is impossible, so our proof by contradiction is complete.
e) To establish the equality, we need to prove inclusion in both directions. To prove that $(B - A) \cup (C - A) \subseteq (B \cup C) - A$, suppose that $x \in (B - A) \cup (C - A)$. Then either $x \in (B - A)$ or $x \in (C - A)$. Without loss of

generality, assume the former (the proof in the latter case is exactly parallel.) Then $x \in B$ and $x \notin A$. From the first of these assertions, it follows that $x \in B \cup C$. Thus we can conclude that $x \in (B \cup C) - A$, as desired. For the converse, that is, to show that $(B \cup C) - A \subseteq (B - A) \cup (C - A)$, suppose that $x \in (B \cup C) - A$. This means that $x \in (B \cup C)$ and $x \notin A$. The first of these assertions tells us that either $x \in B$ or $x \in C$. Thus either $x \in B - A$ or $x \in C - A$. In either case, $x \in (B - A) \cup (C - A)$. (An alternative proof could be given by using Venn diagrams, showing that both sides represent the same region.)

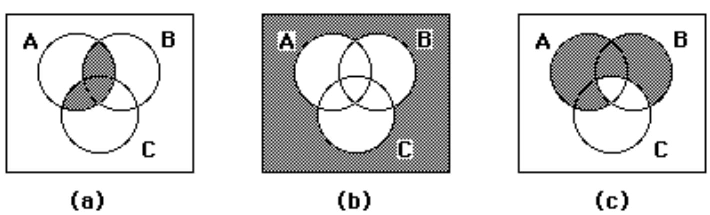
20. **a)** It is always the case that $B \subseteq A \cup B$, so it remains to show that $A \cup B \subseteq B$. But this is clear because if $x \in A \cup B$, then either $x \in A$, in which case $x \in B$ (because we are given $A \subseteq B$) or $x \in B$; in either case $x \in B$.

b) It is always the case that $A \cap B \subseteq A$, so it remains to show that $A \subseteq A \cap B$. But this is clear because if $x \in A$, then $x \in B$ as well (because we are given $A \subseteq B$), so $x \in A \cap B$.

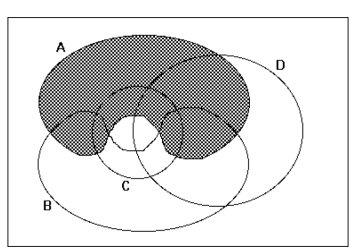
22. First we show that every element of the left-hand side must be in the right-hand side as well. If $x \in A \cap (B \cap C)$, then x must be in A and also in $B \cap C$. Hence x must be in A and also in B and in C. Since x is in both A and B, we conclude that $x \in A \cap B$. This, together with the fact that $x \in C$ tells us that $x \in (A \cap B) \cap C$, as desired. The argument in the other direction (if $x \in (A \cap B) \cap C$ then x must be in $A \cap (B \cap C)$) is nearly identical.

24. First suppose x is in the left-hand side. Then x must be in A but in neither B nor C. Thus $x \in A - C$, but $x \notin B - C$, so x is in the right-hand side. Next suppose that x is in the right-hand side. Thus x must be in $A - C$ and not in $B - C$. The first of these implies that $x \in A$ and $x \notin C$. But now it must also be the case that $x \notin B$, since otherwise we would have $x \in B - C$. Thus we have shown that x is in A but in neither B nor C, which implies that x is in the left-hand side.

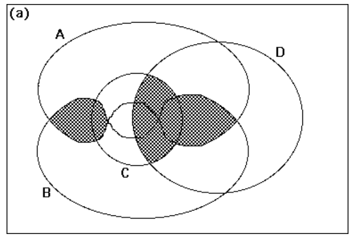
26. The set is shaded in each case.

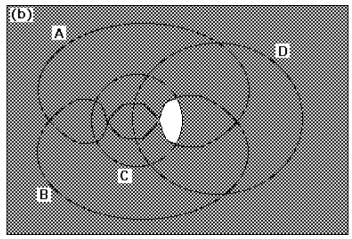


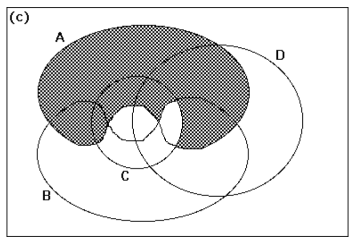
28. Here is a Venn diagram that can be used for four sets. Notice that sets A and B are not convex in this picture. We have shaded set A. Notice that each of the 16 different combinations are represented by a region.



We can now shade in the appropriate regions for each of the expressions in this exercise.







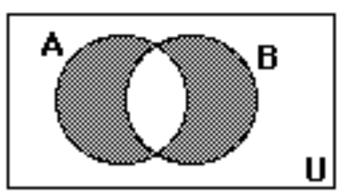
30. **a)** We cannot conclude that $A = B$. For instance, if A and B are both subsets of C, then this equation will always hold, and A need not equal B.

b) We cannot conclude that $A = B$; let $C = \emptyset$, for example.

c) By putting the two conditions together, we *can* now conclude that $A = B$. By symmetry, it suffices to prove that $A \subseteq B$. Suppose that $x \in A$. There are two cases. If $x \in C$, then $x \in A \cap C = B \cap C$, which forces $x \in B$. On the other hand, if $x \notin C$, then because $x \in A \cup C = B \cup C$, we must have $x \in B$.

32. This is the set of elements in exactly one of these sets, namely $\{2, 5\}$.

34. The figure is as shown; we shade that portion of A that is not in B and that portion of B that is not in A.



36. There are precisely two ways that an item can be in either A or B but not both. It can be in A but not B (which is equivalent to saying that it is in $A - B$), or it can be in B but not A (which is equivalent to saying that it is in $B - A$). Thus an element is in $A \oplus B$ if and only if it is in $(A - B) \cup (B - A)$.

38. **a)** This is clear from the symmetry (between A and B) in the definition of symmetric difference.

b) We prove two things. To show that $A \subseteq (A \oplus B) \oplus B$, suppose $x \in A$. If $x \in B$, then $x \notin A \oplus B$, so x is an element of the right-hand side. On the other hand if $x \notin B$, then $x \in A \oplus B$, so again x is in the right-hand side. Conversely, suppose x is an element of the right-hand side. There are two cases. If $x \notin B$, then necessarily $x \in A \oplus B$, whence $x \in A$. If $x \in B$, then necessarily $x \notin A \oplus B$, and the only way for that to happen (since $x \in B$) is for x to be in A.

40. This is an identity; each side consists of those things that are in an odd number of the sets A, B, and C.

42. This is an identity; each side consists of those things that are in an odd number of the sets A, B, C, and D.

44. A finite set is a set with k elements for some natural number k. Suppose that A has n elements and B has m elements. Then the number of elements in $A \cup B$ is at most $n+m$ (it might be less because $A \cap B$ might be nonempty). Therefore by definition, $A \cup B$ is finite.

46. To count the elements of $A \cup B \cup C$ we proceed as follows. First we count the elements in each of the sets and add. This certainly gives us all the elements in the union, but we have overcounted. Each element in $A \cap B$, $A \cap C$, and $B \cap C$ has been counted twice. Therefore we subtract the cardinalities of these intersections to make up for the overcount. Finally, we have compensated a bit too much, since the elements of $A \cap B \cap C$ have now been counted three times and subtracted three times. We adjust by adding back the cardinality of $A \cap B \cap C$.

48. We note that these sets are increasing, that is, $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$. Therefore, the union of any collection of these sets is just the one with the largest subscript, and the intersection is just the one with the smallest subscript.

a) $A_n = \{\ldots, -2, -1, 0, 1, \ldots, n\}$ **b)** $A_1 = \{\ldots, -2, -1, 0, 1\}$

50. **a)** As i increases, the sets get smaller: $\cdots \subset A_3 \subset A_2 \subset A_1$. All the sets are subsets of A_1, which is the set of positive integers, $\mathbf{Z}^+$. It follows that $\bigcup_{i=1}^{\infty} A_i = \mathbf{Z}^+$. Every positive integer is excluded from at least one of the sets (in fact from infinitely many), so $\bigcap_{i=1}^{\infty} A_i = \emptyset$.

b) All the sets are subsets of the set of natural numbers $\mathbf{N}$ (the nonnegative integers). The number 0 is in each of the sets, and every positive integer is in exactly one of the sets, so $\bigcup_{i=1}^{\infty} A_i = \mathbf{N}$ and $\bigcap_{i=1}^{\infty} A_i = \{0\}$.

c) As i increases, the sets get larger: $A_1 \subset A_2 \subset A_3 \cdots$. All the sets are subsets of the set of positive real numbers $\mathbf{R}^+$, and every positive real number is included eventually, so $\bigcup_{i=1}^{\infty} A_i = \mathbf{R}^+$. Because A_1 is a subset of each of the others, $\bigcap_{i=1}^{\infty} A_i = A_1 = (0,1)$ (the interval of all real numbers between 0 and 1, exclusive).

d) This time, as in part **(a)**, the sets are getting smaller as i increases: $\cdots \subset A_3 \subset A_2 \subset A_1$. Because A_1 includes all the others, $\bigcup_{i=1}^{\infty} A_1 = (1, \infty)$ (all real numbers greater than 1). Every number eventually gets excluded as i increases, so $\bigcap_{i=1}^{\infty} A_i = \emptyset$. Notice that ∞ is not a real number, so we cannot write $\bigcap_{i=1}^{\infty} A_i = \{\infty\}$.

52. **a)** 00 1110 0000 **b)** 10 1001 0001 **c)** 01 1100 1110

54. **a)** No elements are included, so this is the empty set.

b) All elements are included, so this is the universal set.

56. The bit string for the symmetric difference is obtained by taking the bitwise exclusive *OR* of the two bit strings for the two sets, since we want to include those elements that are in one set or the other but not both.

58. We can take the bitwise *OR* (for union) or *AND* (for intersection) of all the bit strings for these sets.

60. The successor set has one more element than the original set, namely the original set itself. Therefore the answer is $n+1$.

62. **a)** If the departments share the equipment, then the maximum number of each type is all that is required, so we want to take the union of the multisets, $A \cup B$.

b) Both departments will use the minimum number of each type, so we want to take the intersection of the multisets, $A \cap B$.

c) This will be the difference $B - A$ of the multisets.

d) If no sharing is allowed, then the university needs to purchase a quantity of each type of equipment that is the sum of the quantities used by the departments; this is the sum of the multisets, $A + B$.

64. Taking the maximum for each person, we have $S \cup T = \{0.6 \text{ Alice}, 0.9 \text{ Brian}, 0.4 \text{ Fred}, 0.9 \text{ Oscar}, 0.7 \text{ Rita}\}$.

SECTION 2.3 Functions

2. **a)** This is not a function because the rule is not well-defined. We do not know whether $f(3) = 3$ or $f(3) = -3$. For a function, it cannot be both at the same time.

b) This is a function. For all integers n, $\sqrt{n^2+1}$ is a well-defined real number.

c) This is not a function with domain $\mathbf{Z}$, since for $n = 2$ (and also for $n = -2$) the value of $f(n)$ is not defined by the given rule. In other words, $f(2)$ and $f(-2)$ are not specified since division by 0 makes no sense.

4. **a)** The domain is the set of nonnegative integers, and the range is the set of digits (0 through 9).

b) The domain is the set of positive integers, and the range is the set of integers greater than 1.

c) The domain is the set of all bit strings, and the range is the set of nonnegative integers.

d) The domain is the set of all bit strings, and the range is the set of nonnegative integers (a bit string can have length 0).

6. **a)** The domain is $\mathbf{Z}^+ \times \mathbf{Z}^+$ and the range is $\mathbf{Z}^+$.

b) Since the largest decimal digit of a strictly positive integer cannot be 0, we have domain $\mathbf{Z}^+$ and range $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

c) The domain is the set of all bit strings. The number of 1's minus number of 0's can be any positive or negative integer or 0, so the range is $\mathbf{Z}$.

d) The domain is given as $\mathbf{Z}^+$. Clearly the range is $\mathbf{Z}^+$ as well.

e) The domain is the set of bit strings. The range is the set of strings of 1's, i.e., $\{\lambda, 1, 11, 111, \ldots\}$, where λ is the empty string (containing no symbols).

8. We simply round up or down in each case.

a) 1 **b)** 2 **c)** -1 **d)** 0 **e)** 3 **f)** -2 **g)** $\lfloor \frac{1}{2} + 1 \rfloor = \lfloor \frac{3}{2} \rfloor = 1$

h) $\lceil 0 + 1 + \frac{1}{2} \rceil = \lceil \frac{3}{2} \rceil = 2$

10. **a)** This is one-to-one. **b)** This is not one-to-one, since b is the image of both a and b.

c) This is not one-to-one, since d is the image of both a and d.

12. **a)** This is one-to-one, since if $n_1 - 1 = n_2 - 1$, then $n_1 = n_2$.

b) This is not one-to-one, since, for example, $f(3) = f(-3) = 10$.

c) This is one-to-one, since if $n_1^3 = n_2^3$, then $n_1 = n_2$ (take the cube root of each side).

d) This is not one-to-one, since, for example, $f(3) = f(4) = 2$.

14. **a)** This is clearly onto, since $f(0,-n)=n$ for every integer n.

b) This is not onto, since, for example, 2 is not in the range. To see this, if $m^2-n^2=(m-n)(m+n)=2$, then m and n must have same parity (both even or both odd). In either case, both $m-n$ and $m+n$ are then even, so this expression is divisible by 4 and hence cannot equal 2.

c) This is clearly onto, since $f(0,n-1)=n$ for every integer n.

d) This is onto. To achieve negative values we set $m=0$, and to achieve nonnegative values we set $n=0$.

e) This is not onto, for the same reason as in part **(b)**. In fact, the range here is clearly a subset of the range in that part.

16. **a)** This would normally be one-to-one, unless somehow two students in the class had a strange mobile phone service in which they shared the same phone number.

b) This is surely one-to-one; otherwise the student identification number would not "identify" students very well!

c) This is almost surely not one-to-one; unless the class is very small, it is very likely that two students will receive the same grade.

d) This function will be one-to-one as long as no two students in the class hale from the same town (which is rather unlikely, so the function is probably not one-to-one).

18. Student answers may vary, depending on the choice of codomain.

a) A codomain could be all ten-digit positive integers; the function is not onto because there are many possible phone numbers assigned to people not in the class.

b) Under some student record systems, the student number consists of eight digits, so the codomain could be all natural numbers less than 100,000,000. The class does not have 100,000,000 students in it, so this function is not onto.

c) A codomain might be $\{\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D},\mathrm{F}\}$ (the answer depends on the grading system used at that school). If there were people at all five performance levels in this class, then the function would be onto. If not (for example, if no one failed the course), then it would not be onto.

d) The codomain could be the set of all cities and towns in the world. The function is clearly not onto. Alternatively, the codomain could be just the set of cities and towns from which the students in that class hale, in which case the function would be onto.

20. **a)** $f(n)=n+17$ **b)** $f(n)=\lceil n/2\rceil$

c) We let $f(n)=n-1$ for even values of n, and $f(n)=n+1$ for odd values of n. Thus we have $f(1)=2$, $f(2)=1$, $f(3)=4$, $f(4)=3$, and so on. Note that this is just one function, even though its definition used two formulae, depending on the the parity of n.

d) $f(n)=17$

22. If we can find an inverse, the function is a bijection. Otherwise we must explain why the function is not on-to-one or not onto.

a) This is a bijection since the inverse function is $f^{-1}(x)=(4-x)/3$.

b) This is not one-to-one since $f(17)=f(-17)$, for instance. It is also not onto, since the range is the interval $(-\infty,7]$. For example, 42548 is not in the range.

c) This function is a bijection, but not from $\mathbf{R}$ to $\mathbf{R}$. To see that the domain and range are not $\mathbf{R}$, note that $x=-2$ is not in the domain, and $x=1$ is not in the range. On the other hand, f is a bijection from $\mathbf{R}-\{-2\}$ to $\mathbf{R}-\{1\}$, since its inverse is $f^{-1}(x)=(1-2x)/(x-1)$.

d) It is clear that this continuous function is increasing throughout its entire domain ($\mathbf{R}$) and it takes on both arbitrarily large values and arbitrarily small (large negative) ones. So it is a bijection. Its inverse is clearly $f^{-1}(x)=\sqrt[5]{x-1}$.

24. The key here is that larger denominators make smaller fractions, and smaller denominators make larger fractions. We have two things to prove, since this is an "if and only if" statement. First, suppose that f is strictly increasing. This means that $f(x) < f(y)$ whenever $x < y$. To show that g is strictly decreasing, suppose that $x < y$. Then $g(x) = 1/f(x) > 1/f(y) = g(y)$. Conversely, suppose that g is strictly decreasing. This means that $g(x) > g(y)$ whenever $x < y$. To show that f is strictly increasing, suppose that $x < y$. Then $f(x) = 1/g(x) < 1/g(y) = f(y)$.

26. **a)** Let $f : \mathbf{R} \to \mathbf{R}$ be the given function. We are told that $f(x_1) < f(x_2)$ whenever $x_1 < x_2$. We need to show that $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$. This follows immediately from the given conditions, because without loss of generality, we may assume that $x_1 < x_2$.

b) We need to make the function increasing, but not *strictly* increasing, so, for example, we could take the trivial function $f(x) = 17$. If we want the range to be all of $\mathbf{R}$, we could define f in parts this way: $f(x) = x$ for $x < 0$; $f(x) = 0$ for $0 \leq x \leq 1$; and $f(x) = x - 1$ for $x > 1$.

28. For the function to be invertible, it must be a one-to-one correspondence. This means that it has to be one-to-one, which it is, and onto, which it is not, because, its range is the set of *positive* real numbers, rather than the set of *all* real numbers. When we restrict the codomain to be the set of positive real numbers, we get an invertible function. In fact, there is a well-known name for the inverse function in this case—the natural logarithm function ($g(x) = \ln x$).

30. In all parts, we simply need to compute the values $f(-1)$, $f(0)$, $f(2)$, $f(4)$, and $f(7)$ and collect the values into a set.

a) $\{1\}$ (all five values are the same) **b)** $\{-1, 1, 5, 8, 15\}$ **c)** $\{0, 1, 2\}$ **d)** $\{0, 1, 5, 16\}$

32. **a)** the set of even integers **b)** the set of positive even integers **c)** the set of real numbers

34. To clarify the setting, suppose that $g : A \to B$ and $f : B \to C$, so that $f \circ g : A \to C$. We will prove that if $f \circ g$ is one-to-one, then g is also one-to-one, so not only is the answer to the question "yes," but part of the hypothesis is not even needed. Suppose that g were not one-to-one. By definition this means that there are distinct elements a_1 and a_2 in A such that $g(a_1) = g(a_2)$. Then certainly $f(g(a_1)) = f(g(a_2))$, which is the same statement as $(f \circ g)(a_1) = (f \circ g)(a_2)$. By definition this means that $f \circ g$ is not one-to-one, and our proof is complete.

36. We have $(f \circ g)(x) = f(g(x)) = f(x + 2) = (x + 2)^2 + 1 = x^2 + 4x + 5$, whereas $(g \circ f)(x) = g(f(x)) = g(x^2 + 1) = x^2 + 1 + 2 = x^2 + 3$. Note that they are not equal.

38. Forming the compositions we have $(f \circ g)(x) = acx + ad + b$ and $(g \circ f)(x) = cax + cb + d$. These are equal if and only if $ad + b = cb + d$. In other words, equality holds for all 4-tuples (a, b, c, d) for which $ad + b = cb + d$.

40. **a)** This really has two parts. First suppose that b is in $f(S \cup T)$. Thus $b = f(a)$ for some $a \in S \cup T$. Either $a \in S$, in which case $b \in f(S)$, or $a \in T$, in which case $b \in f(T)$. Thus in either case $b \in f(S) \cup f(T)$. This shows that $f(S \cup T) \subseteq f(S) \cup f(T)$. Conversely, suppose $b \in f(S) \cup f(T)$. Then either $b \in f(S)$ or $b \in f(T)$. This means either that $b = f(a)$ for some $a \in S$ or that $b = f(a)$ for some $a \in T$. In either case, $b = f(a)$ for some $a \in S \cup T$, so $b \in f(S \cup T)$. This shows that $f(S) \cup f(T) \subseteq f(S \cup T)$, and our proof is complete.

b) Suppose $b \in f(S \cap T)$. Then $b = f(a)$ for some $a \in S \cap T$. This implies that $a \in S$ and $a \in T$, so we have $b \in f(S)$ and $b \in f(T)$. Therefore $b \in f(S) \cap f(T)$, as desired.

42. **a)** The answer is the set of all solutions to $x^2 = 1$, namely $\{1, -1\}$.

b) In order for x^2 to be strictly between 0 and 1, we need x to be either strictly between 0 and 1 or strictly between -1 and 0. Therefore the answer is $\{x \mid -1 < x < 0 \vee 0 < x < 1\}$.

c) In order for x^2 to be greater than 4, we need either $x > 2$ or $x < -2$. Therefore the answer is $\{x \mid x > 2 \vee x < -2\}$.

44. **a)** We need to prove two things. First suppose $x \in f^{-1}(S \cup T)$. This means that $f(x) \in S \cup T$. Therefore either $f(x) \in S$ or $f(x) \in T$. In the first case $x \in f^{-1}(S)$, and in the second case $x \in f^{-1}(T)$. In either case, then, $x \in f^{-1}(S) \cup f^{-1}(T)$. Thus we have shown that $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}(T)$. Conversely, suppose that $x \in f^{-1}(S) \cup f^{-1}(T)$. Then either $x \in f^{-1}(S)$ or $x \in f^{-1}(T)$, so either $f(x) \in S$ or $f(x) \in T$. Thus we know that $f(x) \in S \cup T$, so by definition $x \in f^{-1}(S \cup T)$. This shows that $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$, as desired.

b) This is similar to part **(a)**. We have $x \in f^{-1}(S \cap T)$ if and only if $f(x) \in S \cap T$, if and only if $f(x) \in S$ and $f(x) \in T$, if and only if $x \in f^{-1}(S)$ and $x \in f^{-1}(T)$, if and only if $x \in f^{-1}(S) \cap f^{-1}(T)$.

46. There are three cases. Define the "fractional part" of x to be $f(x) = x - \lfloor x \rfloor$. Clearly $f(x)$ is always between 0 and 1 (inclusive at 0, exclusive at 1), and $x = \lfloor x \rfloor + f(x)$. If $f(x)$ is less than $\frac{1}{2}$, then $x + \frac{1}{2}$ will have a value slightly less than $\lfloor x \rfloor + 1$, so when we round down, we get $\lfloor x \rfloor$. In other words, in this case $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$, and indeed that is the integer closest to x. If $f(x)$ is greater than $\frac{1}{2}$, then $x + \frac{1}{2}$ will have a value slightly greater than $\lfloor x \rfloor + 1$, so when we round down, we get $\lfloor x \rfloor + 1$. In other words, in this case $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor + 1$, and indeed that is the integer closest to x in this case. Finally, if the fractional part is exactly $\frac{1}{2}$, then x is midway between two integers, and $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor + 1$, which is the larger of these two integers.

48. If x is not an integer, then $\lceil x \rceil$ is the integer just larger than x, and $\lfloor x \rfloor$ is the integer just smaller than x. Clearly they differ by 1. If x is an integer, then $\lceil x \rceil - \lfloor x \rfloor = x - x = 0$.

50. Write $x = n - \epsilon$, where n is an integer and $0 \le \epsilon < 1$; thus $\lceil x \rceil = n$. Then $\lceil x + m \rceil = \lceil n - \epsilon + m \rceil = n + m = \lceil x \rceil + m$. Alternatively, we could proceed along the lines of the proof of property 4a of Table 1, shown in the text.

52. **a)** The "if" direction is trivial, since $x \le \lceil x \rceil$. For the other direction, suppose that $x \le n$. Since n is an integer no smaller than x, and $\lceil x \rceil$ is by definition the smallest such integer, clearly $\lceil x \rceil \le n$.

b) The "if" direction is trivial, since $\lfloor x \rfloor \le x$. For the other direction, suppose that $n \le x$. Since n is an integer not exceeding x, and $\lfloor x \rfloor$ is by definition the largest such integer, clearly $n \le \lfloor x \rfloor$.

54. To prove the first equality, write $x = n - \epsilon$, where n is an integer and $0 \le \epsilon < 1$; thus $\lceil x \rceil = n$. Therefore, $\lfloor -x \rfloor = \lfloor -n + \epsilon \rfloor = -n = -\lceil x \rceil$. The second equality is proved in the same manner, writing $x = n + \epsilon$, where n is an integer and $0 \le \epsilon < 1$. This time $\lfloor x \rfloor = n$, and $\lceil -x \rceil = \lceil -n - \epsilon \rceil = -n = -\lfloor x \rfloor$.

56. In some sense this question is its own answer—the number of integers between a and b, inclusive, is the number of integers between a and b, inclusive. Presumably we seek an expression involving a, b, and the floor and/or ceiling function to answer this question. If we round a up and round b down to integers, then we will be looking at the smallest and largest integers just inside the range of integers we want to count, respectively. These values are of course $\lceil a \rceil$ and $\lfloor b \rfloor$, respectively. Then the answer is $\lfloor b \rfloor - \lceil a \rceil + 1$ (just think of counting all the integers between these two values, including both ends—if a row of fenceposts one foot apart extends for k feet, then there are $k + 1$ fenceposts). Note that this even works when, for example, $a = 0.3$ and $b = 0.7$.

58. Since a byte is eight bits, all we are asking for in each case is $\lceil n/8 \rceil$, where n is the number of bits.

a) $\lceil 4/8 \rceil = 1$ **b)** $\lceil 10/8 \rceil = 2$ **c)** $\lceil 500/8 \rceil = 63$ **d)** $\lceil 3000/8 \rceil = 375$

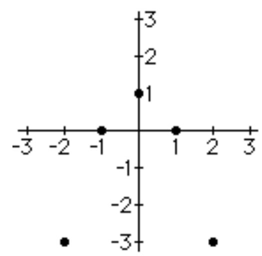
60. From Example 28 we know that one ATM cell is 53 bytes, or $53 \cdot 8 = 424$ bits long. Thus in each case we need to divide the number of bits transmitted in 10 seconds by 424 and round down.

a) In 10 seconds, this link can transmit $128{,}000 \cdot 10 = 1{,}280{,}000$ bits. Therefore the answer is $\lfloor 1{,}280{,}000/424 \rfloor = 3018$.

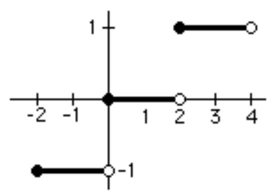
b) In 10 seconds, this link can transmit $300{,}000 \cdot 10 = 3{,}000{,}000$ bits. So the answer is $\lfloor 3{,}000{,}000/424 \rfloor = 7075$.

c) In 10 seconds, this link can transmit $1{,}000{,}000 \cdot 10 = 10{,}000{,}000$ bits. So the answer is $\lfloor 10{,}000{,}000/424 \rfloor = 23{,}584$.

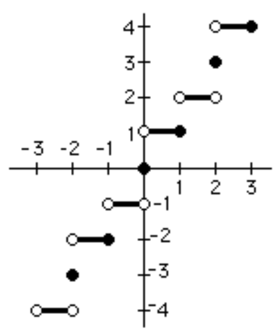
62. The graph consists of the points $(n, 1-n^2)$ for all $n \in \mathbf{Z}$. The picture shows part of the graph on the usual coordinate axes.



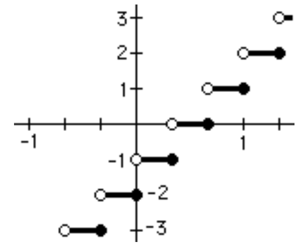
64. The graph is similar to the graph of $f(x) = \lfloor x \rfloor$; the only difference is a change in the scale of the x-axis.



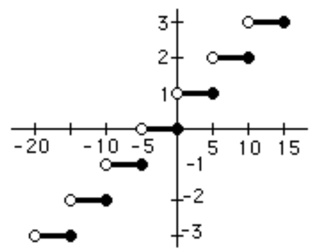
66. The function values for this step function change only at integer values of x, and different things happen for odd x and for even x because of the $x/2$ term. Whatever jump pattern is established on the closed interval $[0, 2]$ must repeat indefinitely in both directions. A thoughtful analysis then yields the following graph.



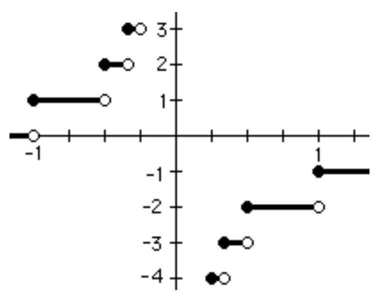
68. a) We can rewrite this as $f(x) = \lceil 3(x - \frac{2}{3}) \rceil$. The graph will therefore look look exactly like the graph of the function $f(x) = \lceil 3x \rceil$, except that the picture will be shifted to the right by $\frac{2}{3}$ unit, since x has been replaced by $x - \frac{2}{3}$. The graph of $f(x) = \lceil 3x \rceil$ is just like the graph shown in Figure 10b, except that the x-axis needs to be rescaled by a factor of 3 (the first jump on the positive x-axis occurs at $x = \frac{1}{3}$ here). Putting this all together yields the following picture. (Alternatively, we can think of this as the graph of $f(x) = \lceil 3x \rceil$ shifted down 2 units, since $\lceil 3x - 2 \rceil = \lceil 3x \rceil - 2$.)



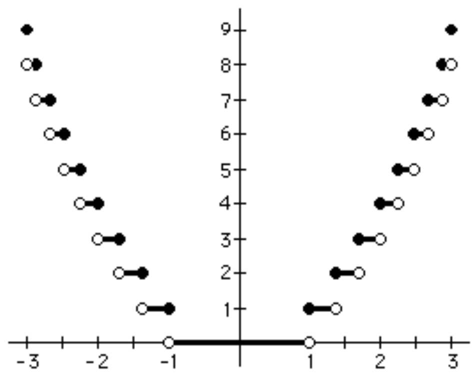
b) The graph will look exactly like the graph shown in Figure 10b, except that the x-axis needs to be rescaled by a factor of 5 (the first jump on the positive x-axis occurs at $x = 5$ here).



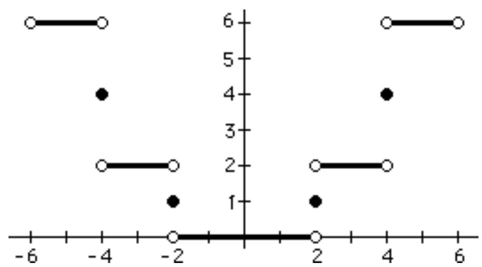
c) Since $\lfloor -1/x \rfloor = -\lceil 1/x \rceil$ (see Exercise 54), the picture is just the picture for Exercise 67d flipped upside down.



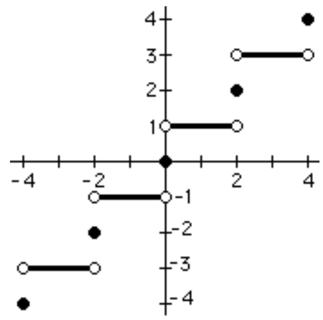
d) The basic shape is the parabola, $y = x^2$. However, because of the greatest integer function, the curve is broken into steps, with jumps at $x = \pm 1, \pm\sqrt{2}, \pm\sqrt{3}, \ldots$. Note the symmetry around the y-axis.



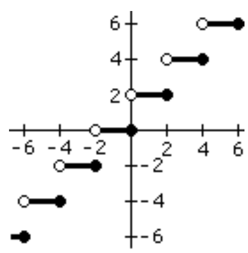
e) The basic shape is the parabola, $y = x^2/4$. However, because of the step functions, the curve is broken into steps. For x an even integer, $f(x) = x^4/4$, since the terms inside the floor and ceiling function symbols are integers. Note how these are isolated point, as in Exercise 67f.



f) When x is an even integer, this is just x. When x is between two even integers, however, this has the value of the odd integer between them. The graph is therefore as shown here.



g) Despite the complicated-looking formula, this is not too hard. Note that the expression inside the outer floor function symbols is always going to be an integer plus $\frac{1}{2}$; therefore we can tell exactly what its rounded-down value will be, namely $2\lceil x/2\rceil$. This is just the graph in Figure 10b, rescaled on both axes.



70. This follows immediately from the definition. We want to show that $\big((f\circ g)\circ(g^{-1}\circ f^{-1})\big)(z)=z$ for all $z\in Z$ and that $\big((g^{-1}\circ f^{-1})\circ(f\circ g)\big)(x)=x$ for all $x\in X$. For the first we have

$$\begin{aligned}\big((f\circ g)\circ(g^{-1}\circ f^{-1})\big)(z)&=(f\circ g)((g^{-1}\circ f^{-1})(z))\\&=(f\circ g)(g^{-1}(f^{-1}(z)))\\&=f(g(g^{-1}(f^{-1}(z))))\\&=f(f^{-1}(z))=z\,.\end{aligned}$$

The second equality is similar.

72. If f is one-to-one, then every element of A gets sent to a different element of B. If in addition to the range of A there were another element in B, then $|B|$ would be at least one greater than $|A|$. This cannot happen, so we conclude that f is onto. Conversely, suppose that f is onto, so that every element of B is the image of some element of A. In particular, there is an element of A for each element of B. If two or more elements of A were sent to the same element of B, then $|A|$ would be at least one greater than the $|B|$. This cannot happen, so we conclude that f is one-to-one.

74. **a)** This is true. Since $\lceil x \rceil$ is already an integer, $\lfloor \lceil x \rceil \rfloor = \lceil x \rceil$.

b) A little experimentation shows that this is not always true. To disprove it we need only produce a counterexample, such as $x = y = \frac{3}{4}$. In this case the left-hand side is $\lfloor 3/2 \rfloor = 1$, while the right-hand side is $0 + 0 = 0$.

c) A little trial and error fails to produce a counterexample, so maybe this is true. We look for a proof. Since we are dividing by 4, let us write $x = 4n + k$, where $0 \le k < 4$. In other words, write x in terms of how much it exceeds the largest multiple of 4 not exceeding it. There are three cases. If $k = 0$, then x is already a multiple of 4, so both sides equal n. If $0 < k \le 2$, then $\lceil x/2 \rceil = 2n + 1$, so the left-hand side is $\lceil n + \frac{1}{2} \rceil = n + 1$. Of course the right-hand side is $n + 1$ as well, so again the two sides agree. Finally, suppose that $2 < k < 4$. Then $\lceil x/2 \rceil = 2n + 2$, and the left-hand side is $\lceil n + 1 \rceil = n + 1$; of course the right-hand side is still $n + 1$, as well. Since we proved that the two sides are equal in all cases, the proof is complete.

d) For $x = 8.5$, the left-hand side is 3, whereas the right-hand side is 2.

e) This is true. Write $x = n + \epsilon$ and $y = m + \delta$, where n and m are integers and ϵ and δ are nonnegative real numbers less than 1. The left-hand side is $n + m + (n + m)$ or $n + m + (n + m + 1)$, the latter occurring if and only if $\epsilon + \delta \ge 1$. The right-hand side is the sum of two quantities. The first is either $2n$ (if $\epsilon < \frac{1}{2}$) or $2n + 1$ (if $\epsilon \ge \frac{1}{2}$). The second is either $2m$ (if $\delta < \frac{1}{2}$) or $2m + 1$ (if $\delta \ge \frac{1}{2}$). The only way, then, for the left-hand side to exceed the right-hand side is to have the left-hand side be $2n + 2m + 1$ and the right-hand side be $2n + 2m$. This can occur only if $\epsilon + \delta \ge 1$ while $\epsilon < \frac{1}{2}$ and $\delta < \frac{1}{2}$. But that is an impossibility, since the sum of two numbers less than $\frac{1}{2}$ cannot be as large as 1. Therefore the right-hand side is always at least as large as the left-hand side.

76. A straightforward way to do this problem is to consider the three cases determined by where in the interval between two consecutive integers the real number x lies. Certainly every real number x lies in an interval $[n, n + 1)$ for some integer n; indeed, $n = \lfloor x \rfloor$. (Recall that $[s, t)$ is the notation for the set of real numbers greater than or equal to s and less than t.) If $x \in [n, n + \frac{1}{3})$, then $3x$ lies in the interval $[3n, 3n + 1)$, so $\lfloor 3x \rfloor = 3n$. Moreover in this case $x + \frac{1}{3}$ is still less than $n + 1$, and $x + \frac{2}{3}$ is still less than $n + 1$, so $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + n = 3n$ as well. For the second case, we assume that $x \in [n + \frac{1}{3}, n + \frac{2}{3})$. This time $3x \in [3n + 1, 3n + 2)$, so $\lfloor 3x \rfloor = 3n + 1$. Moreover in this case $x + \frac{1}{3}$ is in $[n + \frac{2}{3}, n + 1)$, and $x + \frac{2}{3}$ is in $[n + 1, n + \frac{4}{3})$, so $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + (n + 1) = 3n + 1$ as well. The third case, $x \in [n + \frac{2}{3}, n + 1)$, is similar, with both sides equaling $3n + 2$.

78. **a)** We merely have to remark that f^* is well-defined by the rule given here. For each $a \in A$, either a is in the domain of definition of f or it is not. If it is, then $f^*(a)$ is the well-defined element $f(a) \in B$, and otherwise $f^*(a) = u$. In either case $f^*(a)$ is a well-defined element of $B \cup \{u\}$.

b) We simply need to set $f^*(a) = u$ for each a not in the domain of definition of f. In part **(a)**, then, $f^*(n) = 1/n$ for $n \ne 0$, and $f^*(0) = u$. In part **(b)** we have a total function already, so $f^*(n) = \lceil n/2 \rceil$ for all $n \in \mathbf{Z}$. In part **(c)** $f^*(m, n) = m/n$ if $n \ne 0$, and $f^*(m, 0) = u$ for all $m \in \mathbf{Z}$. In part **(d)** we have a total function already, so $f^*(m, n) = mn$ for all values of m and n. In part **(e)** the rule only applies if $m > n$, so $f^*(m, n) = m - n$ if $m > n$, and $f^*(m, n) = u$ if $m \le n$.

80. For the "if" direction, we simply need to note that if S is a finite set, with cardinality m, then every proper subset of S has cardinality strictly smaller than m, so there is no possible one-to-one correspondence between the elements of S and the elements of the proper subset. (This is essentially the pigeonhole principle, to be discussed in Section 6.2.)

The "only if" direction is much deeper. Let S be the given infinite set. Clearly S is not empty, because by definition, the empty set has cardinality 0, a nonnegative integer. Let a_0 be one element of S, and let $A = S - \{a_0\}$. Clearly A is also infinite (because if it were finite, then we would have $|S| = |A| + 1$, making

S finite). We will now construct a one-to-one correspondence between S and A; think of this as a one-to-one and onto function f from S to A. (This construction is an infinite process; technically we are using something called the Axiom of Choice.) In order to define $f(a_0)$, we choose an arbitrary element a_1 in A (which is possible because A is infinite) and set $f(a_0) = a_1$. Next we define f at a_1. To do so, we choose an arbitrary element a_2 in $A - \{a_1\}$ (which is possible because $A - \{a_1\}$ is necessarily infinite) and set $f(a_1) = a_2$. Next we define f at a_2. To do so, we choose an arbitrary element a_3 in $A - \{a_1, a_2\}$ (which is possible because $A - \{a_1, a_2\}$ is necessarily infinite) and set $f(a_2) = a_3$. We continue this process forever. Finally, we let f be the identity function on $S - \{a_0, a_1, a_2, \ldots\}$. The function thus defined has $f(a_i) = a_{i+1}$ for all natural numbers i and $f(x) = x$ for all $x \in S - \{a_0, a_1, a_2, \ldots\}$. Our construction forced f to be one-to-one and onto.

SECTION 2.4 Sequences and Summations

2. In each case we just plug $n = 8$ into the formula.
a) $2^{8-1} = 128$ **b)** 7 **c)** $1 + (-1)^8 = 0$ **d)** $-(-2)^8 = -256$

4. a) $a_0 = (-2)^0 = 1$, $a_1 = (-2)^1 = -2$, $a_2 = (-2)^2 = 4$, $a_3 = (-2)^3 = -8$
b) $a_0 = a_1 = a_2 = a_3 = 3$
c) $a_0 = 7 + 4^0 = 8$, $a_1 = 7 + 4^1 = 11$, $a_2 = 7 + 4^2 = 23$, $a_3 = 7 + 4^3 = 71$
d) $a_0 = 2^0 + (-2)^0 = 2$, $a_1 = 2^1 + (-2)^1 = 0$, $a_2 = 2^2 + (-2)^2 = 8$, $a_3 = 2^3 + (-2)^3 = 0$

6. These are easy to compute by hand, calculator, or computer.
a) 10, 7, 4, 1, -2, -5, -8, -11, -14, -17
b) We can use the formula in Table 2, or we can just keep adding to the previous term ($1+2=3$, $3+3=6$, $6+4=10$, and so on): 1, 3, 6, 10, 15, 21, 28, 36, 45, 55. These are called the triangular numbers.
c) 1, 5, 19, 65, 211, 665, 2059, 6305, 19171, 58025
d) 1, 1, 1, 2, 2, 2, 2, 2, 3, 3 (there will be $2k+1$ copies of k) **e)** 1, 5, 6, 11, 17, 28, 45, 73, 118, 191
f) The largest number whose binary expansion has n bits is $(11\ldots1)_2$, which is $2^n - 1$. So the sequence is 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.
g) 1, 2, 2, 4, 8, 11, 33, 37, 148, 153 **h)** 1, 2, 2, 2, 2, 3, 3, 3, 3, 3

8. One rule could be that each term is 2 greater than the previous term; the sequence would be 3, 5, 7, 9, 11, 13, ... Another rule could be that the n^{th} term is the n^{th} odd prime; the sequence would be 3, 5, 7, 11, 13, 17, ... Actually, we could choose any number we want for the fourth term (say 12) and find a third degree polynomial whose value at n would be the n^{th} term; in this case we need to solve for A, B, C, and D in the equations $y = Ax^3 + Bx^2 + Cx + D$ where $(1,3)$, $(2,5)$, $(3,7)$, $(4,12)$ have been plugged in for x and y. Doing so yields $(x^3 - 6x^2 + 15x - 4)/2$. With this formula, the sequence is 3, 5, 7, 12, 23, 43, 75, 122, 187, 273. Obviously many other answers are possible.

10. In each case we simply plug $n = 0, 1, 2, 3, 4, 5$, using the initial conditions for the first few and then the recurrence relation.
a) $a_0 = -1$, $a_1 = -2a_0 = 2$, $a_2 = -2a_1 = -4$, $a_3 = -2a_2 = 8$, $a_4 = -2a_3 = -16$, $a_5 = -2a_4 = 32$
b) $a_0 = 2$, $a_1 = -1$, $a_2 = a_1 - a_0 = -3$, $a_3 = a_2 - a_1 = -2$, $a_4 = a_3 - a_2 = 1$, $a_5 = a_4 - a_3 = 3$
c) $a_0 = 1$, $a_1 = 3a_0^2 = 3$, $a_2 = 3a_1^2 = 27 = 3^3$, $a_3 = 3a_2^2 = 2187 = 3^7$, $a_4 = 3a_3^2 = 14348907 = 3^{15}$, $a_5 = 3a_4^2 = 617673396283947 = 3^{31}$
d) $a_0 = -1$, $a_1 = 0$, $a_2 = 2a_1 + a_0^2 = 1$, $a_3 = 3a_2 + a_1^2 = 3$, $a_4 = 4a_3 + a_2^2 = 13$, $a_5 = 5a_4 + a_3^2 = 74$
e) $a_0 = 1$, $a_1 = 1$, $a_2 = 2$, $a_3 = a_2 - a_1 + a_0 = 2$, $a_4 = a_3 - a_2 + a_1 = 1$, $a_5 = a_4 - a_3 + a_2 = 1$

12. **a)** $-3a_{n-1}+4a_{n-2}=-3\cdot 0+4\cdot 0=0=a_n$ **b)** $-3a_{n-1}+4a_{n-2}=-3\cdot 1+4\cdot 1=1=a_n$
c) $-3a_{n-1}+4a_{n-2}=-3\cdot(-4)^{n-1}+4\cdot(-4)^{n-2}=(-4)^{n-2}\big((-3)(-4)+4\big)=(-4)^{n-2}\cdot 16=(-4)^{n-2}(-4)^2=(-4)^n=a_n$
d) $-3a_{n-1}+4a_{n-2}=-3\cdot\big(2(-4)^{n-1}+3\big)+4\cdot\big(2(-4)^{n-2}+3\big)=(-4)^{n-2}\big((-6)(-4)+4\cdot 2\big)-9+12=(-4)^{n-2}\cdot 32+3=(-4)^{n-2}(-4)^2\cdot 2+3=2\cdot(-4)^n+3=a_n$

14. In each case, one possible answer is just the equation as presented (it is a recurrence relation of degree 0). We will give an alternate answer.
a) One possible answer is $a_n=a_{n-1}$.
b) Note that $a_n-a_{n-1}=2n-(2n-2)=2$. Therefore we have $a_n=a_{n-1}+2$ as one possible answer.
c) Just as in part **(b)**, we have $a_n=a_{n-1}+2$.
d) Probably the simplest answer is $a_n=5a_{n-1}$.
e) Since $a_n-a_{n-1}=n^2-(n-1)^2=2n-1$, we have $a_n=a_{n-1}+2n-1$.
f) This is similar to part **(e)**. One answer is $a_n=a_{n-1}+2n$.
g) Note that $a_n-a_{n-1}=n+(-1)^n-(n-1)-(-1)^{n-1}=1+2(-1)^n$. Thus we have $a_n=a_{n-1}+1+2(-1)^n$.
h) $a_n=na_{n-1}$

16. In the iterative approach, we write a_n in terms of a_{n-1}, then write a_{n-1} in terms of a_{n-2} (using the recurrence relation with $n-1$ plugged in for n), and so on. When we reach the end of this procedure, we use the given initial value of a_0. This will give us an explicit formula for the answer or it will give us a finite series, which we then sum to obtain an explicit formula for the answer.
a) $a_n=-a_{n-1}=(-1)^2a_{n-2}=\cdots=(-1)^na_{n-n}=(-1)^na_0=5\cdot(-1)^n$
b) $a_n=3+a_{n-1}=3+3+a_{n-2}=2\cdot 3+a_{n-2}=3\cdot 3+a_{n-3}=\cdots=n\cdot 3+a_{n-n}=n\cdot 3+a_0=3n+1$
c)
$$\begin{aligned}
a_n&=-n+a_{n-1}\\
&=-n+\big(-(n-1)+a_{n-2}\big)=-\big(n+(n-1)\big)+a_{n-2}\\
&=-\big(n+(n-1)\big)+\big(-(n-2)+a_{n-3}\big)=-\big(n+(n-1)+(n-2)\big)+a_{n-3}\\
&\ \ \vdots\\
&=-\big(n+(n-1)+(n-2)+\cdots+(n-(n-1))\big)+a_{n-n}\\
&=-\big(n+(n-1)+(n-2)+\cdots+1\big)+a_0\\
&=-\frac{n(n+1)}{2}+4=\frac{-n^2-n+8}{2}
\end{aligned}$$
d)
$$\begin{aligned}
a_n&=-3+2a_{n-1}\\
&=-3+2(-3+2a_{n-2})=-3+2(-3)+4a_{n-2}\\
&=-3+2(-3)+4(-3+2a_{n-3})=-3+2(-3)+4(-3)+8a_{n-3}\\
&=-3+2(-3)+4(-3)+8(-3+2a_{n-4})=-3+2(-3)+4(-3)+8(-3)+16a_{n-4}\\
&\ \ \vdots\\
&=-3(1+2+4+\cdots+2^{n-1})+2^na_{n-n}=-3(2^n-1)+2^n(-1)=-2^{n+2}+3
\end{aligned}$$
e)
$$\begin{aligned}
a_n&=(n+1)a_{n-1}=(n+1)na_{n-2}\\
&=(n+1)n(n-1)a_{n-3}=(n+1)n(n-1)(n-2)a_{n-4}\\
&\ \ \vdots\\
&=(n+1)n(n-1)(n-2)(n-3)\cdots(n-(n-2))\,a_{n-n}\\
&=(n+1)n(n-1)(n-2)(n-3)\cdots 2\cdot a_0\\
&=(n+1)!\cdot 2=2(n+1)!
\end{aligned}$$

f)

$$\begin{aligned}
a_n &= 2na_{n-1} \\
&= 2n\big(2(n-1)a_{n-2}\big) = 2^2\big(n(n-1)\big)a_{n-2} \\
&= 2^2\big(n(n-1)\big)\big(2(n-2)a_{n-3}\big) = 2^3\big(n(n-1)(n-2)\big)a_{n-3} \\
&\ \ \vdots \\
&= 2^n n(n-1)(n-2)(n-3)\cdots\big(n-(n-1)\big)a_{n-n} \\
&= 2^n n(n-1)(n-2)(n-3)\cdots 1\cdot a_0 \\
&= 3\cdot 2^n n!
\end{aligned}$$

g)

$$\begin{aligned}
a_n &= n-1-a_{n-1} \\
&= n-1-\big((n-1-1)-a_{n-2}\big) = (n-1)-(n-2)+a_{n-2} \\
&= (n-1)-(n-2)+\big((n-2-1)-a_{n-3}\big) = (n-1)-(n-2)+(n-3)-a_{n-3} \\
&\ \ \vdots \\
&= (n-1)-(n-2)+\cdots+(-1)^{n-1}(n-n)+(-1)^n a_{n-n} \\
&= \frac{2n-1+(-1)^n}{4}+(-1)^n\cdot 7
\end{aligned}$$

18. **a)** The amount after $n-1$ years is multiplied by 1.09 to give the amount after n years, since 9% of the value must be added to account for the interest. Thus we have $a_n = 1.09a_{n-1}$. The initial condition is $a_0 = 1000$.
b) Since we multiply by 1.09 for each year, the solution is $a_n = 1000(1.09)^n$.
c) $a_{100} = 1000(1.09)^{100} \approx \$5{,}529{,}041$

20. This is just like Exercise 18. We are letting a_n be the population, in billions of people, n years after 2010.
a) $a_n = 1.011a_{n-1}$, with $a_0 = 6.9$ **b)** $a_n = 6.9\cdot(1.011)^n$
c) $a_{20} = 6.9\cdot(1.011)^{20} \approx 8.6$ billion people

22. We let a_n be the salary, in thousands of dollars, n years after 2009.
a) $a_n = 1+1.05a_{n-1}$, with $a_0 = 50$
b) Here $n = 8$. We can either iterate the recurrence relation 8 times, or we can use the result of part **(c)**. The answer turns out to be approximately $a_8 = 83.4$, i.e., a salary of approximately $\$83{,}400$.
c) We use the iterative approach.

$$\begin{aligned}
a_n &= 1+1.05a_{n-1} \\
&= 1+1.05(1+1.05a_{n-2}) \\
&= 1+1.05+(1.05)^2 a_{n-2} \\
&\ \ \vdots \\
&= 1+1.05+(1.05)^2+\cdots+(1.05)^{n-1}+(1.05)^n a_0 \\
&= \frac{(1.05)^n-1}{1.05-1}+50\cdot(1.05)^n \\
&= 70\cdot(1.05)^n-20
\end{aligned}$$

24. **a)** Each month our account accrues some interest that must be paid. Since the balance the previous month is $B(k-1)$, the amount of interest we owe is $(r/12)B(k-1)$. After paying this interest, the rest of the P dollar payment we make each month goes toward reducing the principle. Therefore we have $B(k) =$

$B(k-1) - (P - (r/12)B(k-1))$. This can be simplified to $B(k) = (1 + (r/12))B(k-1) - P$. The initial condition is that $B(0) =$ the amount borrowed.

b) Solving this by iteration yields

$$B(k) = (1 + (r/12))^k (B(0) - 12P/r) + 12P/r\,.$$

Setting $B(k) = 0$ and solving this for k yields the desired value of T after some messy algebra, namely

$$T = \frac{\log(-12P/(B(0)r - 12P))}{\log(1 + (r/12))}\,.$$

26. **a)** The first term is 3, and the n^{th} term is obtained by adding $2n-1$ to the previous term. In other words, we successively add 3, then 5, then 7, and so on. Alternatively, we see that the n^{th} term is n^2+2; we can see this by inspection if we happen to notice how close each term is to a perfect square, or we can fit a quadratic polynomial to the data. The next three terms are 123, 146, 171.

b) This is an arithmetic sequence whose first term is 7 and whose difference is 4. Thus the n^{th} term is $7 + 4(n-1) = 4n+3$. Thus the next three terms are 47, 51, 55.

c) The n^{th} term is clearly the binary expansion of n. Thus the next three terms are 1100, 1101, 1110.

d) The sequence consists of one 1, followed by three 2's, followed by five 3's, followed by seven 5's, and so on, with the number of copies of the next value increasing by 2 each time, and the values themselves following the rule that the first two values are 1 and 2 and each subsequent value is the sum of the previous two values. Obviously other answers are possible as well. By our rule, the next three terms would be 8, 8, 8.

e) If we stare at this sequence long enough and compare it with Table 1, then we notice that the n^{th} term is $3^n - 1$. Thus the next three terms are 59048, 177146, 531440.

f) We notice that each term evenly divides the next, and the multipliers are successively 3, 5, 7, 9, 11, and so on. That must be the intended pattern. One notation for this is to use $n!!$ to mean $n(n-2)(n-4)\cdots$; thus the n^{th} term is $(2n-1)!!$. Thus the next three terms are 654729075, 13749310575, 316234143225.

g) The sequence consists of one 1, followed by two 0s, then three 1s, four 0s, five 1s, and so on, alternating between 0s and 1s and having one more item in each group than in the previous group. Thus six 0's will follow next, so the next three terms are 0, 0, 0.

h) It doesn't take long to notice that each term is the square of its predecessor. The next three terms get very big very fast: 18446744073709551616, $340282366920938463463374607431768211456$, and then

$$115792089237316195423570985008687907853269984665640564039457584007913129639936\,.$$

(These were computed using *Maple*.)

28. Let us ask ourselves which is the last term in the sequence whose value is k? Clearly it is $1+2+3+\cdots+k$, which equals $k(k+1)/2$. We can rephrase this by saying that $a_n \le k$ if and only if $k(k+1)/2 \ge n$. Thus, to find k as a function of n, we must find the smallest k such that $k(k+1)/2 \ge n$. This is equivalent to $k^2 + k - 2n \ge 0$. By the quadratic formula, this tells us that k has to be at least $(-1+\sqrt{1+8n})/2$. Therefore we have $k = \lceil(-1+\sqrt{1+8n})/2\rceil = \left\lceil -\frac{1}{2} + \sqrt{2n+\frac{1}{4}}\right\rceil$. By Exercise 47 in Section 2.3, this is the same as the integer closest to $\sqrt{2n+\frac{1}{4}}$, where we choose the smaller of the two closest integers if $\sqrt{2n+\frac{1}{4}}$ is a half integer. The desired answer is $\lfloor\sqrt{2n}+\frac{1}{2}\rfloor$, which by Exercise 46 in Section 2.3 is the integer closest to $\sqrt{2n}$ (note that $\sqrt{2n}$ can never be a half integer). To see that these are the same, note that it can never happen that $\sqrt{2n} \le m + \frac{1}{2}$ while $\sqrt{2n+\frac{1}{4}} > m + \frac{1}{2}$ for some positive integer m, since this would imply that $2n \le m^2 + m + \frac{1}{4}$ and $2n > m^2 + m$, an impossibility. Therefore the integer closest to $\sqrt{2n}$ and the (smaller) integer closest to $\sqrt{2n+\frac{1}{4}}$ are the same, and we are done.

30. **a)** $1+3+5+7=16$ **b)** $1^2+3^2+5^2+7^2=84$
c) $(1/1)+(1/3)+(1/5)+(1/7)=176/105$ **d)** $1+1+1+1=4$

32. **a)** The terms of this sequence alternate between 2 (if j is even) and 0 (if j is odd). Thus the sum is $2+0+2+0+2+0+2+0+2=10$.
b) We can break this into two parts and compute $\left(\sum_{j=0}^{8} 3^j\right)-\left(\sum_{j=0}^{8} 2^j\right)$. Each summation can be computed from the formula for the sum of a geometric progression. Thus the answer is

$$\frac{3^9-1}{3-1}-\frac{2^9-1}{2-1}=9841-511=9330\,.$$

c) As in part **(b)** we can break this into two parts and compute $\left(\sum_{j=0}^{8} 2\cdot 3^j\right)+\left(\sum_{j=0}^{8} 3\cdot 2^j\right)$. Each summation can be computed from the formula for the sum of a geometric progression. Thus the answer is

$$\frac{2\cdot 3^9-2}{3-1}+\frac{3\cdot 2^9-3}{2-1}=19682+1533=21215\,.$$

d) This could be worked as in part **(b)**, but it is easier to note that the sum telescopes (see Exercise 35). Each power of 2 cancels except for the -2^0 when $j=0$ and the 2^9 when $j=8$. Therefore the answer is $2^9-2^0=511$. (Alternatively, note that $2^{j+1}-2^j=2^j$.)

34. We will just write out the sums explicitly in each case.
a) $(1-1)+(1-2)+(2-1)+(2-2)+(3-1)+(3-2)=3$
b) $(0+0)+(0+2)+(0+4)+(3+0)+(3+2)+(3+4)+(6+0)+(6+2)+(6+4)+(9+0)+(9+2)+(9+4)=78$
c) $(0+1+2)+(0+1+2)+(0+1+2)=9$
d) $(0+0+0+0)+(0+1+8+27)+(0+4+32+108)=180$

36. We use the suggestion (simple algebra shows that this is indeed an identity) and note that all the terms in the summation cancel out except for the $1/k$ when $k=1$ and the $1/(k+1)$ when $k=n$:

$$\sum_{k=1}^{n}\frac{1}{k(k+1)}=\sum_{k=1}^{n}\left(\frac{1}{k}-\frac{1}{k+1}\right)=\frac{1}{1}-\frac{1}{n+1}=\frac{n}{n+1}$$

38. First we note that $k^3-(k-1)^3=3k^2-3k+1$. Then we sum this equation for all values of k from 1 to n. On the left, because of telescoping, we have just n^3; on the right we have

$$3\sum_{k=1}^{n}k^2-3\sum_{k=1}^{n}k+\sum_{k=1}^{n}1=3\sum_{k=1}^{n}k^2-\frac{3n(n+1)}{2}+n\,.$$

Equating the two sides and solving for $\sum_{k=1}^{n}k^2$, we obtain the desired formula.

$$\begin{aligned}\sum_{k=1}^{n}k^2&=\frac{1}{3}\left(n^3+\frac{3n(n+1)}{2}-n\right)\\&=\frac{n}{3}\left(\frac{2n^2+3n+3-2}{2}\right)\\&=\frac{n}{3}\left(\frac{2n^2+3n+1}{2}\right)=\frac{n(n+1)(2n+1)}{6}\end{aligned}$$

40. This exercise is like Example 23. From Table 2 we know that $\sum_{k=1}^{200}k^3=200^2\cdot 201^2/4=404{,}010{,}000$, and $\sum_{k=1}^{98}k^3=98^2\cdot 99^2/4=23{,}532{,}201$. Therefore the desired sum is $404{,}010{,}000-23{,}532{,}201=380{,}477{,}799$.

42. If we write down the first few terms of this sum we notice a pattern. It starts $(1+1+1+1+1+1+1)+(2+2+2+2+2+2+2+2+2+2+2+2+2+2+2+2+2+2+2)+(3+3+3+3+\cdots+3)+\cdots$. There are seven 1s, then 19 2s, then 37 3s, and so on; in general, the number of i's is $(i+1)^3-i^3=3i^2+3i+1$. So we need to sum $i(3i^2+3i+1)$ for an appropriate range of values for i. We must find this range. It gets a little messy at the end if m is such that the sequence stops before a complete range of the last value is present. Let $n=\lfloor\sqrt[3]{m}\rfloor-1$. Then there are $n+1$ blocks, and $(n+1)^3-1$ is where the next-to-last block ends. The sum of those complete blocks is $\sum_{i=1}^{n} i(3i^2+3i+1)=\sum_{i=1}^{n} 3i^3+3i^2+i=n(3n+4)(n+1)^2/4$ (using Table 2 and algebra). The remaining terms in our summation all have the value $n+1$ and the number of them present is $m-((n+1)^3-1)$. Our final answer is therefore $n(3n+4)(n+1)^2/4+(n+1)(m-(n+1)^3+1)$, where, once again, $n=\lfloor\sqrt[3]{m}\rfloor-1$.

44. $n!=\displaystyle\prod_{i=1}^{n} i$

46. $(0!)(1!)(2!)(3!)(4!)=1\cdot 1\cdot 2\cdot 6\cdot 24=288$

SECTION 2.5 Cardinality of Sets

2. **a)** This set is countably infinite. The integers in the set are 11, 12, 13, 14, and so on. We can list these numbers in that order, thereby establishing the desired correspondence. In other words, the correspondence is given by $1\leftrightarrow 11$, $2\leftrightarrow 12$, $3\leftrightarrow 13$, and so on; in general $n\leftrightarrow(n+10)$.

b) This set is countably infinite. The integers in the set are -1, -3, -5, -7, and so on. We can list these numbers in that order, thereby establishing the desired correspondence. In other words, the correspondence is given by $1\leftrightarrow -1$, $2\leftrightarrow -3$, $3\leftrightarrow -5$, and so on; in general $n\leftrightarrow -(2n-1)$.

c) This set is $\{-999{,}999, -999{,}998, \ldots, -1, 0, 1, \ldots, 999{,}999\}$. It is finite, with cardinality 1,999,999.

d) This set is uncountable. We can prove it by the same diagonalization argument as was used to prove that the set of all reals is uncountable in Example 5.

e) This set is countable. We can list its elements in the order $(2,1),(3,1),(2,2),(3,2),(2,3),(3,3),\ldots$, giving us the one-to-one correspondence $1\leftrightarrow(2,1), 2\leftrightarrow(3,1), 3\leftrightarrow(2,2), 4\leftrightarrow(3,2), 5\leftrightarrow(2,3), 6\leftrightarrow(3,3),\ldots$.

f) This set is countable. The integers in the set are 0, ± 10, ± 20, ± 30, and so on. We can list these numbers in the order 0, 10, -10, 20, -20, 30, $\ldots$, thereby establishing the desired correspondence. In other words, the correspondence is given by $1\leftrightarrow 0$, $2\leftrightarrow 10$, $3\leftrightarrow -10$, $4\leftrightarrow 20$, $5\leftrightarrow -20$, $6\leftrightarrow 30$, and so on.

4. **a)** This set is countable. The integers in the set are ± 1, ± 2, ± 4, ± 5, ± 7, and so on. We can list these numbers in the order 1, -1, 2, -2, 4, -4, 5, -5, 7, -7, $\ldots$, thereby establishing the desired correspondence. In other words, the correspondence is given by $1\leftrightarrow 1$, $2\leftrightarrow -1$, $3\leftrightarrow 2$, $4\leftrightarrow -2$, $5\leftrightarrow 4$, and so on.

b) This is similar to part **(a)**; we can simply list the elements of the set in order of increasing absolute value, listing each positive term before its corresponding negative: 5, -5, 10, -10, 15, -15, 20, -20, 25, -25, 30, -30, 40, -40, 45, -45, 50, -50, $\ldots$.

c) This set is countable but a little tricky. We can arrange the numbers in a 2-dimensional table as follows:

$.\overline{1}$	.1	.11	.111	.1111	.11111	.111111	…
$1.\overline{1}$	1	1.1	1.11	1.111	1.1111	1.11111	…
$11.\overline{1}$	11	11.1	11.11	11.111	11.1111	11.11111	…
$111.\overline{1}$	111	111.1	111.11	111.111	111.1111	111.11111	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Thus we have shown that our set is the countable union of countable sets (each of the countable sets is one row of this table). Therefore by Exercise 27, the entire set is countable. For an explicit correspondence with the positive integers, we can zigzag along the positive-sloping diagonals as in Figure 3: $1 \leftrightarrow .\overline{1}$, $2 \leftrightarrow 1.\overline{1}$, $3 \leftrightarrow .1$, $4 \leftrightarrow .11$, $5 \leftrightarrow 1$, and so on.

d) This set is not countable. We can prove it by the same diagonalization argument as was used to prove that the set of all reals is uncountable in Example 5. All we need to do is choose $d_i = 1$ when $d_{ii} = 9$ and choose $d_i = 9$ when $d_{ii} = 1$ or d_{ii} is blank (if the decimal expansion is finite).

6. We want a one-to-one function from the set of positive integers to the set of odd positive integers. The simplest one to use is $f(n) = 2n - 1$. We put the guest currently in Room n into Room $(2n - 1)$. Thus the guest in Room 1 stays put, the guest in Room 2 moves to Room 3, the guest in Room 3 moves to Room 5, and so on.

8. First we can make the move explained in Exercise 6, which frees up all the even-numbered rooms. The new guests can go into those rooms (the first into Room 2, the second into Room 4, and so on).

10. In each case, let us take A to be the set of real numbers.

a) We can let B be the set of real numbers as well; then $A - B = \emptyset$, which is finite.

b) We can let B be the set of real numbers that are not positive integers; in symbols, $B = A - \mathbf{Z}^+$. Then $A - B = \mathbf{Z}^+$, which is countably infinite.

c) We can let B be the set of positive real numbers. Then $A - B$ is the set of negative real numbers and 0, which is certainly uncountable.

12. The definition of $|A| \le |B|$ is that there is a one-to-one function from A to B. In this case the desired function is just $f(x) = x$ for each $x \in A$.

14. If A and B have the same cardinality, then we have a one-to-one correspondence $f : A \to B$. The function f meets the requirement of the definition that $|A| \le |B|$, and f^{-1} meets the requirement of the definition that $|B| \le |A|$.

16. If a set A is countable, then we can list its elements, $a_1, a_2, a_3, \ldots, a_n, \ldots$ (possibly ending after a finite number of terms). Every subset of A consists of some (or none or all) of the items in this sequence, and we can list them in the same order in which they appear in the sequence. This gives us a sequence (again, infinite or finite) listing all the elements of the subset. Thus the subset is also countable.

18. The hypothesis gives us a one-to-one and onto function f from A to B. By Exercise 16e in the supplementary exercises for this chapter, the function S_f from $\mathcal{P}(A)$ to $\mathcal{P}(B)$ defined by $S_f(X) = f(X)$ for all $X \subseteq A$ is one-to-one and onto. Therefore $\mathcal{P}(A)$ and $\mathcal{P}(B)$ have the same cardinality.

20. By definition, we have one-to-one onto functions $f : A \to B$ and $g : B \to C$. Then $g \circ f$ is a one-to-one onto function from A to C, so $|A| = |C|$.

22. If $A = \emptyset$, then the only way for the conditions to be met are that $B = \emptyset$ as well, and we are done. So assume that A is nonempty. Let f be the given onto function from A to B, and let $g : \mathbf{Z}^+ \to A$ be an onto function that establishes the countability of A. (If A is finite rather than countably infinite, say of cardinality k, then the function g will be defined so that $g(1)$, $g(2)$, $\ldots$, $g(k)$ will list the elements of A, and $g(n) = g(1)$ for $n > k$.) We need to find an onto function from $\mathbf{Z}^+$ to B. The function $f \circ g$ does the trick, because the composition of two onto functions is onto (Exercise 33b in Section 2.3).

24. Because $|A| < |\mathbf{Z}^+|$, there is a one-to-one function $f : A \to \mathbf{Z}^+$. We are also given that A is infinite, so the range of f has to be infinite. We will construct a bijection g from $\mathbf{Z}^+$ to A. For each $n \in \mathbf{Z}^+$, let m be the n^{th} smallest element in the range of f. Then $g(n) = f^{-1}(m)$. The existence of g contradicts the definition of $|A| < |\mathbf{Z}^+|$, and our proof is complete.

26. We can label the rational numbers with strings from the set $\{0,1,2,3,4,5,6,7,8,9,/,-\}$ by writing down the string that represents that rational number in its simplest form (no leading 0's, denominator not 0, no common factors greater than 1 between numerator and denominator, and the minus sign in front if the number is negative). The labels are unique. It follows immediately from Exercise 25 that the set of rational numbers is countable.

28. We can think of $\mathbf{Z}^+ \times \mathbf{Z}^+$ as the countable union of countable sets, where the i^{th} set in the collection, for $i \in \mathbf{Z}^+$, is $\{(i,n) \mid n \in \mathbf{Z}^+\}$. The statement now follows from Exercise 27.

30. There are at most two real solutions of each quadratic equation, so the number of solutions is countable as long as the number of triples (a,b,c), with a, b, and c integers, is countable. But this follows from Exercise 27 in the following way. There are a countable number of pairs (b,c), since for each b (and there are countably many b's) there are only a countable number of pairs with that b as its first coordinate. Now for each a (and there are countably many a's) there are only a countable number of triples with that a as its first coordinate (since we just showed that there are only a countable number of pairs (b,c)). Thus again by Exercise 27 there are only countably many triples.

32. We saw in Exercise 31 that

$$f(m,n) = \frac{(m+n-2)(m+n-1)}{2} + m$$

is a one-to-one function with domain $\mathbf{Z}^+ \times \mathbf{Z}^+$. We want to expand the domain to be $\mathbf{Z} \times \mathbf{Z}$, so things need to be spread out a little if we are to keep it one-to-one. If we can find a one-to-one function g from $\mathbf{Z} \times \mathbf{Z}$ to $\mathbf{Z}^+ \times \mathbf{Z}^+$, then composing these two functions will be our desired one-to-one function from $\mathbf{Z} \times \mathbf{Z}$ to $\mathbf{Z}$ (we know from Exercise 33a in Section 2.3 that the composition of one-to-one functions is one-to-one). The function suggested here is $g(m,n) = ((3m+1)^2, (3n+1)^2)$, so that the composed function is $(f \circ g)(m,n) = ((3m+1)^2 + (3n+1)^2 - 2)((3m+1)^2 + (3n+1)^2 - 1)/2 + (3m+1)^2$. To see that g is one-to-one, first note that it is enough to show that the behavior in each coordinate is one-to-one; that is, the function that sends integer k to positive integer $(3k+1)^2$ is one-to-one. To see this, first note that if $k_1 \neq k_2$ and k_1 and k_2 are both positive or both negative, then $(3k_1+1)^2 \neq (3k_2+1)^2$. And if one is nonnegative and the other is negative, then they cannot have the same images under this function because the nonnegative integers are sent to squares of numbers that leave a remainder of 1 when divided by 3 ($0 \to 1^2$, $1 \to 4^2$, $2 \to 7^2$, $\ldots$), but negative integers are sent to squares of numbers that leave a remainder of 2 when divided by 3 ($-1 \to 2^2$, $-2 \to 5^2$, $-3 \to 8^2$, $\ldots$).

34. It suffices to find one-to-one functions $f:(0,1) \to \mathbf{R}$ and $g:\mathbf{R} \to (0,1)$. We can obviously use the function $f(x) = x$ in the first case. For the second, we can compress $\mathbf{R}$ onto $(0,1)$ by using the arctangent function, which is known to be injective; let $g(x) = 2\arctan(x)/\pi$. It then follows from the Schröder-Bernstein theorem that $|(0,1)| = |\mathbf{R}|$.

36. We can encode subsets of the set of positive integers as strings of, say, 5's and 6's, where the i^{th} symbol is a 5 if i is in the subset and a 6 otherwise. If we interpret this string as a real number by putting a 0 and a decimal point in front, then we have constructed a one-to-one function from $\mathcal{P}(\mathbf{Z}^+)$ to $(0,1)$. Also, we can construct a one-to-one function from $(0,1)$ to $\mathcal{P}(\mathbf{Z}+)$ by sending the number whose binary expansion is $0.d_1d_2d_3\ldots$ to the set $\{i \mid d_i = 1\}$. Therefore by the Schröder-Bernstein theorem we have $|\mathcal{P}(\mathbf{Z}^+)| = |(0,1)|$. By Exercise 34, $|(0,1)| = |\mathbf{R}|$, so we have shown that $|\mathcal{P}(\mathbf{Z}^+)| = |\mathbf{R}|$. (We already know from Cantor's diagonal argument that $\aleph_0 < |\mathbf{R}|$.) There is one technical point here. In order for our function from $(0,1)$ to $\mathcal{P}(\mathbf{Z}+)$ to be well-defined, we must choose which of two equivalent expressions to represent numbers that have terminating binary expansions to use (for example, $0.10010\overline{1}$ versus $0.10011\overline{0}$); we can decide to always use the terminating form, i.e., the one ending in all 0's.)

38. We know from Example 5 that the set of real numbers between 0 and 1 is uncountable. Let us associate to each real number in this range (including 0 but excluding 1) a function from the set of positive integers to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ as follows: If x is a real number whose decimal representation is $0.d_1d_2d_3\ldots$ (with ambiguity resolved by forbidding the decimal to end with an infinite string of 9's), then we associate to x the function whose rule is given by $f(n) = d_n$. Clearly this is a one-to-one function from the set of real numbers between 0 and 1 and a subset of the set of all functions from the set of positive integers to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Two different real numbers must have different decimal representations, so the corresponding functions are different. (A few functions are left out, because of forbidding representations such as $0.239999\ldots$.) Since the set of real numbers between 0 and 1 is uncountable, the subset of functions we have associated with them must be uncountable. But the set of all such functions has at least this cardinality, so it, too, must be uncountable (by Exercise 15).

40. We follow the hint. Suppose that f is a function from S to $\mathcal{P}(S)$. We must show that f is not onto. Let $T = \{\, s \in S \mid s \notin f(s) \,\}$. We will show that T is not in the range of f. If it were, then we would have $f(t) = T$ for some $t \in S$. Now suppose that $t \in T$. Then because $t \in f(t)$, it follows from the definition of T that $t \notin T$; this is a contradiction. On the other hand, suppose that $t \notin T$. Then because $t \notin f(t)$, it follows from the definition of T that $t \in T$; this is again a contradiction. This completes our proof by contradiction that f is not onto. On the other hand, the function sending x to $\{x\}$ for each $x \in S$ is a one-to-one function from S to $\mathcal{P}(S)$, so by Definition 2 $|S| \le |\mathcal{P}(S)|$. By the same definition, since $|S| = |\mathcal{P}(S)|$ (from what we have just proved and Definition 1), it follows that $|S| < |\mathcal{P}(S)|$.

SECTION 2.6 Matrices

2. We just add entry by entry.

a) $\begin{bmatrix} 0 & 3 & 9 \\ 1 & 4 & -1 \\ 2 & -5 & -3 \end{bmatrix}$ **b)** $\begin{bmatrix} -4 & 9 & 2 & 10 \\ -4 & -5 & 4 & 0 \end{bmatrix}$

4. To multiply matrices $\mathbf{A}$ and $\mathbf{B}$, we compute the $(i,j)^{\text{th}}$ entry of the product $\mathbf{AB}$ by adding all the products of elements from the i^{th} row of $\mathbf{A}$ with the corresponding element in the j^{th} column of $\mathbf{B}$, that is $\sum_{k=1}^{n} a_{ik}b_{kj}$. This can only be done, of course, when the number of columns of $\mathbf{A}$ equals the number of rows of $\mathbf{B}$ (called n in the formula shown here).

a) $\begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 1 & -2 & 1 \end{bmatrix}$ **b)** $\begin{bmatrix} 4 & -1 & -7 & 6 \\ -7 & -5 & 8 & 5 \\ 4 & 0 & 7 & 3 \end{bmatrix}$ **c)** $\begin{bmatrix} 2 & 0 & -3 & -4 & -1 \\ 24 & -7 & 20 & 29 & 2 \\ -10 & 4 & -17 & -24 & -3 \end{bmatrix}$

6. First note that $\mathbf{A}$ must be a 3×3 matrix in order for the sizes to work out as shown. If we name the elements of $\mathbf{A}$ in the usual way as $[a_{ij}]$, then the given equation is really nine equations in the nine unknowns a_{ij}, obtained simply by writing down what the matrix multiplication on the left means:

$$\begin{aligned}
1\cdot a_{11}+3\cdot a_{21}+2\cdot a_{31}&=7\\
1\cdot a_{12}+3\cdot a_{22}+2\cdot a_{32}&=1\\
1\cdot a_{13}+3\cdot a_{23}+2\cdot a_{33}&=3\\
2\cdot a_{11}+1\cdot a_{21}+1\cdot a_{31}&=1\\
2\cdot a_{12}+1\cdot a_{22}+1\cdot a_{32}&=0\\
2\cdot a_{13}+1\cdot a_{23}+1\cdot a_{33}&=3\\
4\cdot a_{11}+0\cdot a_{21}+3\cdot a_{31}&=-1\\
4\cdot a_{12}+0\cdot a_{22}+3\cdot a_{32}&=-3\\
4\cdot a_{13}+0\cdot a_{23}+3\cdot a_{33}&=7
\end{aligned}$$

This is really not as bad as it looks, since each variable only appears in three equations. For example, the first, fourth, and seventh equations are a system of three equations in the three variables a_{11}, a_{21}, and a_{31}. We can solve them using standard algebraic techniques to obtain $a_{11}=-1$, $a_{21}=2$ and $a_{31}=1$. By similar reasoning we also obtain $a_{12}=0$, $a_{22}=1$ and $a_{32}=-1$; and $a_{13}=1$, $a_{23}=0$ and $a_{33}=1$. Thus our answer is

$$\mathbf{A}=\begin{bmatrix}-1&0&1\\2&1&0\\1&-1&1\end{bmatrix}.$$

As a check we can carry out the matrix multiplication and verify that we obtain the given right-hand side.

8. Since the entries of $\mathbf{A}+\mathbf{B}$ are $a_{ij}+b_{ij}$ and the entries of $\mathbf{B}+\mathbf{A}$ are $b_{ij}+a_{ij}$, that $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$ follows from the commutativity of addition of real numbers.

10. **a)** This product is a 3×5 matrix.
b) This is not defined since the number of columns of $\mathbf{B}$ does not equal the number of rows of $\mathbf{A}$.
c) This product is a 3×4 matrix.
d) This is not defined since the number of columns of $\mathbf{C}$ does not equal the number of rows of $\mathbf{A}$.
e) This is not defined since the number of columns of $\mathbf{B}$ does not equal the number of rows of $\mathbf{C}$.
f) This product is a 4×5 matrix.

12. We use the definition of matrix addition and multiplication. All summations here are from 1 to k.
a) $(\mathbf{A}+\mathbf{B})\mathbf{C}=\left[\sum(a_{iq}+b_{iq})c_{qj}\right]=\left[\sum a_{iq}c_{qj}+\sum b_{iq}c_{qj}\right]=\mathbf{AC}+\mathbf{BC}$
b) $\mathbf{C}(\mathbf{A}+\mathbf{B})=\left[\sum c_{iq}(a_{qj}+b_{qj})\right]=\left[\sum c_{iq}a_{qj}+\sum c_{iq}b_{qj}\right]=\mathbf{CA}+\mathbf{CB}$

14. Let $\mathbf{A}$ and $\mathbf{B}$ be two diagonal $n\times n$ matrices. Let $\mathbf{C}=[c_{ij}]$ be the product $\mathbf{AB}$. From the definition of matrix multiplication, $c_{ij}=\sum a_{iq}b_{qj}$. Now all the terms a_{iq} in this expression are 0 except for $q=i$, so $c_{ij}=a_{ii}b_{ij}$. But $b_{ij}=0$ unless $i=j$, so the only nonzero entries of $\mathbf{C}$ are the diagonal entries $c_{ii}=a_{ii}b_{ii}$.

16. The $(i,j)^{\text{th}}$ entry of $(\mathbf{A}^t)^t$ is the $(j,i)^{\text{th}}$ entry of $\mathbf{A}^t$, which is the $(i,j)^{\text{th}}$ entry of $\mathbf{A}$.

18. We need to multiply these two matrices together in both directions and check that both products are $\mathbf{I}_3$. Indeed, they are.

20. **a)** Using Exercise 19, noting that $ad-bc=-5$, we write down the inverse immediately:

$$\begin{bmatrix}-3/5&2/5\\1/5&1/5\end{bmatrix}.$$

b) We multiply to obtain $\mathbf{A}^2 = \begin{bmatrix} 3 & 4 \\ 2 & 11 \end{bmatrix}$ and then $\mathbf{A}^3 = \begin{bmatrix} 1 & 18 \\ 9 & 37 \end{bmatrix}$.

c) We multiply to obtain $(\mathbf{A}^{-1})^2 = \begin{bmatrix} 11/25 & -4/25 \\ -2/25 & 3/25 \end{bmatrix}$ and then $(\mathbf{A}^{-1})^3 = \begin{bmatrix} -37/125 & 18/125 \\ 9/125 & -1/125 \end{bmatrix}$.

d) Applying the method of Exercise 19 for obtaining inverses to the answer in part **(b)**, we obtain the answer in part **(c)**. Therefore $(\mathbf{A}^3)^{-1} = (\mathbf{A}^{-1})^3$.

22. A matrix is symmetric if and only if it equals its transpose. So let us compute the transpose of $\mathbf{AA}^t$ and see if we get this matrix back. Using Exercise 17b and then Exercise 16, we have $(\mathbf{AA}^t)^t = \big((\mathbf{A}^t)^t\big)\mathbf{A}^t = \mathbf{AA}^t$, as desired.

24. a) We simply note that under the given definitions of $\mathbf{A}$, $\mathbf{X}$, and $\mathbf{B}$, the definition of matrix multiplication is exactly the system of equations shown.

b) The given system is the matrix equation $\mathbf{AX} = \mathbf{B}$. If $\mathbf{A}$ is invertible with inverse $\mathbf{A}^{-1}$, then we can multiply both sides of this equation by $\mathbf{A}^{-1}$ to obtain $\mathbf{A}^{-1}\mathbf{AX} = \mathbf{A}^{-1}\mathbf{B}$. The left-hand side simplifies to $\mathbf{IX}$, however, by the definition of inverse, and this is simply $\mathbf{X}$. Thus the given system is equivalent to the system $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$, which obviously tells us exactly what $\mathbf{X}$ is (and therefore what all the values x_i are).

26. We follow the definitions.

a) $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ **b)** $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ **c)** $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

28. We follow the definition and obtain $\begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$.

30. a) $\mathbf{A} \vee \mathbf{A} = [a_{ij} \vee a_{ij}] = [a_{ij}] = \mathbf{A}$ **b)** $\mathbf{A} \wedge \mathbf{A} = [a_{ij} \wedge a_{ij}] = [a_{ij}] = \mathbf{A}$

32. a) $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} = [(a_{ij} \vee b_{ij}) \vee c_{ij}] = [a_{ij} \vee (b_{ij} \vee c_{ij})] = \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$

b) This is identical to part **(a)**, with $\wedge$ replacing $\vee$.

34. Since the i^{th} row of $\mathbf{I}$ consists of all 0's except for a 1 in the $(i,i)^{\text{th}}$ position, we have $\mathbf{I} \odot \mathbf{A} = [(0 \wedge a_{1j}) \vee \cdots \vee (1 \wedge a_{ij}) \vee \cdots \vee (0 \wedge a_{nj})] = [a_{ij}] = \mathbf{A}$. Similarly, since the j^{th} column of $\mathbf{I}$ consists of all 0's except for a 1 in the $(j,j)^{\text{th}}$ position, we have $\mathbf{A} \odot \mathbf{I} = [(a_{i1} \wedge 0) \vee \cdots \vee (a_{ij} \wedge 1) \vee \cdots \vee (a_{in} \wedge 0)] = [a_{ij}] = \mathbf{A}$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 2

2. We are given that $A \subseteq B$. We want to prove that the power set of A is a subset of the power set of B, which means that if $C \subseteq A$ then $C \subseteq B$. But this follows directly from Exercise 17 in Section 2.1.

4. a) **Z** **b)** $\emptyset$ **c)** **O** **d)** **E**

6. If $A \subseteq B$, then every element in A is also in B, so clearly $A \cap B = A$. Conversely, if $A \cap B = A$, then every element of A must also be in $A \cap B$, and hence in B. Therefore $A \subseteq B$.

8. This identity is true, so we must show that every element in the left-hand side is also an element in the right-hand side and conversely. Let $x \in (A - B) - C$. Then $x \in A - B$ but $x \notin C$. This means that $x \in A$, but $x \notin B$ and $x \notin C$. Therefore $x \in A - C$, and therefore $x \in (A - C) - B$. The converse is proved in exactly the same way.

10. The inequality follows from the obvious fact that $A \cap B \subseteq A \cup B$. Equality can hold only if there are no elements in either A or B that are not in both A and B, and this can happen only if $A = B$.

12. Since $\overline{A} \cap \overline{B} = \overline{(A \cup B)}$, we are asked to show that $|\overline{(A \cup B)}| = |U| - \big(|A| + |B| - |A \cap B|\big)$. This follows immediately from the facts that $|\overline{X}| = |U| - |X|$ (which is clear from the definitions) and (see the discussion following Example 5 in Section 2.2) that $|A \cup B| = |A| + |B| - |A \cap B|$.

14. Define a function $g : f(S) \to S$ by choosing, for each element x in $f(S)$, an element $g(x) \in S$ such that $f(g(x)) = x$. Clearly g is one-to-one, so $|f(S)| \le |S|$. Note that we do not need the hypothesis that A and B are finite.

16. **a)** We are given that f is one-to-one, and we must show that S_f is one-to-one. So suppose that $X_1 \ne X_2$, where these are subsets of A. We have to show that $S_f(X_1) \ne S_f(X_2)$. Without loss of generality there is an element $a \in X_1 - X_2$. This means that $f(a) \in S_f(X_1)$. If $f(a)$ were also an element of $S_f(X_2)$, then we would need an element $a' \in X_2$ such that $f(a') = f(a)$. But since f is one-to-one, this forces $a' = a$, which is impossible, because $a \notin X_2$. Therefore $f(a) \in S_f(X_1) - S_f(X_2)$, so $S_f(X_1) \ne S_f(X_2)$.

b) We are given that f is onto, and we must show that S_f is onto. So suppose that $Y \subseteq B$. We have to find $X \subseteq A$ such that $S_f(X) = Y$. Let $X = \{\, x \in A \mid f(x) \in Y \,\}$. We claim that $S_f(X) = Y$. Clearly $S_f(X) \subseteq Y$. To see that $Y \subseteq S_f(X)$, suppose that $b \in Y$. Then because f is onto, there is some $a \in A$ such that $f(a) = b$. By our definition of X, $a \in X$. Therefore by definition $b \in S_f(X)$.

c) We are given that f is onto, and we must show that $S_{f^{-1}}$ is one-to-one. So suppose that $Y_1 \ne Y_2$, where these are subsets of B. We have to show that $S_{f^{-1}}(Y_1) \ne S_{f^{-1}}(Y_2)$. Without loss of generality there is an element $b \in Y_1 - Y_2$. Because f is onto, there is an $a \in A$ such that $f(a) = b$. Therefore $a \in S_{f^{-1}}(Y_1)$. But we also know that $a \notin S_{f^{-1}}(Y_2)$, because if a were an element of $S_{f^{-1}}(Y_2)$, then we would have $b = f(a) \in Y_2$, contrary to our choice of b. The existence of this a shows that $S_{f^{-1}}(Y_1) \ne S_{f^{-1}}(Y_2)$.

d) We are given that f is one-to-one, and we must show that $S_{f^{-1}}$ is onto. So suppose that $X \subseteq A$. We have to find $Y \subseteq B$ such that $S_{f^{-1}}(Y) = X$. Let $Y = S_f(X)$. In other words, $Y = \{\, f(x) \mid x \in X \,\}$. We must show that $S_{f^{-1}}(Y) = X$, which means that we must show that $\{\, u \in A \mid f(u) \in \{\, f(x) \mid x \in X \,\}\,\} = X$ (we changed the dummy variable to u for clarity). That the right-hand side is a subset of the left-hand side is immediate, because if $u \in X$, then $f(u)$ is an $f(x)$ for some $x \in X$. Conversely, suppose that u is in the left-hand side. Thus $f(u) = f(x_0)$ for some $x_0 \in X$. But because f is one-to-one, we know that $u = x_0$; that is $u \in X$.

e) This follows immediately from the earlier parts, because to be a one-to-one correspondence means to be one-to-one and onto.

18. If n is even , then $n/2$ is an integer, so $\lceil n/2\rceil + \lfloor n/2\rfloor = (n/2) + (n/2) = n$. If n is odd, then $\lceil n/2\rceil = (n+1)/2$ and $\lfloor n/2\rfloor = (n-1)/2$, so again the sum is n.

20. This is certainly true if either x or y is an integer, since then this equation is equivalent to the identity (4b) in Table 1 of Section 2.3. Otherwise, write x and y in terms of their integer and fractional parts: $x = n + \epsilon$ and $y = m + \delta$, where $n = \lfloor x\rfloor$, $0 < \epsilon < 1$, $m = \lfloor y\rfloor$, and $0 < \delta < 1$. If $\delta + \epsilon > 1$, then the equation is true, since both sides equal $m + n + 2$; if $\delta + \epsilon \le 1$, then the equation is false, since the left-hand side equals $m + n + 1$, but the right-hand side equals $m + n + 2$. To summarize: the equation is true if and only if either at least one of x and y is an integer or the sum of the fractional parts of x and y exceeds 1.

22. The values of the floor and ceiling function will depend on whether their arguments are integral or not. So there seem to be two cases here. First let us suppose that n is even. Then $n/2$ is an integer, and $n^2/4$ is also an integer, so the equation is a simple algebraic fact. The second case is harder. Suppose that n is odd, say $n = 2k+1$. Then $n/2 = k + \frac{1}{2}$. Therefore the left-hand side gives us $k(k+1) = k^2 + k$, since we have to round down for the first factor and round up for the second. What about the right-hand side? $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$, so $n^2/4 = k^2 + k + \frac{1}{4}$. Therefore the floor function gives us $k^2 + k$, and the proof is completed.

24. Since we are dividing by 4, let us write $x = 4n - k$, where $0 \le k < 4$. In other words, write x in terms of how much it is less than the smallest multiple of 4 not less than it. There are three cases. If $k = 0$, then x is already a multiple of 4, so both sides equal n. If $0 < k \le 2$, then $\lfloor x/2 \rfloor = 2n - 1$, so the left-hand side is $\lfloor n - \frac{1}{2} \rfloor = n - 1$. Of course the right-hand side is $n - 1$ as well, so again the two sides agree. Finally, suppose that $2 < k < 4$. Then $\lfloor x/2 \rfloor = 2n - 2$, and the left-hand side is $\lfloor n - 1 \rfloor = n - 1$; of course the right-hand side is still $n - 1$, as well. Since we proved that the two sides are equal in all cases, the proof is complete.

26. If x is an integer, then of course the two sides are identical. So suppose that $x = k + \epsilon$, where k is an integer and ϵ is a real number with $0 < \epsilon < 1$. Then the values of the left-hand side, which is $\lfloor (k+n)/m \rfloor$, and the right-hand side, which is $\lfloor (k+n+\epsilon)/m \rfloor$, are the same, since adding a number strictly between 0 and 1 to the numerator of a fraction whose numerator and denominator are integers cannot cause the fraction to reach the next higher integer value (the numerator cannot reach the next multiple of m).

28. **a)** $1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, 36, 38, 47, 48, 53, 57, 62, 69$

b) Suppose there were only a finite set of Ulam numbers, say $u_1 < u_2 < \cdots < u_n$. Then it is clear that $u_{n-1} + u_n$ can be written uniquely as the sum of two distinct Ulam numbers, so this is an Ulam number larger than u_n, a contradiction. Therefore there are an infinite number of Ulam numbers.

30. If we work at this long enough, we might notice that each term after the first three is the sum of the previous three terms. With this rule the next four terms will be 169, 311, 572, 1052. One way to use the power of technology here is to submit the given sequence to The On-Line Encyclopedia of Integer Sequences (`oeis.org`).

32. We know that the set of rational numbers is countable. If the set of irrational numbers were also countable, then the union of these two sets would also be countable by Theorem 1 in Section 2.5. But their union, the set of real numbers, is known to be uncountable. This contradiction tells us that the set of irrational numbers is not countable.

34. A finite subset of $\mathbf{Z}^+$ has a largest element and therefore is a subset of $\{1, 2, 3, \ldots, n\}$ for some positive integer n. Let S_n be the set of subsets of $\{1, 2, 3, \ldots, n\}$. It is finite and therefore countable; in fact $|S_n| = 2^n$. The set of all finite subsets of $\mathbf{Z}^+$ is the union $\bigcup_{n=1}^{\infty} S_n$. Being a countable union of countable sets, it is countable by Exercise 27 in Section 2.5.

36. This follows immediately from Exercise 35, because $\mathbf{C}$ can be identified with $\mathbf{R} \times \mathbf{R}$ by sending the complex number $a + bi$, where a and b are real numbers, to the ordered pair (a, b).

38. Since $\mathbf{A}$ is the matrix defined by $a_{ii} = c$ and $a_{ij} = 0$ for $i \ne j$, it is easy to see from the definition of multiplication that $\mathbf{AB}$ and $\mathbf{BA}$ are both the same as $\mathbf{B}$ except that every entry has been multiplied by c. Therefore these two matrices are equal.

40. We simply need to show that the alleged inverse of $\mathbf{AB}$ has the correct defining property—that its product with $\mathbf{AB}$ (on either side) is the identity. Thus we compute

$$(\mathbf{AB})(\mathbf{B}^{-1}\mathbf{A}^{-1}) = \mathbf{A}(\mathbf{BB}^{-1})\mathbf{A}^{-1} = \mathbf{AIA}^{-1} = \mathbf{AA}^{-1} = \mathbf{I},$$

and similarly $(\mathbf{B}^{-1}\mathbf{A}^{-1})(\mathbf{AB}) = \mathbf{I}$. Therefore $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$. (Note that the indicated matrix multiplications were all defined, since the hypotheses implied that both $\mathbf{A}$ and $\mathbf{B}$ were $n \times n$ matrices for some (and the same) n.)

CHAPTER 3
Algorithms

SECTION 3.1 Algorithms

2. a) This procedure is not finite, since execution of the **while** loop continues forever.

b) This procedure is not effective, because the step $m := 1/n$ cannot be performed when $n = 0$, which will eventually be the case.

c) This procedure lacks definiteness, since the value of i is never set.

d) This procedure lacks definiteness, since the statement does not tell whether x is to be set equal to a or to b.

4. Set the answer to be $-\infty$. For i going from 1 through $n-1$, compute the value of the $(i+1)^{\text{st}}$ element in the list minus the i^{th} element in the list. If this is larger than the answer, reset the answer to be this value.

6. We need to go through the list and count the negative entries.

```
procedure negatives(a_1, a_2, ..., a_n : integers)
k := 0
for i := 1 to n
        if a_i < 0 then k := k + 1
return k {the number of negative integers in the list}
```

8. This is similar to Exercise 7, modified to keep track of the largest even integer we encounter.

```
procedure largest even location(a_1, a_2, ..., a_n : integers)
k := 0
largest := −∞
for i := 1 to n
        if (a_i is even and a_i > largest) then
                k := i
                largest := a_i
return k {the desired location (or 0 if there are no evens)}
```

10. We assume that if the input $x = 0$, then $n > 0$, since otherwise x^n is not defined. In our procedure, we let $m = |n|$ and compute x^m in the obvious way. Then if n is negative, we replace the answer by its reciprocal.

```
procedure power(x : real number, n : integer)
m := |n|
power := 1
for i := 1 to m
        power := power · x
if n < 0 then power := 1/power
return power { power = x^n }
```

12. Four assignment statements are needed, one for each of the variables and a temporary assignment to get started so that we do not lose one of the original values.

$temp := x$
$x := y$
$y := z$
$z := temp$

14. **a)** With linear search we start at the beginning of the list, and compare 7 successively with 1, 3, 4, 5, 6, 8, 9, and 11. When we come to the end of the list and still have not found 7, we conclude that it is not in the list.

b) We begin the search on the entire list, with $i = 1$ and $j = n = 8$. We set $m := 4$ and compare 7 to the fourth element of the list. Since $7 > 5$, we next restrict the search to the second half of the list, with $i = 5$ and $j = 8$. This time we set $m := 6$ and compare 7 to the sixth element of the list. Since $7 \not> 8$, we next restrict ourselves to the first half of the second half of the list, with $i = 5$ and $j = 6$. This time we set $m := 5$, and compare 7 to the fifth element. Since $7 > 6$, we now restrict ourselves to the portion of the list between $i = 6$ and $j = 6$. Since at this point $i \not< j$, we exit the loop. Since the sixth element of the list is not equal to 7, we conclude that 7 is not in the list.

16. We let *min* be the smallest element found so far. At the end, it is the smallest element, since we update it as necessary as we scan through the list.

```
procedure smallest(a_1, a_2, ..., a_n : natural numbers)
min := a_1
for i := 2 to n
        if a_i < min then min := a_i
return min {the smallest integer among the input}
```

18. This is similar to Exercise 17.

```
procedure last smallest(a_1, a_2, ..., a_n : integers)
min := a_1
location := 1
for i := 2 to n
        if min ≥ a_i then
                min := a_i
                location := i
return location {the location of the last occurrence of the smallest element in the list}
```

20. We just combine procedures for finding the largest and smallest elements.

```
procedure smallest and largest(a_1, a_2, ..., a_n : integers)
min := a_1
max := a_1
for i := 2 to n
        if a_i < min then min := a_i
        if a_i > max then max := a_i
{ min is the smallest integer among the input, and max is the largest}
```

22. We assume that the input is a sequence of symbols, a_1, a_2, ..., a_n, each of which is either a letter or a blank. We build up the longest word in *word*; its length is *length*. We denote the empty word by λ.

```
procedure longest word(a_1, a_2, ..., a_n : symbols)
maxlength := 0
maxword := λ
i := 1
while i ≤ n
        word := λ
        length := 0
        while a_i ≠ blank and i ≤ n
                length := length + 1
                word := concatenation of word and a_i
                i := i + 1
        if length > max then
                maxlength := length
                maxword := word
        i := i + 1
return maxword {the longest word in the sentence}
```

24. This is similar to Exercise 23. We let the array *hit* keep track of which elements of the codomain B have already been found to be images of elements of the domain A. When we find an element that has already been hit being hit again, we conclude that the function is not one-to-one.

```
procedure one_one(f : function, a_1, a_2, ..., a_n, b_1, b_2, ..., b_m : integers)
for i := 1 to m
        hit(b_i) := 0
one_one := true
for j := 1 to n
        if hit(f(a_j)) = 0 then hit(f(a_j)) := 1
        else one_one := false
return one_one
```

26. There are two changes. First, we need to test $x = a_m$ (right after the computation of m) and take appropriate action if equality holds (what we do is set i and j both to be m). Second, if $x \not> a_m$, then instead of setting j equal to m, we can set j equal to $m-1$. The advantages are that this allows the size of the "half" of the list being looked at to shrink slightly faster, and it allows us to stop essentially as soon as we have found the element we are looking for.

28. This could be thought of as just doing two iterations of binary search at once. We compare the sought-after element to the middle element in the still-active portion of the list, and then to the middle element of either the top half or the bottom half. This will restrict the subsequent search to one of four sublists, each about one-quarter the size of the previous list. We need to stop when the list has length three or less and make explicit checks. Here is the pseudocode.

procedure *tetrary search*(x : integer, $a_1, a_2, \ldots, a_n$: increasing integers)
$i := 1$
$j := n$
while $i < j - 2$
    $l := \lfloor (i+j)/4 \rfloor$
    $m := \lfloor (i+j)/2 \rfloor$
    $u := \lfloor 3(i+j)/4 \rfloor$
    if $x > a_m$ **then if** $x \le a_u$ **then**
            $i := m + 1$
            $j := u$
        else $i := u + 1$
    else if $x > a_l$ **then**
            $i := l + 1$
            $j := m$
        else $j := l$
if $x = a_i$ **then** *location* $:= i$
else if $x = a_j$ **then** *location* $:= j$
else if $x = a_{\lfloor (i+j)/2 \rfloor}$ **then** *location* $:= \lfloor (i+j)/2 \rfloor$
else *location* $:= 0$
return *location* {the subscript of the term equal to x (0 if not found)}

30. The following algorithm will find all modes in the sequence and put them into a list L. At each point in the execution of this algorithm, *modecount* is the number of occurrences of the elements found to occur most often so far (the elements in L). Whenever a more frequently occurring element is found (the main inner loop), *modecount* and L are updated; whenever an element is found with this same count, it is added to L.

procedure *find all modes*($a_1, a_2, \ldots, a_n$: nondecreasing integers)
modecount $:= 0$
$i := 1$
while $i \le n$
    value $:= a_i$
    count $:= 1$
    while $i \le n$ and $a_i =$ *value*
        count $:=$ *count* $+ 1$
        $i := i + 1$
    if *count* $>$ *modecount* **then**
        modecount $:=$ *count*
        set L to consist just of *value*
    else if *count* $=$ *modecount* **then** add *value* to L
return L {the list of all the values occurring most often, namely *modecount* times}

32. The following algorithm will find all terms of a finite sequence of integers that are greater than the sum of all the previous terms. We put them into a list L, but one could just as easily have them printed out, if that were desired. It might be more useful to put the *indices* of these terms into L, rather than the terms themselves (i.e., their values), but we take the former approach for variety. As usual, the empty list is considered to have sum 0, so the first term in the sequence is included in L if and only if it positive.

procedure *find all biggies*($a_1, a_2, \ldots, a_n$: integers)
set L to be the empty list
sum $:= 0$
$i := 1$
while $i \le n$
    if $a_i >$ *sum* **then** append a_i to L
    sum $:=$ *sum* $+ a_i$
    $i := i + 1$
return L {the list of all the values that exceed the sum of all the previous terms in the sequence}

34. There are five passes through the list. After one pass the list reads $2, 3, 1, 5, 4, 6$, since the 6 is compared and moved at each stage. During the next pass, the 2 and the 3 are not interchanged, but the 3 and the 1 are, as are the 5 and the 4, yielding $2, 1, 3, 4, 5, 6$. On the third pass, the 2 and the 1 are interchanged, yielding $1, 2, 3, 4, 5, 6$. There are two more passes, but no further interchanges are made, since the list is now in order.

36. The procedure is the same as that given in the solution to Exercise 35. We will exhibit the lists obtained after each step, with all the lists obtained during one pass on the same line.

$dfkmab$, $dfkmab$, $dfkmab$, $dfkamb$, $dfkabm$
$dfkabm$, $dfkabm$, $dfakbm$, $dfabkm$
$dfabkm$, $dafbkm$, $dabfkm$
$adbfkm$, $abdfkm$
$abdfkm$

38. We start with $6, 2, 3, 1, 5, 4$. The first step inserts 2 correctly into the sorted list 6, producing $2, 6, 3, 1, 5, 4$. Next 3 is inserted into $2, 6$, and the list reads $2, 3, 6, 1, 5, 4$. Next 1 is inserted into $2, 3, 6$, and the list reads $1, 2, 3, 6, 5, 4$. Next 5 is inserted into $1, 2, 3, 6$, and the list reads $1, 2, 3, 5, 6, 4$. Finally 4 is inserted into $1, 2, 3, 5, 6$, and the list reads $1, 2, 3, 4, 5, 6$. At each insertion, the element to be inserted is compared with the elements already sorted, starting from the beginning, until its correct spot is found, and then the previously sorted elements beyond that spot are each moved one position toward the back of the list.

40. We start with d, f, k, m, a, b. The first step inserts f correctly into the sorted list d, producing no change. Similarly, no change results when k and m are inserted into the sorted lists d, f and d, f, k, respectively. Next a is inserted into d, f, k, m, and the list reads a, d, f, k, m, b. Finally b is inserted into a, d, f, k, m, and the list reads a, b, d, f, k, m. At each insertion, the element to be inserted is compared with the elements already sorted, starting from the beginning, until its correct spot is found, and then the previously sorted elements beyond that spot are each moved one position toward the back of the list.

42. We let *minspot* be the place at which the minimum remaining element is found. After we find it on the i^{th} pass, we just have to interchange the elements in location *minspot* and location i.

```
procedure selection(a_1, a_2, ..., a_n)
for i := 1 to n − 1
        minspot := i
        for j := i + 1 to n
                if a_j < a_minspot then minspot := j
        interchange a_minspot and a_i
{the list is now in order}
```

44. We carry out the binary search algorithm given as Algorithm 3 in this section, except that we replace the final check with **if** $x < a_i$ **then** *location* $:= i$ **else** *location* $:= i + 1$.

46. We are counting just the comparisons of the numbers in the list, not any comparisons needed for the bookkeeping in the **for** loop. The second element in the list must be compared only with the first (in other words, when $j = 2$ in Algorithm 5, i takes the values 1 before we drop out of the **while** loop). Similarly, the third element must be compared only with the first. We continue in this way, until finally the n^{th} element must be compared only with the first. So the total number of comparisons is $n - 1$. This is the best case for insertion sort in terms of the number of comparisons, but moving the elements to do the insertions requires much more effort.

48. For the insertion sort, one comparison is needed to find the correct location of the 4, one for the 3, four for the 8, one for the 1, four for the 5, and two for the 2. This is a total of 13 comparisons. For the binary insertion sort, one comparison is needed to find the correct location of the 4, two for the 3, two for the 8, three for the 1, three for the 5, and four for the 2. This is a total of 15 comparisons. If the list were long (and not almost in decreasing order to begin with), we would use many fewer comparisons using binary insertion sort. The reason that the answer came out "wrong" here is that the list is so short that the binary search was not efficient.

50. **a)** This is essentially the same as Algorithm 5, but working from the other end. However, we can do the moving while we do the searching for the correct insertion spot, so the pseudocode has only one section.

procedure *backward insertion sort*$(a_1, a_2, \ldots, a_n$: real numbers with $n \geq 2)$
for $j := 2$ **to** n
  $m := a_j$
  $i := j - 1$
  while $(m < a_i$ and $i > 0)$
    $a_{i+1} := a_i$
    $i := i - 1$
  $a_{i+1} := m$
$\{a_1, a_2, \ldots, a_n$ are sorted$\}$

b) On the first pass the 2 is compared to the 3 and found to be less, so the 3 moves to the right. We have reached the beginning of the list, so the loop terminates ($i = 0$), and the 2 is inserted, yielding $2, 3, 4, 5, 1, 6$. On the second pass the 4 is compared to the 3, and since $4 > 3$, the **while** loop terminates and nothing changes. Similarly, no changes are made as the 5 is inserted. One the fourth pass, the 1 is compared all the way to the front of the list, with each element moving toward the back of the list as the comparisons go on, and finally the 1 is inserted in its correct position, yielding $1, 2, 3, 4, 5, 6$. The final pass produces no change.

c) Only one comparison is used during each pass, since the condition $m < a_i$ is immediately false. Therefore a total of $n - 1$ comparisons are used.

d) The j^{th} pass requires $j - 1$ comparisons of elements, so the total number of comparisons is $1 + 2 + \cdots + (n-1) = n(n-1)/2$.

52. In each case we use as many quarters as we can, then as many dimes to achieve the remaining amount, then as many nickels, then as many pennies.

a) The algorithm uses the maximum number of quarters, three, leaving 12 cents. It then uses the maximum number of dimes (one) and nickels (none), before using two pennies.

b) one quarter, leaving 24 cents, then two dimes, leaving 4 cents, then four pennies

c) three quarters, leaving 24 cents, then two dimes, leaving 4 cents, then four pennies

d) one quarter, leaving 8 cents, then one nickel and three pennies

54. **a)** The algorithm uses the maximum number of quarters, three, leaving 12 cents. It then uses the maximum number of dimes (one), and then two pennies. The greedy algorithm worked, since we got the same answer as in Exercise 52.

b) one quarter, leaving 24 cents, then two dimes, leaving 4 cents, then four pennies (the greedy algorithm worked, since we got the same answer as in Exercise 52)

c) three quarters, leaving 24 cents, then two dimes, leaving 4 cents, then four pennies (the greedy algorithm worked, since we got the same answer as in Exercise 52)

d) The greedy algorithm would have us use one quarter, leaving 8 cents, then eight pennies, a total of nine coins. However, we could have used three dimes and three pennies, a total of six coins. Thus the greedy algorithm is not correct for this set of coins.

56. One approach is to come up with an example in which using the 12-cent coin before using dimes or nickels would be inefficient. A dime and a nickel together are worth 15 cents, but the greedy algorithm would have us use four coins (a 12-cent coin and three pennies) rather than two. An alternative example would be 29 cents, in which case the greedy algorithm would use a quarter and four pennies, but we could have done better using two 12-cent coins and a nickel.

58. Here is one counterexample, using 11 talks. Suppose the start and end times are as follows: A 1–3, B 3–5, C 5–7, D 7–9, E 2–4, F 2–4, G 2–4, H 4–6, J 6–8, K 6–8, L 6–8. The optimal schedule is talks A, B, C, and D. However, the talk with the fewest overlaps with other talks is H, which overlaps only with B and C (all the other talks overlap with three or four other talks). However, once we have decided to include talk H, we can no longer schedule four talks, so this algorithm will not produce an optimum solution.

60. If all the men get their first choices, then the matching will be stable, because no man will be part of an unstable pair, preferring another woman to his assigned partner. Thus the pairing (m_1w_3, m_2w_1, m_3w_2) is stable. Similarly, if all the women get their first choices, then the matching will be stable, because no woman will be part of an unstable pair, preferring another man to her assigned partner. Thus the matching (m_1w_1, m_2w_2, m_3w_3) is stable. Two of the other four matchings pair m_1 with w_2, and this cannot be stable, because m_1 prefers w_1 to w_2, his assigned partner, and w_1 prefers m_1 to her assigned partner, whoever it is, because m_1 is her favorite. In a similar way, the matching (m_1w_3, m_2w_2, m_3w_1) is unstable because of the unhappy unmatched pair m_3w_3 (each preferring the other to his or her assigned partner). Finally, the matching (m_1w_1, m_2w_3, m_3w_2) is stable, because each couple has a reason not to break up: w_1 got her favorite and so is content, m_3 got his favorite and so is content, and w_3 only prefers m_3 to her assigned partner but he doesn't prefer her to his assigned partner.

62. The algorithm given in the solution to Exercise 61 will terminate if at some point at the conclusion of the **while** loop, no man is rejected. If this happens, then that must mean that each man has one and only one proposal pending with some woman, because he proposed to only one in that round, and since he was not rejected, his proposal is the only one pending with that woman. It follows that at that point there are s pending proposals, one from each man, so each woman will be matched with a unique man. Finally, we argue that there are at most s^2 iterations of the **while** loop, so the algorithm must terminate. Indeed, if at the conclusion of the **while** loop rejected men remain, then some man must have been rejected, because no man is marked as rejected at the conclusion of the proposal phase (first **for** loop inside the **while** loop). If a man is rejected, then his rejection list grows. Thus each pass through the **while** loop, at least one more of the s^2 possible rejections will have been recorded, unless the loop is about to terminate. (Actually there will be fewer than s^2 iterations, because no man is rejected by the woman with whom he is eventually matched.) There is one more subtlety we need to address. Is it possible that at the end of some round, some man has been rejected by *every* woman and therefore the algorithm cannot continue? We claim not. If at the end of some round some man has been rejected by every woman, then every woman has one pending proposal at the completion of that round (from someone she likes better—otherwise she never would have rejected that poor man), and of course these proposals are all from different men because a man proposes only once in each round. That means s men have pending proposals, so in fact our poor universally-rejected man does not exist.

64. Suppose we had a program S that could tell whether a program with its given input ever prints the digit 1. Here is an algorithm for solving the halting problem: Given a program P and its input I, construct a program P', which is just like P but never prints anything (even if P did print something) except that if and when it is about to halt, it prints a 1 and halts. Then P halts on an input if and only if P' ever prints a 1 on that same input. Feed P' and I to S, and that will tell us whether or not P halts on input I. Since we know that the halting problem is in fact not solvable, we have a contradiction. Therefore no such program S exists.

66. The decision problem has no input. The answer is either always yes or always no, depending on whether or not the specific program with its specific input halts or not. In the former case, the decision procedure is "say yes," and in the latter case it is "say no."

SECTION 3.2 The Growth of Functions

2. Note that the choices of C and k witnesses are not unique.

a) Yes, since $17x + 11 \leq 17x + x = 18x \leq 18x^2$ for all $x > 11$. The witnesses are $C = 18$ and $k = 11$.

b) Yes, since $x^2 + 1000 \leq x^2 + x^2 = 2x^2$ for all $x > \sqrt{1000}$. The witnesses are $C = 2$ and $k = \sqrt{1000}$.

c) Yes, since $x \log x \leq x \cdot x = x^2$ for all x in the domain of the function. (The fact that $\log x < x$ for all x follows from the fact that $x < 2^x$ for all x, which can be seen by looking at the graphs of these two functions.) The witnesses are $C = 1$ and $k = 0$.

d) No. If there were a constant C such that $x^4/2 \leq Cx^2$ for sufficiently large x, then we would have $C \geq x^2/2$. This is clearly impossible for a constant to satisfy.

e) No. If 2^x were $O(x^2)$, then the fraction $2^x/x^2$ would have to be bounded above by some constant C. It can be shown that in fact $2^x > x^3$ for all $x \geq 10$ (using mathematical induction—see Section 5.1—or calculus), so $2^x/x^2 \geq x^3/x^2 = x$ for large x, which is certainly not less than or equal to C.

f) Yes, since $\lfloor x \rfloor \lceil x \rceil \leq x(x+1) \leq x \cdot 2x = 2x^2$ for all $x > 1$. The witnesses are $C = 2$ and $k = 1$.

4. If $x > 5$, then $2^x + 17 \leq 2^x + 2^x = 2 \cdot 2^x \leq 2 \cdot 3^x$. This shows that $2^x + 17$ is $O(3^x)$ (the witnesses are $C = 2$ and $k = 5$).

6. We can use the following inequalities, valid for all $x > 1$ (note that making the denominator of a fraction smaller makes the fraction larger).

$$\frac{x^3 + 2x}{2x + 1} \leq \frac{x^3 + 2x^3}{2x} = \frac{3}{2}x^2$$

This proves the desired statement, with witnesses $k = 1$ and $C = 3/2$.

8. a) Since $x^3 \log x$ is not $O(x^3)$ (because the $\log x$ factor grows without bound as x increases), $n = 3$ is too small. On the other hand, certainly $\log x$ grows more slowly than x, so $2x^2 + x^3 \log x \leq 2x^4 + x^4 = 3x^4$. Therefore $n = 4$ is the answer, with $C = 3$ and $k = 0$.

b) The $(\log x)^4$ is insignificant compared to the x^5 term, so the answer is $n = 5$. Formally we can take $C = 4$ and $k = 1$ as witnesses.

c) For large x, this fraction is fairly close to 1. (This can be seen by dividing numerator and denominator by x^4.) Therefore we can take $n = 0$; in other words, this function is $O(x^0) = O(1)$. Note that $n = -1$ will not do, since a number close to 1 is not less than a constant times n^{-1} for large n. Formally we can write $f(x) \leq 3x^4/x^4 = 3$ for all $x > 1$, so witnesses are $C = 3$ and $k = 1$.

d) This is similar to the previous part, but this time $n = -1$ will do, since for large x, $f(x) \approx 1/x$. Formally we can write $f(x) \leq 6x^3/x^3 = 6$ for all $x > 1$, so witnesses are $C = 6$ and $k = 1$.

10. Since $x^3 \leq x^4$ for all $x > 1$, we know that x^3 is $O(x^4)$ (witnesses $C = 1$ and $k = 1$). On the other hand, if $x^4 \leq Cx^3$, then (dividing by x^3) $x \leq C$. Since this latter condition cannot hold for all large x, no matter what the value of the constant C, we conclude that x^4 is not $O(x^3)$.

12. We showed that $x \log x$ is $O(x^2)$ in Exercise 2c. To show that x^2 is not $O(x \log x)$ it is enough to show that $x^2/(x \log x)$ is unbounded. This is the same as showing that $x/\log x$ is unbounded. First let us note that $\log x < \sqrt{x}$ for all $x > 16$. This can be seen by looking at the graphs of these functions, or by calculus. Therefore the fraction $x/\log x$ is greater than $x/\sqrt{x} = \sqrt{x}$ for all $x > 16$, and this clearly is not bounded.

14. **a)** No, by an argument similar to Exercise 10.
b) Yes, since $x^3 \le x^3$ for all x (witnesses $C = 1$, $k = 0$).
c) Yes, since $x^3 \le x^2 + x^3$ for all x (witnesses $C = 1$, $k = 0$).
d) Yes, since $x^3 \le x^2 + x^4$ for all x (witnesses $C = 1$, $k = 0$).
e) Yes, since $x^3 \le 2^x \le 3^x$ for all $x > 10$ (see Exercise 2e). Thus we have witnesses $C = 1$ and $k = 10$.
f) Yes, since $x^3 \le 2 \cdot (x^3/2)$ for all x (witnesses $C = 2$, $k = 0$).

16. The given information says that $|f(x)| \le C|x|$ for all $x > k$, where C and k are particular constants. Let k' be the larger of k and 1. Then since $|x| \le |x^2|$ for all $x > 1$, we have $|f(x)| \le C|x^2|$ for all $x > k'$, as desired.

18. $1^k + 2^k + \cdots + n^k \le n^k + n^k + \cdots + n^k = n \cdot n^k = n^{k+1}$

20. They both are. For the first we have $\log(n+1) < \log(2n) = \log n + \log 2 < 2\log n$ for $n > 2$. For the second one we have $\log(n^2+1) < \log(2n^2) = 2\log n + \log 2 < 3\log n$ for $n > 2$.

22. The ordering is straightforward when we remember that exponential functions grow faster than polynomial functions, that factorial functions grow faster still, and that logarithmic functions grow very slowly. The order is $(\log n)^3$, $\sqrt{n}\log n$, $n^{99} + n^{98}$, n^{100}, 1.5^n, 10^n, $(n!)^2$.

24. The first algorithm uses fewer operations because $n^2 2^n$ is $O(n!)$ but $n!$ is not $O(n^2 2^n)$. In fact, the second function overtakes the first function for good at $n = 8$, when $8^2 \cdot 2^8 = 16{,}384$ and $8! = 40{,}320$.

26. The approach in these problems is to pick out the most rapidly growing term in each sum and discard the rest (including the multiplicative constants).
a) This is $O(n^3 \cdot \log n + \log n \cdot n^3)$, which is the same as $O(n^3 \cdot \log n)$.
b) Since 2^n dominates n^2, and 3^n dominates n^3, this is $O(2^n \cdot 3^n) = O(6^n)$.
c) The dominant terms in the two factors are n^n and $n!$, respectively. Therefore this is $O(n^n n!)$.

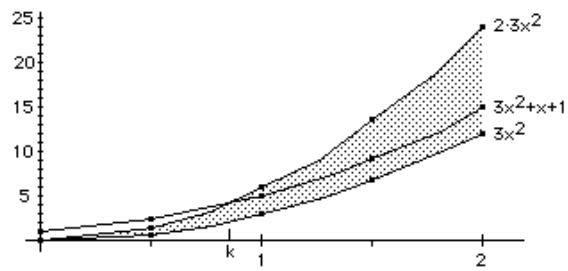
28. We can use the following rule of thumb to determine what simple big-Theta function to use: throw away all the lower order terms (those that don't grow as fast as other terms) and all constant coefficients.
a) This function is $\Theta(1)$, so it is not $\Theta(x)$, since 1 (or 10) grows more slowly than x. To be precise, x is not $O(10)$. For the same reason, this function is not $\Omega(x)$.
b) This function is $\Theta(x)$; we can ignore the " $+\,7$" since it is a lower order term, and we can ignore the coefficient. Of course, since $f(x)$ is $\Theta(x)$, it is also $\Omega(x)$.
c) This function grows faster than x. Therefore $f(x)$ is not $\Theta(x)$ but it is $\Omega(x)$.
d) This function grows more slowly than x. Therefore $f(x)$ is not $\Theta(x)$ or $\Omega(x)$.
e) This function has values that are, for all practical purposes, equal to x (certainly $\lfloor x \rfloor$ is always between $x/2$ and x, for $x > 2$), so it is $\Theta(x)$ and therefore also $\Omega(x)$.
f) As in part **(e)** this function has values that are, for all practical purposes, equal to $x/2$, so it is $\Theta(x)$ and therefore also $\Omega(x)$.

30. **a)** This follows from the fact that for all $x > 7$, $x \le 3x + 7 \le 4x$.
b) For large x, clearly $x^2 \le 2x^2 + x - 7$. On the other hand, for $x \ge 1$ we have $2x^2 + x - 7 \le 3x^2$.
c) For $x > 2$ we certainly have $\lfloor x + \frac{1}{2} \rfloor \le 2x$ and also $x \le 2\lfloor x + \frac{1}{2} \rfloor$.
d) For $x > 2$, $\log(x^2+1) \le \log(2x^2) = 1 + 2\log x \le 3\log x$ (recall that log means $\log_2$). On the other hand, since $x < x^2 + 1$ for all positive x, we have $\log x \le \log(x^2+1)$.
e) This follows from the fact that $\log_{10} x = C(\log_2 x)$, where $C = 1/\log_2 10$.

32. We just need to look at the definitions. To say that $f(x)$ is $O(g(x))$ means that there are constants C and k such that $|f(x)| \leq C|g(x)|$ for all $x > k$. Note that without loss of generality we may take C and k to be positive. To say that $g(x)$ is $\Omega(f(x))$ is to say that there are positive constants C' and k' such that $|g(x)| \geq C'|f(x)|$ for all $x > k$. These are saying exactly the same thing if we set $C' = 1/C$ and $k' = k$.

34. **a)** By Exercise 31 we have to show that $3x^2 + x + 1$ is $O(3x^2)$ and that $3x^2$ is $O(3x^2 + x + 1)$. The latter is trivial, since $3x^2 \leq 3x^2 + x + 1$ for $x > 0$. The former is almost as trivial, since $3x^2 + x + 1 \leq 3x^2 + 3x^2 = 2 \cdot 3x^2$ for all $x > 1$. What we have shown is that $1 \cdot 3x^2 \leq 3x^2 + x + 1 \leq 2 \cdot 3x^2$ for all $x > 1$; in other words, $C_1 = 1$ and $C_2 = 2$ in Exercise 33.

b) The following picture shows that graph of $3x^2 + x + 1$ falls in the shaded region between the graph of $3x^2$ and the graph of $2 \cdot 3x^2$ for all $x > 1$.



36. Looking at the definition, we see that to say that $f(x)$ is $\Omega(1)$ means that $|f(x)| \geq C$ when $x > k$, for some positive constants k and C. In other words, $f(x)$ keeps at least a certain distance away from 0 for large enough x. For example, $1/x$ is not $\Omega(1)$, since it gets arbitrary close to 0; but $(x-2)(x-10)$ is $\Omega(1)$, since $f(x) \geq 9$ for $x > 11$.

38. The n^{th} odd positive integer is $2n-1$. Thus each of the first n odd positive integers is at most $2n$. Therefore their product is at most $(2n)^n$, so one answer is $O\big((2n)^n\big)$. Of course other answers are possible as well.

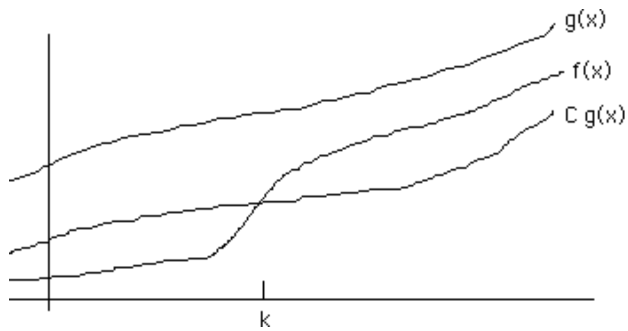
40. This follows from the fact that $\log_b x$ and $\log_a x$ are the same except for a multiplicative constant, namely $d = \log_b a$. Thus if $f(x) \leq C \log_b x$, then $f(x) \leq Cd \log_a x$.

42. This does not follow. Let $f(x) = 2x$ and $g(x) = x$. Then $f(x)$ is $O(g(x))$. Now $2^{f(x)} = 2^{2x} = 4^x$, and $2^{g(x)} = 2^x$, and 4^x is not $O(2^x)$. Indeed, $4^x/2^x = 2^x$, so the ratio grows without bound as x grows—it is not bounded by a constant.

44. The definition of "$f(x)$ is $\Theta(g(x))$" is that $f(x)$ is both $O(g(x))$ and $\Omega(g(x))$. That means that there are positive constants C_1, k_1, C_2, and k_2 such that $|f(x)| \leq C_2|g(x)|$ for all $x > k_2$ and $|f(x)| \geq C_1|g(x)|$ for all $x > k_1$. Similarly, we have that there are positive constants C_1', k_1', C_2', and k_2' such that $|g(x)| \leq C_2'|h(x)|$ for all $x > k_2'$ and $|g(x)| \geq C_1'|h(x)|$ for all $x > k_1'$. We can combine these inequalities to obtain $|f(x)| \leq C_2C_2'|h(x)|$ for all $x > \max(k_2, k_2')$ and $|f(x)| \geq C_1C_1'|h(x)|$ for all $x > \max(k_1, k_1')$. This means that $f(x)$ is $\Theta(h(x))$.

46. The definitions tell us that there are positive constants C_1, k_1, C_2, and k_2 such that $|f_1(x)| \leq C_2|g_1(x)|$ for all $x > k_2$ and $|f_1(x)| \geq C_1|g_1(x)|$ for all $x > k_1$, and that there are positive constants C_1', k_1', C_2', and k_2' such that $|f_2(x)| \leq C_2'|g_2(x)|$ for all $x > k_2'$ and $|f_2(x)| \geq C_1'|g_2(x)|$ for all $x > k_1'$. We can multiply these inequalities to obtain $|f_1(x)f_2(x)| \leq C_2C_2'|g_1(x)g_2(x)|$ for all $x > \max(k_2, k_2')$ and $|f_1(x)f_2(x)| \geq C_1C_1'|g_1(x)g_2(x)|$ for all $x > \max(k_1, k_1')$. This means that $f_1(x)f_2(x)$ is $\Theta(g_1(x)g_2(x))$.

48. Typically C will be less than 1. From some point onward to the right ($x > k$), the graph of $f(x)$ must be above the graph of $g(x)$ after the latter has been scaled down by the factor C. Note that $f(x)$ does not have to be larger than $g(x)$ itself.



50. We need to show inequalities both ways. First, we show that $|f(x)| \le Cx^n$ for all $x \ge 1$, as follows, noting that $x^i \le x^n$ for such values of x whenever $i < n$. We have the following inequalities, where M is the largest of the absolute values of the coefficients and C is $M(n+1)$:

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\ &\le |a_n|x^n + |a_{n-1}|x^{n-1} + \cdots + |a_1|x + |a_0| \\ &\le |a_n|x^n + |a_{n-1}|x^n + \cdots + |a_1|x^n + |a_0|x^n \\ &\le Mx^n + Mx^n + \cdots + Mx^n + Mx^n = Cx^n \end{aligned}$$

For the other direction, which is a little messier, let k be chosen larger than 1 and larger than $2nm/|a_n|$, where m is the largest of the absolute values of the a_i's for $i < n$. Then each a_{n-i}/x^i will be smaller than $|a_n|/2n$ in absolute value for all $x > k$. Now we have for all $x > k$,

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\ &= x^n \left| a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n} \right| \\ &\ge x^n \, |a_n/2| \,, \end{aligned}$$

as desired.

52. We just make the analogous change in the definition of big-Omega that was made in the definition of big-O: there exist positive constants C, k_1, and k_2 such that $|f(x,y)| \ge C|g(x,y)|$ for all $x > k_1$ and $y > k_2$.

54. For all values of x and y greater than 1, each term of the given expression is greater than x^3y^3, so the entire expression is greater than x^3y^3. In other words, we take $C = k_1 = k_2 = 1$ in the definition given in Exercise 52.

56. For all positive values of x and y, we know that $\lceil xy \rceil \ge xy$ by definition (since the ceiling function value cannot be less than the argument). Thus $\lceil xy \rceil$ is $\Omega(xy)$ from the definition, taking $C = 1$ and $k_1 = k_2 = 0$. In fact, $\lceil xy \rceil$ is also $O(xy)$ (and therefore $\Theta(xy)$); this is easy to see since $\lceil xy \rceil \le (x+1)(y+1) \le (2x)(2y) = 4xy$ for all x and y greater than 1.

58. It suffices to show that

$$\lim_{n\to\infty} \frac{(\log_b n)^c}{n^d} = 0\,,$$

where we think of n as a continuous variable. Because both numerator and denominator approach ∞, we apply L'Hôpital's rule and evaluate

$$\lim_{n\to\infty} \frac{c(\log_b n)^{c-1}}{d \cdot n^d \cdot \ln b}\,.$$

At this point, if $c \le 1$, then the limit is 0. Otherwise we again have an expression of type ∞/∞, so we apply L'Hôpital's rule once more, obtaining

$$\lim_{n\to\infty} \frac{c(c-1)(\log_b n)^{c-2}}{d^2 \cdot n^d \cdot (\ln b)^2}\,.$$

If $c \le 2$, then the limit is 0; if not, we repeat. Eventually the exponent on $\log_b n$ becomes nonpositive and we conclude that the limit is 0, as desired.

60. If suffices to look at $\lim_{n\to\infty} b^n/c^n = (b/c)^n$ and $\lim_{n\to\infty} c^n/b^n = (c/b)^n$. Because $c > b > 1$, we have $0 < b/c < 1$ and $c/b > 1$, so the former limit is clearly 0 and the latter limit is clearly ∞.

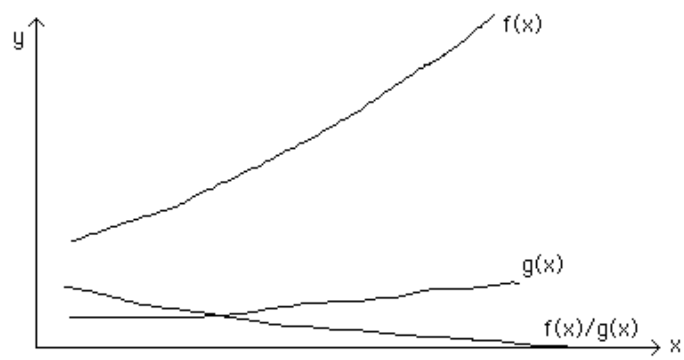
62. a) Under the hypotheses,

$$\lim_{x\to\infty} \frac{cf(x)}{g(x)} = c \lim_{x\to\infty} \frac{f(x)}{g(x)} = c \cdot 0 = 0\,.$$

b) Under the hypotheses,

$$\lim_{x\to\infty} \frac{f_1(x)+f_2(x)}{g(x)} = \lim_{x\to\infty} \frac{f_1(x)}{g(x)} + \lim_{x\to\infty} \frac{f_2(x)}{g(x)} = 0+0 = 0\,.$$

64. The behaviors of f and g alone are not really at issue; what is important is whether $f(x)/g(x)$ approaches 0 as $x \to \infty$. Thus, as shown in the picture, it might happen that the graphs of f and g rise, but f increases enough more rapidly than g so that the ratio gets small. In the picture, we see that $f(x)/g(x)$ is asymptotic to the x-axis.



66. No. Let $f(x) = x$ and $g(x) = x^2$. Then clearly $f(x)$ is $o(g(x))$, but the ratio of the logs of the absolute values is the constant 2, and 2 does not approach 0. Therefore it is not the case in this example that $\log|f(x)|$ is $o(\log|g(x)|)$.

68. This follows from the fact that the limit of $f(x)/g(x)$ is 0 in this case, as can be most easily seen by dividing numerator and denominator by x^n (the numerator then is bounded and the absolute value of the denominator grows without bound as $x \to \infty$).

70. Since $f(x) = 1/x$ is a decreasing function which has the value $1/x$ at $x = j$, it is clear that $1/j < 1/x$ throughout the interval from $j-1$ to j. Summing over all the intervals for $j = 2, 3, \ldots, n$, and noting that the definite integral is the area under the curve, we obtain the inequality in the hint. Therefore

$$H_n = 1 + \sum_{j=2}^{n} \frac{1}{j} < 1 + \int_1^n \frac{1}{x}\,dx = 1 + \ln n = 1 + C\log n \le 2C\log n$$

for $n > 2$, where $C = \log e$.

72. By Example 6, $\log n!$ is $O(n \log n)$. By Exercise 71, $n \log n$ is $O(\log n!)$. Thus by Exercise 31, $\log n!$ is $\Theta(n \log n)$.

74. In each case we need to evaluate the limit of $f(x)/g(x)$ as $x \to \infty$. If it equals 1, then f and g are asymptotic; otherwise (including the case in which the limit does not exist) they are not. Most of these are straightforward applications of algebra, elementary notions about limits, or L'Hôpital's rule.

a) $\displaystyle\lim_{x\to\infty} \frac{x^2+3x+7}{x^2+10} = \lim_{x\to\infty} \frac{1+3/x+7/x^2}{1+10/x^2} = 1$, so f and g are asymptotic.

b) $\displaystyle\lim_{x\to\infty} \frac{x^2 \log x}{x^3} = \lim_{x\to\infty} \frac{\log x}{x} = \lim_{x\to\infty} \frac{1}{x \cdot \ln 2} = 0$ (we used L'Hôpital's rule for the last equivalence), so f and g are not asymptotic.

c) Here $f(x)$ is dominated by its leading term, x^4, and $g(x)$ is a polynomial of degree 4, so the ratio approaches 1, the ratio of the leading coefficients, as in part **(a)**. Therefore f and g are asymptotic.

d) Here f and g are polynomials of degree 12, so the ratio approaches 1, the ratio of the leading coefficients, as in part **(a)**. Therefore f and g are asymptotic.

SECTION 3.3 Complexity of Algorithms

2. The statement $t := t + i + j$ is executed n^2 times, so the number of operations is $O(n^2)$. (Specifically, $2n^2$ additions are used, not counting any arithmetic needed for bookkeeping in the loops.)

4. The value of i keeps doubling, so the loop terminates after k iterations as soon as $2^k > n$. The value of k that makes this happen is $O(\log n)$, because $2^{\log n} = n$. Within the loop there are two additions or multiplications, so the answer to the question is $O(\log n)$.

6. a) We can sort the first four elements by copying the steps in Algorithm 5 but only up to $j = 4$.

```
procedure sort four(a_1, a_2, ..., a_n : real numbers)
for j := 2 to 4
        i := 1
        while a_j > a_i
                i := i + 1
        m := a_j
        for k := 0 to j - i - 1
                a_{j-k} := a_{j-k-1}
        a_i := m
```

b) Only a (small) finite number of steps are performed here, regardless of the length of the list, so this algorithm has complexity $O(1)$.

8. If we successively square k times, then we have computed x^{2^k}. Thus we can compute x^{2^k} with only k multiplications, rather than the $2^k - 1$ multiplications that the naive algorithm would require, so this method is much more efficient.

10. a) By the way that $S - 1$ is defined, it is clear that $S \land (S - 1)$ is the same as S except that the rightmost 1 bit has been changed to a 0. Thus we add 1 to *count* for every one bit (since we stop as soon as $S = 0$, i.e., as soon as S consists of just 0 bits).

b) Obviously the number of bitwise *AND* operations is equal to the final value of *count*, i.e., the number of one bits in S.

12. a) There are three loops, each nested inside the next. The outer loop is executed n times, the middle loop is executed at most n times, and the inner loop is executed at most n times. Therefore the number of times the one statement inside the inner loop is executed is at most n^3. This statement requires one comparison, so the total number of comparisons is $O(n^3)$.

b) We follow the hint, not worrying about the fractions that might result from roundoff when dividing by 2 or 4 (these don't affect the final answer in big-Omega terms). The outer loop is executed at least $n/4$ times, once for each value of i from 1 to $n/4$ (we ignore the rest of the values of i). The middle loop is executed at least $n/4$ times, once for each value of j from $3n/4$ to n. The inner loop for these values of i and j is executed at least $(3n/4) - (n/4) = n/2$ times. Therefore the statement within the inner loop, which requires one comparison, is executed at least $(n/4)(n/4)(n/2) = n/32$ times, which is $\Omega(n^3)$. The second statement follows by definition.

14. a) Initially $y := 3$. For $i = 1$ we set y to $3 \cdot 2 + 1 = 7$. For $i = 2$ we set y to $7 \cdot 2 + 1 = 15$, and we are done.

b) There is one multiplication and one addition for each of the n passes through the loop, so there are n multiplications and n additions in all.

16. If each bit operation takes 10^{-11} second, then we can carry out 10^{11} bit operations per second, and therefore $60 \cdot 60 \cdot 24 \cdot 10^{11} = 864 \cdot 10^{13}$ bit operations per day. Therefore in each case we want to solve the inequality $f(n) = 864 \cdot 10^{13}$ for n and round down to an integer. Obviously a calculator or computer software will come in handy here.

a) If $\log n = 864 \cdot 10^{13}$, then $n = 2^{864 \cdot 10^{13}}$, which is an unfathomably huge number.

b) If $1000n = 864 \cdot 10^{13}$, then $n = 864 \cdot 10^{10}$, which is still a very large number.

c) If $n^2 = 864 \cdot 10^{13}$, then $n = \sqrt{864 \cdot 10^{13}}$, which works out to about $9.3 \cdot 10^7$.

d) If $1000n^2 = 864 \cdot 10^{13}$, then $n = \sqrt{864 \cdot 10^{10}}$, which works out to about $2.9 \cdot 10^6$.

e) If $n^3 = 864 \cdot 10^{13}$, then $n = (864 \cdot 10^{13})^{1/3}$, which works out to about $2.1 \cdot 10^5$.

f) If $2^n = 864 \cdot 10^{13}$, then $n = \lfloor \log(864 \cdot 10^{13}) \rfloor = 52$. (Remember, we are taking log to the base 2.)

g) If $2^{2n} = 864 \cdot 10^{13}$, then $n = \lfloor \log(864 \cdot 10^{13})/2 \rfloor = 26$.

h) If $2^{2^n} = 864 \cdot 10^{13}$, then $n = \lfloor \log(\log(864 \cdot 10^{13})) \rfloor = 5$.

18. We are asked to compute $(2n^2 + 2^n) \cdot 10^{-9}$ for each of these values of n. When appropriate, we change the units from seconds to some larger unit of time.

a) 1.224×10^{-6} seconds **b)** approximately 1.05×10^{-3} seconds

c) approximately 1.13×10^6 seconds, which is about 13 days (nonstop)

d) approximately 1.27×10^{21} seconds, which is about 4×10^{13} years (nonstop)

20. In each case we want to compare the function evaluated at $2n$ to the function evaluated at n. The most desirable form of the comparison (subtraction or division) will vary.

a) Notice that

$$\log\log 2n - \log\log n = \log \frac{\log 2 + \log n}{\log n} = \log \frac{1 + \log n}{\log n}.$$

If n is large, the fraction in this expression is approximately equal to 1, and therefore the expression is approximately equal to 0. In other words, hardly any extra time is required. For example, in going from $n = 1024$ to $n = 2048$, the number of extra milliseconds is $\log 11/10 \approx 0.14$.

b) Here we have $\log 2n - \log n = \log \frac{2n}{n} = \log 2 = 1$. One extra millisecond is required, independent of n.

c) This time it makes more sense to use a ratio comparison, rather than a difference comparison. Because $100(2n)/(100n) = 2$, we conclude that twice as much time is needed for the larger problem.

d) The controlling factor here is n, rather than $\log n$, so again we look at the ratio:

$$\frac{2n\log(2n)}{n\log n} = 2\cdot\frac{1+\log n}{\log n}$$

For large n, the final fraction is approximately 1, so we can say that the time required for $2n$ is a bit more than twice what it is for n.

e) Because $(2n)^2/n^2 = 4$, we see that four times as much time is required for the larger problem.

f) Because $(3n)^2/n^2 = 9$, we see that nine times as much time is required for the larger problem.

g) The relevant ratio is $2^{2n}/2^n$, which equals 2^n. If n is large, then this is a huge number. For example, in going from $n = 10$ to $n = 20$, the number of milliseconds increases over 1000-fold.

22. a) The number of comparisons does not depend on the values of a_1 through a_n. Exactly $2n-1$ comparisons are used, as was determined in Example 1. In other words, the best case performance is $O(n)$.

b) In the best case $x = a_1$. We saw in Example 4 that three comparisons are used in that case. The best case performance, then, is $O(1)$.

c) It is hard to give an exact answer, since it depends on the binary representation of the number n, among other things. In any case, the best case performance is really not much different from the worst case performance, namely $O(\log n)$, since the list is essentially cut in half at each iteration, and the algorithm does not stop until the list has only one element left in it.

24. a) In order to find the maximum element of a list of n elements, we need to make at least $n-1$ comparisons, one to rule out each of the other elements. Since Algorithm 1 in Section 3.1 used just this number (not counting bookkeeping), it is optimal.

b) Linear search is not optimal, since we found that binary search was more efficient. This assumes that we can be given the list already sorted into increasing order.

26. We will count comparisons of elements in the list to x. (This ignores comparisons of subscripts, but since we are only interested in a big-O analysis, no harm is done.) Furthermore, we will assume that the number of elements in the list is a power of 4, say $n = 4^k$. Just as in the case of binary search, we need to determine the maximum number of times the **while** loop is iterated. Each pass through the loop cuts the number of elements still being considered (those whose subscripts are from i to j) by a factor of 4. Therefore after k iterations, the active portion of the list will have length 1; that is, we will have $i = j$. The loop terminates at this point. Now each iteration of the loop requires two comparisons in the worst case (one with a_m and one with either a_l or a_u). Three more comparisons are needed at the end. Therefore the number of comparisons is $2k+3$, which is $O(k)$. But $k = \log_4 n$, which is $O(\log n)$ since logarithms to different bases differ only by multiplicative constants, so the time complexity of this algorithm (in all cases, not just the worst case) is $O(\log n)$.

28. The algorithm we gave for finding all the modes essentially just goes through the list once, doing a little bookkeeping at each step. In particular, between any two successive executions of the statement $i := i+1$ there are at most about eight operations (such as comparing *count* with *modecount*, or reinitializing *value*). Therefore at most about $8n$ steps are done in all, so the time complexity in all cases is $O(n)$.

30. The algorithm we gave is clearly of linear time complexity, i.e., $O(n)$, since we were able to keep updating the sum of previous terms, rather than recomputing it each time. This applies in all cases, not just the worst case.

32. The algorithm read through the list once and did a bounded amount of work on each term. Looked at another way, only a bounded amount of work was done between increments of j in the algorithm given in the solution. Thus the complexity is $O(n)$.

34. It takes $n-1$ comparisons to find the least element in the list, then $n-2$ comparisons to find the least element among the remaining elements, and so on. Thus the total number of comparisons is $(n-1)+(n-2)+\cdots+2+1 = n(n-1)/2$, which is $O(n^2)$.

36. Each iteration (determining whether we can use a coin of a given denomination) takes a bounded amount of time, and there are at most n iterations, since each iteration decreases the number of cents remaining. Therefore there are $O(n)$ comparisons.

38. First we sort the talks by earliest end time; this takes $O(n \log n)$ time if there are n talks. We initialize a variable *opentime* to be 0; it will be updated whenever we schedule another talk to be the time at which that talk ends. Next we go through the list of talks in order, and for each talk we see whether its start time does not precede *opentime* (we already know that its ending time exceeds *opentime*). If so, then we schedule that talk and update *opentime* to be its ending time. This all takes $O(1)$ time per talk, so the entire process after the initial sort has time complexity $O(n)$. Combining this with the initial sort, we get an overall time complexity of $O(n \log n)$.

40. **a)** The bubble sort algorithm uses about $n^2/2$ comparisons for a list of length n, and $(2n)^2/2 = 2n^2$ comparisons for a list of length $2n$. Therefore the number of comparisons goes up by a factor of 4.

b) The analysis is the same as for bubble sort.

c) The analysis is the same as for bubble sort.

d) The binary insertion sort algorithm uses about $Cn \log n$ comparisons for a list of length n, where C is a constant. Therefore it uses about $C \cdot 2n \log 2n = C \cdot 2n \log 2 + C \cdot 2n \log n = C \cdot 2n + C \cdot 2n \log n$ comparisons for a list of length $2n$. Therefore the number of comparisons increases by about a factor of 2 (for large n, the first term is small compared to the second and can be ignored).

42. In an $n \times n$ upper-triangular matrix, all entries a_{ij} are zero unless $i \le j$. Therefore we can store such matrices in about half the space that would be required to store an ordinary $n \times n$ matrix. In implementing something like Algorithm 1, then, we need only do the computations for those values of the indices that can produce nonzero entries. The following algorithm does this. We follow the usual notation: $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$.

```
procedure triangular matrix multiplication(A, B : upper-triangular matrices)
for i := 1 to n
    for j := i to n {since we want j ≥ i}
        c_ij := 0
        for k := i to j {the only relevant part}
            c_ij := c_ij + a_ik b_kj
{the upper-triangular matrix C = [c_ij] is the product of A and B}
```

44. We have two choices: $(\mathbf{AB})\mathbf{C}$ or $\mathbf{A}(\mathbf{BC})$. For the first choice, it takes $3 \cdot 9 \cdot 4 = 144$ multiplications to form the 3×4 matrix $\mathbf{AB}$, and then $3 \cdot 4 \cdot 2 = 24$ multiplications to get the final answer, for a total of 168 multiplications. For the second choice, it takes $9 \cdot 4 \cdot 2 = 72$ multiplications to form the 9×2 matrix $\mathbf{BC}$, and then $3 \cdot 9 \cdot 2 = 54$ multiplications to get the final answer, for a total of 126 multiplications. The second method uses fewer multiplications and so is the better choice.

46. **a)** Let us call the text $s_1 s_2 \ldots s_n$ and call the target $t_1 t_2 \ldots t_m$. We want to find the first occurrence of $t_1 t_2 \ldots t_m$ in $s_1 s_2 \ldots s_n$, which means we want to find the smallest $k \ge 0$ such that $t_1 t_2 \ldots t_m = s_{k+1} s_{k+2} \ldots s_{k+m}$. The brute force algorithm will try $k = 0, 1, \ldots, n-m$ and for each such k check whether $t_j = s_{k+j}$ for $j = 1, 2, \ldots, m$. If these equalities all hold, the value $k+1$ will be returned (that's where the target starts); otherwise 0 will be returned (as a code for "not there").

b) The implementation is straightforward:

procedure *findit*($s_1 s_2 \ldots s_n, t_1 t_2 \ldots t_m$: strings)
found := **false**
$k := 0$
while $k \le m - n$ and not *found*
    found := **true**
    for $j := i$ **to** m
        if $t_j \ne s_{k+j}$ **then** *found* := **false**
    if *found* **then return** $k + 1$ {location of start of target $t_1 t_2 \ldots t_m$ in text $s_1 s_2 \ldots s_n$ }
return 0 {target $t_1 t_2 \ldots t_m$ does not appear in text $s_1 s_2 \ldots s_n$ }

c) Because of the nested loops, the worst-case time complexity will be $O(mn)$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 3

2. a) We need to keep track of the first and second largest elements as we go along, updating as we look at the elements in the list.

procedure *toptwo*($a_1, a_2, \ldots, a_n$: integers)
largest := a_1
second := $-\infty$
for $i := 2$ **to** n
    if $a_i >$ *second* **then** *second* := a_i
    if $a_i >$ *largest* **then**
        second := *largest*
        largest := a_i
{ *largest* and *second* are the required values}

b) The loop is executed $n - 1$ times, and there are 2 comparisons per iteration. Therefore (ignoring bookkeeping) there are $2n - 2$ comparisons.

4. a) Since the list is in order, all the occurrences appear consecutively. Thus the output of our algorithm will be a pair of numbers, *first* and *last*, which give the first location and the last location of occurrences of x, respectively. All the numbers between *first* and *last* are also locations of appearances of x. If there are no appearances of x, we set *first* equal to 0 to indicate this fact.

procedure *all*($x, a_1, a_2, \ldots, a_n$: integers, with $a_1 \ge a_2 \ge \cdots \ge a_n$)
$i := 1$
while $i \le n$ and $a_i < x$
    $i := i + 1$
if $i = n + 1$ **then** *first* := 0
else if $a_i > x$ **then** *first* := 0
else
    first := i
    $i := i + 1$
    while $i \le n$ and $a_i = x$
        $i := i + 1$
    last := $i - 1$
{see above for the interpretation of the variables}

b) The number of comparisons depends on the data. Roughly speaking, in the worst case we have to go all the way through the list. This requires that x be compared with each of the elements, a total of n comparisons (not including bookkeeping). The situation is really a bit more complicated than this, but in any case the answer is $O(n)$.

6. **a)** We follow the instructions given. If n is odd then we start the loop at $i = 2$, and if n is even then we start the loop at $i = 3$. Within the loop, we compare the next two elements to see which is larger and which is smaller. The larger is possibly the new maximum, and the smaller is possibly the new minimum.

b)

```
procedure clever smallest and largest(a_1, a_2, ..., a_n : integers)
if n is odd then
        min := a_1
        max := a_1
else if a_1 < a_2 then
        min := a_1
        max := a_2
else
        min := a_2
        max := a_1
if n is odd then i := 2 else i := 3
while i < n
        if a_i < a_{i+1} then
                smaller := a_i
                bigger := a_{i+1}
        else
                smaller := a_{i+1}
                bigger := a_i
        if smaller < min then min := smaller
        if bigger > max then max := bigger
        i := i + 2
{ min is the smallest integer among the input, and max is the largest}
```

c) If n is even, then pairs of elements are compared (first with second, third with fourth, and so on), which accounts for $n/2$ comparisons, and there are an additional $2((n/2) - 1) = n - 2$ comparisons to determine whether to update *min* and *max*. This gives a total of $(3n - 4)/2$ comparisons. If n is odd, then there are $(n - 1)/2$ pairs to compare and $2((n - 1)/2) = n - 1$ comparisons for the updates, for a total of $(3n - 3)/2$. Note that in either case, this total is $\lceil 3n/2 \rceil - 2$ (see Exercise 7).

8. The naive approach would be to keep track of the largest element found so far and the second largest element found so far. Each new element is compared against the largest, and if it is smaller also compared against the second largest, and the "best-so-far" values are updated if necessary. This would require about $2n$ comparisons in all. We can do it more efficiently by taking Exercise 6 as a hint. If n is odd, set l to be the first element in the list, and set s to be $-\infty$. If n is even, set l to be the larger of the first two elements and s to be the smaller. At each stage, l will be the largest element seen so far, and s the second largest. Now consider the remaining elements two by two. Compare them and set a to be the larger and b the smaller. Compare a with l. If $a > l$, then a will be the new largest element seen so far, and the second largest element will be either l or b; compare them to find out which. If $a < l$, then l is still the largest element, and we can compare a and s to determine the second largest. Thus it takes only three comparisons for every pair of elements, rather than the four needed with the naive approach. The counting of comparisons is exactly the same as in Exercise 6: $\lceil 3n/2 \rceil - 2$.

10. Following the hint, we first sort the list and call the resulting sorted list $a_1, a_2, \ldots, a_n$. To find the last occurrence of a closest pair, we initialize *diff* to ∞ and then for i from 1 to $n - 1$ compute $a_{i+1} - a_i$. If this value is less than *diff*, then we reset *diff* to be this value and set k to equal i. Upon completion of this loop, a_k and a_{k+1} are a closest pair of integers in the list. Clearly the time complexity is $O(n \log n)$, the time needed for the sorting, because the rest of the procedure takes time $O(n)$.

12. We start with the solution to Exercise 37 in Section 3.1 and modify it to alternately examine the list from the front and from the back. The variables *front* and *back* will show what portion of the list still needs work. (After the k^{th} pass from front to back, we know that the final k elements are in their correct positions, and after the k^{th} pass from back to front, we know that the first k elements are in their correct positions.) The outer **if** statement takes care of changing directions each pass.

```
procedure shakersort(a_1, ..., a_n)
front := 1
back := n
still_interchanging := true
while front < back and still_interchanging
        if n + back + front is odd then {process from front to back}
                still_interchanging := false
                for j := front to back − 1
                        if a_j > a_{j+1} then
                                still_interchanging := true
                                interchange a_j and a_{j+1}
                back := back − 1
        else {process from back to front}
                still_interchanging := false
                for j := back down to front + 1
                        if a_{j−1} > a_j then
                                still_interchanging := true
                                interchange a_{j−1} and a_j
                front := front + 1
{ a_1, ..., a_n is in nondecreasing order}
```

14. Lists that are already in close to the correct order will have few items out of place. One pass through the shaker sort will then have a good chance of moving these items to their correct positions. If we are lucky, significantly fewer than $n-1$ passes through the list will be needed.

16. Since $8x^3 + 12x + 100\log x \le 8x^3 + 12x^3 + 100x^3 = 120x^3$ for all $x > 1$, the conclusion follows by definition.

18. This is a sum of n things, each of which is no larger than $2n^2$. Therefore the sum is $O(2n^3)$, or more simply, $O(n^3)$. This is the "best" possible answer.

20. Let us look at the ratio $n^n/n!$. We can write this as

$$\frac{n}{n}\cdot\frac{n}{n-1}\cdot\frac{n}{n-2}\cdots\frac{n}{2}\cdot\frac{n}{1}\,.$$

Each factor is greater than or equal to 1, and the last factor is n. Therefore the ratio is greater than or equal to n. In particular, it cannot be bounded above by a constant C. Therefore the defining condition for n^n being $O(n!)$ cannot be met.

22. By ignoring lower order terms, we see that the orders of these functions in simplest terms are 2^n, n^2, 4^n, $n!$, 3^n, and n^4, respectively. None of them is of the same order as any of the others.

24. We know that any power of a logarithmic functions grows more slowly than any power function (with power greater than 0), so such a value of n must exist. Begin by squaring both sides, to give $(\log n)^{2^{101}} < n$, and then because of the logarithm, let $n = 2^k$. This gives us $k^{2^{101}} < 2^k$. Taking logs of both sides gives $2^{101}\log k < k$. Letting $k = 2^m$ gives $2^{101}\cdot m < 2^m$. This is almost true when $m = 101$, but not quite; if we let $m = 108$, however, then the inequality is satisfied, because $2^7 > 108$. Thus our value of n is $2^{2^{108}}$, which is very big! Notice that there was not much wiggle room in our analysis, so something significantly smaller than this will not do.

26. The first five of these functions grow very rapidly, whereas the last four grow fairly slowly, so we can analyze each group separately. The value of n swamps the value of $\log n$ for large n, so among the last four, clearly $n^{3/2}$ is the fastest growing and $n^{4/3}(\log n)^2$ is next. The other two have a factor of n in common, so the issue is comparing $\log n \log\log n$ to $(\log n)^{3/2}$; because logs are much smaller than their argument, $\log\log n$ is much smaller than $\log n$, so the extra one-half power wins out. Therefore among these four, the desired order is $\log n \log\log n$, $(\log n)^{3/2}$, $n^{4/3}(\log n)^2$, $n^{3/2}$. We now turn to the large functions in the list and take the logarithm of each in order to make comparison easier: $100n$, n^2, $n!$, 2^n, and $(\log n)^2$. These are easily arranged in increasing big-O order, so our final answer is

$$\log n \log\log n, \quad (\log n)^{3/2}, \quad n^{4/3}(\log n)^2, \quad n^{3/2}, \quad n^{\log n}, \quad 2^{100n}, \quad 2^{n^2}, \quad 2^{2^n}, \quad 2^{n!}.$$

28. The greedy algorithm in this case will produce the base c expansion for the number of cents required (except that for amounts greater than or equal to c^{k+1}, the c^k coins must be used rather than nonexistent c^i coins for $i > k$). Since such expansions are unique if each digit (other than the digit in the c^k place) is less than c, the only other ways to make change would involve using c or more coins of a given denomination, and this would obviously not be minimal, since c coins of denomination c^i could be replaced by one coin of denomination c^{i+1}.

30. **a)** We follow the hint, first sorting the sequence into $a_1, a_2, \ldots, a_n$. We can then loop **for** $i := 1$ **to** $n-1$ and within that **for** $j := i+1$ **to** n and for each such pair (i,j) use binary search to determine whether $a_j - a_i$ is in the sorted sequence.

b) Recall that sorting can be done in $O(n \log n)$ time and that binary searching can be done in $O(\log n)$ time. Therefore the time inside the loops is $O(n^2 \log n)$, and the sorting adds nothing appreciable to this, so the efficiency is $O(n^2 \log n)$. This is better than the brute-force algorithm, which clearly takes time $\Omega(n^3)$.

32. We will prove this essentially by induction on the round in which the woman rejects the man under consideration. Suppose that the algorithm produces a matching that is not male optimal; in particular, suppose that Joe is not assigned the valid partner highest on his preference list. The way the algorithm works, Joe proposes first to his highest-ranked woman, say Rita. If she rejects him in the first round, it is because she prefers another man, say Sam, who has Rita as his first choice. This means that any matching in which Joe is married to Rita would not be stable, because Rita and Sam would each prefer each other to their spouses. Next suppose that Rita leaves Joe's proposal pending in the first round but rejects him in favor of Ken in the second round. The reason that Ken proposed to Rita in the second round is that he was rejected in the first round, which as we have seen means that there is no stable matching in which Ken is married to his first choice. If Joe and Rita were to be married, then Rita and Ken would form an unstable pair. Therefore again Rita is not a valid partner for Joe. We can continue with this argument through all the rounds and conclude that Joe in fact got his highest choice among valid partners: Anyone who rejected him would have been part of an unstable pair if she had married him.

It remains to prove that the deferred acceptance algorithm in which the men do the proposing is female pessimal, that each woman ends up with the valid partner ranking lowest on her preference list. Suppose that Jan is matched with Ken by the algorithm, but that Jan ranks Ken higher than she ranks Jerry. We must show that Jerry is not a valid partner. Suppose there were a stable matching in which Jan was married to Jerry. Because Ken got the highest ranked valid partner he could, in this hypothetical situation he would be married to someone he liked less than Jan. But then Jan and Ken would be an unstable pair. So no such matching exists.

34. This follows immediately from Exercise 32 because the roles of the sexes are reversed.

36. This exercise deals with a problem studied in the following paper: V. M. F. Dias, G. D. da Fonseca, C. M. H. de Figueiredo, and J. L. Szwarcfiter, "The stable marriage problem with restricted pairs," *Theoretical Computer Science* **306** (2003), 391–405. See that article for details, which are too complex to present here.

38. Consider the situation in Exercise 37. We saw there that it is possible to achieve a maximum lateness of 5. If we schedule the jobs in order of increasing slackness, then Job 4 will be scheduled fourth and finish at time 65. This will give it a lateness of 10, which gives a maximum lateness worse than the previous schedule.

40. Clearly we cannot gain by leaving any idle time, so we may assume that the jobs are scheduled back-to-back. Furthermore, suppose that at some point in time, say t_0, we have a choice between scheduling Job A, with time $t_{\rm A}$ and deadline $d_{\rm A}$, and Job B, with time $t_{\rm B}$ and deadline $d_{\rm B}$, such that $d_{\rm A} > d_{\rm B}$, one after the other. We claim that there is no advantage in scheduling Job A first. Indeed, the lateness of any job other than A or B is independent of the order in which we schedule these two jobs. Suppose we schedule A first. Then its lateness, if any, is $t_0 + t_{\rm A} - d_{\rm A}$. This value is clearly exceeded by the lateness (if any) of B, which is $t_0 + t_{\rm A} + t_{\rm B} - d_{\rm B}$. This latter value is also greater than both $t_0 + t_{\rm B} - d_{\rm B}$ (which is the lateness, if any, of B if we schedule B first) and $t_0 + t_{\rm A} + t_{\rm B} - d_{\rm A}$ (which is the lateness, if any, of A if we schedule B first). Therefore the possible contribution toward maximum lateness is always worse if we schedule A first. It now follows that we can always get a better or equal schedule (in terms of minimizing maximum lateness) if we swap any two jobs that are out of order in terms of deadlines. Therefore we get the best schedule by scheduling the jobs in order of increasing deadlines.

42. We can assign Job 1 and Job 4 to Processor 1 (load 10), Job 2 and Job 3 to Processor 2 (load 9), and Job 5 to Processor 3 (load 8), for a makespan of 10. This is best possible, because to achieve a makespan of 9, all three processors would have to have a load of 9, and this clearly cannot be achieved with the given running times.

44. In the pseudocode below, we have reduced the finding of the smallest load at a certain point to one statement; in practice, of course, this can be done by looping through all p processors and finding the one with smallest L_j (the current load). The input is as specified in the preamble.

```
procedure assign(p, t_1, t_2, ..., t_n)
for j := 1 to p
        L_j := 0
for i := 1 to n
        m := the value of j that minimizes L_j
        assign job i to processor m
        L_m := L_m + t_i
```

46. From Exercise 43 we know that the minimum makespan L satisfies two conditions: $L \ge \max_j t_j$ and $L \ge \frac{1}{p}\sum_{j=1}^{n} t_j$. Suppose processor i^* is the one that ends up with the maximum load using this greedy algorithm, and suppose job j^* is the last job to be assigned to processor i^*, giving it a total load of T_{i^*}. We must show that $T_{i^*} \le 2L$. Now at the point at which job j^* was assigned to processor i^*, its load was $T_{i^*} - t_{j^*}$, and this was the smallest load at that time, meaning that every processor at that time had load at least $T_{i^*} - t_{j^*}$. Adding up the loads on all p processors we get $\sum_{i=1}^{p} T_i \ge p(T_{i^*} - t_{j^*})$, where T_i is the load on processor i at that time. This is equivalent to $T_{i^*} - t_{j^*} \le \frac{1}{p}\sum_{i=1}^{p} T_i$. But $\sum_{i=1}^{p} T_i$ is the total load at that time, which is just the sum of the times of all the jobs considered so far, so it is less than or equal to $\sum_{j=1}^{n} t_j$. Combining this with the second inequality in the first sentence of this solution gives $T_{i^*} - t_{j^*} \le L$. It remains to figure in the contribution of job j^* to the load of processor i^*. By the first inequality in the first sentence of this solution, $t_{j^*} \le L$. Adding these two inequalities gives us $T_{i^*} \le 2L$, as desired.

CHAPTER 4
Number Theory and Cryptography

SECTION 4.1 Divisibility and Modular Arithmetic

2. **a)** $1 \mid a$ since $a = 1 \cdot a$. **b)** $a \mid 0$ since $0 = a \cdot 0$.

4. Suppose $a \mid b$, so that $b = at$ for some t, and $b \mid c$, so that $c = bs$ for some s. Then substituting the first equation into the second, we obtain $c = (at)s = a(ts)$. This means that $a \mid c$, as desired.

6. Under the hypotheses, we have $c = as$ and $d = bt$ for some s and t. Multiplying we obtain $cd = ab(st)$, which means that $ab \mid cd$, as desired.

8. The simplest counterexample is provided by $a = 4$ and $b = c = 2$.

10. In each case we can carry out the arithmetic on a calculator.
a) Since $8 \cdot 5 = 40$ and $44 - 40 = 4$, we have quotient 44 **div** $8 = 5$ and remainder 44 **mod** $8 = 4$.
b) Since $21 \cdot 37 = 777$, we have quotient 777 **div** $21 = 37$ and remainder 777 **mod** $21 = 0$.
c) As above, we can compute 123 **div** $19 = 6$ and 123 **mod** $19 = 9$. However, since the dividend is negative and the remainder is nonzero, the quotient is $-(6+1) = -7$ and the remainder is $19 - 9 = 10$. To check that -123 **div** $19 = -7$ and -123 **mod** $19 = 10$, we note that $-123 = (-7)(19) + 10$.
d) Since 1 **div** $23 = 0$ and 1 **mod** $23 = 1$, we have -1 **div** $23 = -1$ and -1 **mod** $23 = 22$.
e) Since 2002 **div** $87 = 23$ and 2002 **mod** $87 = 1$, we have -2002 **div** $87 = -24$ and 2002 **mod** $87 = 86$.
f) Clearly 0 **div** $17 = 0$ and 0 **mod** $17 = 0$.
g) We have 1234567 **div** $1001 = 1233$ and 1234567 **mod** $1001 = 334$.
h) Since 100 **div** $101 = 0$ and 100 **mod** $101 = 100$, we have -100 **div** $101 = -1$ and -100 **mod** $101 = 1$.

12. **a)** Because 100 **mod** $24 = 4$, the clock reads the same as 4 hours after 2:00, namely 6:00.
b) Essentially we are asked to compute $12 - 45$ **mod** $24 = -33$ **mod** $24 = -33 + 48$ **mod** $24 = 15$. The clock reads 15:00.
c) Because $168 \equiv 0 \pmod{24}$, the clock read 19:00.

14. This problem is equivalent to asking for the right-hand side **mod** 19. So we just do the arithmetic and compute the remainder upon division by 19.
a) $13 \cdot 11 = 143 \equiv 10 \pmod{19}$ **b)** $8 \cdot 3 = 24 \equiv 5 \pmod{19}$
c) $11 - 3 = 8 \pmod{19}$ **d)** $7 \cdot 11 + 3 \cdot 3 = 86 \equiv 10 \pmod{19}$
e) $2 \cdot 11^2 + 3 \cdot 3^2 = 269 \equiv 3 \pmod{19}$ **f)** $11^3 + 4 \cdot 3^3 = 1439 \equiv 14 \pmod{19}$

16. Assume that $a \equiv b \pmod{m}$. This means that $m \mid a - b$, say $a - b = mc$, so that $a = b + mc$. Now let us compute a **mod** m. We know that $b = qm + r$ for some nonnegative r less than m (namely, $r = b$ **mod** m). Therefore we can write $a = qm + r + mc = (q+c)m + r$. By definition this means that r must also equal a **mod** m. That is what we wanted to prove.

18. By Theorem 2 we have $a = dq + r$ with $0 \le r < d$. Dividing the equation by d we obtain $a/d = q + (r/d)$, with $0 \le (r/d) < 1$. Thus by definition it is clear that q is $\lfloor a/d \rfloor$. The original equation shows, of course, that $r = a - dq$, proving the second of the original statements.

20. In each case we just apply the division algorithm (carry out the division) to obtain the quotient and remainder, as in elementary school. However, if the dividend is negative, we must make sure to make the remainder positive, which may involve a quotient 1 less than might be expected.

a) Since $-17 = 2 \cdot (-9) + 1$, the remainder is 1. That is, -17 **mod** $2 = 1$. Note that we do not write $-17 = 2 \cdot (-8) - 1$, so -17 **mod** $2 \ne -1$.

b) Since $144 = 7 \cdot 20 + 4$, the remainder is 4. That is, 144 **mod** $7 = 4$.

c) Since $-101 = 13 \cdot (-8) + 3$, the remainder is 3. That is, -101 **mod** $13 = 3$. Note that we do not write $-101 = 13 \cdot (-7) - 10$; we can't have -101 **mod** $13 = -10$, because a **mod** b is always nonnegative.

d) Since $199 = 19 \cdot 10 + 9$, the remainder is 9. That is, 199 **mod** $19 = 9$.

22. In each case we do the division and report the quotient (a **div** m) and the remainder (a **mod** m). It is important to remember that the quotient needs to be rounded down, which means that if the dividend is negative, as in part **(a)**, the quotient is a number with a *larger* absolute value.

a) $111/99$ is between 1 and 2, so the quotient is -2 and the remainder is $-111-(-2)\cdot 99 = -111+198 = 87$.

b) $-9999/101 = -99$, so that is the quotient and the remainder is 0.

c) 10299 **div** $999 = 10$, 10299 **mod** $999 = 10299 - 10 \cdot 999 = 309$

d) 123456 **div** $1001 = 123$, 123456 **mod** $1001 = 333$

24. **a)** We can get into the desired range and stay within the same modular equivalence class by subtracting $2\cdot 23$, so the answer is $a = 43 - 46 = -3$.

b) $17 - 29 = -12$, so $a = -12$. **c)** $a = -11 + 5 \cdot 21 = 94$

26. Among the infinite set of correct answers are 4, 16, -8, 1204, and -7016360.

28. We just subtract 3 from the given number; the answer is "yes" if and only if the difference is divisible by 7.

a) $37 - 3$ **mod** $7 = 34$ **mod** $7 = 6 \ne 0$, so $37 \not\equiv 3 \pmod 7$.

b) $66 - 3$ **mod** $7 = 63$ **mod** $7 = 0$, so $66 \equiv 3 \pmod 7$.

c) $-17 - 3$ **mod** $7 = -20$ **mod** $7 = 1 \ne 0$, so $-17 \not\equiv 3 \pmod 7$.

d) $-67 - 3$ **mod** $7 = -70$ **mod** $7 = 0$, so $-67 \equiv 3 \pmod 7$.

30. **a)** $(177 \textbf{ mod } 31 + 270 \textbf{ mod } 31) \textbf{ mod } 31 = (22 + 22) \textbf{ mod } 31 = 44 \textbf{ mod } 31 = 13$

b) $(177 \textbf{ mod } 31 \cdot 270 \textbf{ mod } 31) \textbf{ mod } 31 = (22 \cdot 22) \textbf{ mod } 31 = 484 \textbf{ mod } 31 = 19$

32. **a)** $(19^2 \textbf{ mod } 41) \textbf{ mod } 9 = (361 \textbf{ mod } 41) \textbf{ mod } 9 = 33 \textbf{ mod } 9 = 6$

b) $(32^3 \textbf{ mod } 13)^2 \textbf{ mod } 11 = (32768 \textbf{ mod } 13)^2 \textbf{ mod } 11 = 8^2 \textbf{ mod } 11 = 64 \textbf{ mod } 11 = 9$

c) $(7^3 \textbf{ mod } 23)^2 \textbf{ mod } 31 = (343 \textbf{ mod } 23)^2 \textbf{ mod } 31 = 21^2 \textbf{ mod } 31 = 441 \textbf{ mod } 31 = 7$

d) $(21^2 \textbf{ mod } 15)^3 \textbf{ mod } 22 = (441 \textbf{ mod } 15)^3 \textbf{ mod } 22 = 6^3 \textbf{ mod } 22 = 216 \textbf{ mod } 22 = 18$

34. From $a \equiv b \pmod m$ we know that $b = a + sm$ for some integer s. Similarly, $d = c + tm$. Subtracting, we have $b - d = (a - c) + (s - t)m$, which means that $a - c \equiv b - d \pmod m$.

36. From $a \equiv b \pmod m$ we know that $b = a + sm$ for some integer s. Multiplying by c we have $bc = ac + s(mc)$, which means that $ac \equiv bc \pmod{mc}$.

38. There are two cases. If n is even, then $n = 2k$ for some integer k, so $n^2 = 4k^2$, which means that $n^2 \equiv 0 \pmod 4$. If n is odd, then $n = 2k+1$ for some integer k, so $n^2 = 4k^2+4k+1 = 4(k^2+k)+1$, which means that $n^2 \equiv 1 \pmod 4$.

40. Write $n = 2k+1$ for some integer k. Then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. Since either k or $k+1$ is even, $4k(k+1)$ is a multiple of 8. Therefore n^2-1 is a multiple of 8, so $n^2 \equiv 1 \pmod 8$.

42. The closure property states that $a +_m b \in \mathbf{Z}_m$ whenever $a, b \in \mathbf{Z}_m$. Recall that $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ and that $a +_m b$ is defined to be $(a+b)$ **mod** m. But this last expression will by definition be an integer in the desired range. To see that addition in $\mathbf{Z}_m$ is associative, we must show that $(a +_m b) +_m c = a +_m (b +_m c)$. This is equivalent to

$$((a+b \text{ **mod** } m)+c) \mathbf{\ mod\ } m = (a+(b+c \mathbf{\ mod\ } m)) \mathbf{\ mod\ } m\,.$$

This is true, because both sides equal $(a+b+c)$ **mod** m, addition of integers is associative. Similarly, addition in $\mathbf{Z}_m$ is commutative because addition in $\mathbf{Z}$ is commutative, and 0 is the additive identity for $\mathbf{Z}_m$ because 0 is the additive identity for $\mathbf{Z}$. Finally, to see that $m-a$ is an inverse of a modulo m, we just note that $(m-a) +_m a = m-a+a \mathbf{\ mod\ } m = 0$. (It is also worth observing that 0 is its own additive inverse in $\mathbf{Z}_m$.)

44. The distributive property of multiplication over addition states that $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ whenever $a, b, c \in \mathbf{Z}_m$. By the definition of these modular operations and Corollary 2, the left-hand side equals $a(b+c)$ **mod** m and the right-hand side equals $ab+ac$ **mod** m. These are equal because multiplication is distributive over addition for integers.

46. We will use $+$ and $\cdot$ for these operations to save space and improve the appearance of the table. Notice that we really can get by with a little more than half of this table if we observe that these operations are commutative; thus it would suffice to list $a+b$ and $a \cdot b$ only for $a \le b$.

$0+0=0$	$0+1=1$	$0+2=2$	$0+3=3$	$0+4=4$	$0+5=5$
$1+0=1$	$1+1=2$	$1+2=3$	$1+3=4$	$1+4=5$	$1+5=0$
$2+0=2$	$2+1=3$	$2+2=4$	$2+3=5$	$2+4=0$	$2+5=1$
$3+0=3$	$3+1=4$	$3+2=5$	$3+3=0$	$3+4=1$	$3+5=2$
$4+0=4$	$4+1=5$	$4+2=0$	$4+3=1$	$4+4=2$	$4+5=3$
$5+0=5$	$5+1=0$	$5+2=1$	$5+3=2$	$5+4=3$	$5+5=4$

$0\cdot 0=0$	$0\cdot 1=0$	$0\cdot 2=0$	$0\cdot 3=0$	$0\cdot 4=0$	$0\cdot 5=0$
$1\cdot 0=0$	$1\cdot 1=1$	$1\cdot 2=2$	$1\cdot 3=3$	$1\cdot 4=4$	$1\cdot 5=5$
$2\cdot 0=0$	$2\cdot 1=2$	$2\cdot 2=4$	$2\cdot 3=0$	$2\cdot 4=2$	$2\cdot 5=4$
$3\cdot 0=0$	$3\cdot 1=3$	$3\cdot 2=0$	$3\cdot 3=3$	$3\cdot 4=0$	$3\cdot 5=3$
$4\cdot 0=0$	$4\cdot 1=4$	$4\cdot 2=2$	$4\cdot 3=0$	$4\cdot 4=4$	$4\cdot 5=2$
$5\cdot 0=0$	$5\cdot 1=5$	$5\cdot 2=4$	$5\cdot 3=3$	$5\cdot 2=2$	$5\cdot 5=1$

SECTION 4.2 Integer Representations and Algorithms

2. To convert from decimal to binary, we successively divide by 2. We write down the remainders so obtained from right to left; that is the binary representation of the given number.

a) Since $321/2$ is 160 with a remainder of 1, the rightmost digit is 1. Then since $160/2$ is 80 with a remainder of 0, the second digit from the right is 0. We continue in this manner, obtaining successive quotients of 40, 20, 10, 5, 2, 1, and 0, and remainders of 0, 0, 0, 0, 1, 0, and 1. Putting all these remainders in order from right to left we obtain $(1\ 0100\ 0001)_2$ as the binary representation. We could, as a check, expand this binary numeral: $2^0 + 2^6 + 2^8 = 1 + 64 + 256 = 321$.

b) We could carry out the same process as in part **(a)**. Alternatively, we might notice that $1023 = 1024 - 1 = 2^{10} - 1$. Therefore the binary representation is 1 less than $(100\ 0000\ 0000)_2$, which is clearly $(11\ 1111\ 1111)_2$.

c) If we carry out the divisions by 2, the quotients are 50316, 25158, 12579, 6289, 3144, 1572, 786, 393, 196, 98, 49, 24, 12, 6, 3, 1, and 0, with remainders of 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, and 1. Putting the remainders in order from right to left we have $(1\ 1000\ 1001\ 0001\ 1000)_2$.

4. **a)** $1 + 2 + 8 + 16 = 27$ **b)** $1 + 4 + 16 + 32 + 128 + 512 = 693$
c) $2 + 4 + 8 + 16 + 32 + 128 + 256 + 512 = 958$
d) $1 + 2 + 4 + 8 + 16 + 1024 + 2048 + 4096 + 8192 + 16384 = 31775$

6. We follow the procedure of Example 7.
a) $(1111\ 0111)_2 = (011\ 110\ 111)_2 = (367)_8$
b) $(1010\ 1010\ 1010)_2 = (101\ 010\ 101\ 010)_2 = (5252)_8$
c) $(111\ 0111\ 0111\ 0111)_2 = (111\ 011\ 101\ 110\ 111)_2 = (73567)_8$
d) $(101\ 0101\ 0101\ 0101)_2 = (101\ 010\ 101\ 010\ 101)_2 = (52525)_8$

8. Following Example 7, we simply write the binary equivalents of each digit. Since $(\mathrm{A})_{16} = (1010)_2$, $(\mathrm{B})_{16} = (1011)_2$, $(\mathrm{C})_{16} = (1100)_2$, $(\mathrm{D})_{16} = (1101)_2$, $(\mathrm{E})_{16} = (1110)_2$, and $(\mathrm{F})_{16} = (1111)_2$, we have $(\mathrm{BADFACED})_{16} = (10111010110111111010110011101101)_2$. Following the convention shown in Exercise 3 of grouping binary digits by fours, we can write this in a more readable form as 1011 1010 1101 1111 1010 1100 1110 1101.

10. We follow the procedure of Example 7.
a) $(1111\ 0111)_2 = (\mathrm{F7})_{16}$ **b)** $(1010\ 1010\ 1010)_2 = (\mathrm{AAA})_{16}$
c) $(111\ 0111\ 0111\ 0111)_2 = (7777)_{16}$ **d)** $(101\ 0101\ 0101\ 0101)_2 = (5555)_{16}$

12. Following Example 7, we simply write the hexadecimal equivalents of each group of four binary digits. Note that we group from the right, so the left-most group, which is just 1, becomes 0001. Thus we have $(0001\ 1000\ 0110\ 0011)_2 = (1863)_{16}$.

14. Let $(\ldots h_2h_1h_0)_{16}$ be the hexadecimal expansion of a positive integer. The value of that integer is, therefore, $h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots = h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots$. If we replace each hexadecimal digit h_i by its binary expansion $(b_{i3}b_{i2}b_{i1}b_{i0})_2$, then $h_i = b_{i0} + 2b_{i1} + 4b_{i2} + 8b_{i3}$. Therefore the value of the entire number is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13}) \cdot 2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23}) \cdot 2^8 + \cdots = b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 2^4b_{10} + 2^5b_{11} + 2^6b_{12} + 2^7b_{13} + 2^8b_{20} + 2^9b_{21} + 2^{10}b_{22} + 2^{11}b_{23} + \cdots$, which is the value of the binary expansion $(\ldots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$.

16. Let $(\ldots d_2d_1d_0)_8$ be the octal expansion of a positive integer. The value of that integer is, therefore, $d_0 + d_1 \cdot 8 + d_2 \cdot 8^2 + \cdots = d_0 + d_1 \cdot 2^3 + d_2 \cdot 2^6 + \cdots$. If we replace each octal digit d_i by its binary expansion $(b_{i2}b_{i1}b_{i0})_2$, then $d_i = b_{i0} + 2b_{i1} + 4b_{i2}$. Therefore the value of the entire number is $b_{00} + 2b_{01} + 4b_{02} + (b_{10} + 2b_{11} + 4b_{12}) \cdot 2^3 + (b_{20} + 2b_{21} + 4b_{22}) \cdot 2^6 + \cdots = b_{00} + 2b_{01} + 4b_{02} + 2^3b_{10} + 2^4b_{11} + 2^5b_{12} + 2^6b_{20} + 2^6b_{21} + 2^8b_{22} + \cdots$, which is the value of the binary expansion $(\ldots b_{22}b_{21}b_{20}b_{12}b_{11}b_{10}b_{02}b_{01}b_{00})_2$.

18. Since we have procedures for converting both octal and hexadecimal to and from binary (Example 7), to convert from hexadecimal to octal, we first convert from hexadecimal to binary and then convert from binary to octal.

20. Note that $64 = 2^6 = 8^2$. In base 64 we need 64 symbols, from 0 up to something representing 63 (maybe we could use, for example, digits up to 9, then lower and upper case letters from a to Z, and finally symbols @ and $ to represent 62 and 63). Corresponding to each such symbol would be a binary string of six digits, from 000000 for 0, through 001010 for a, 100011 for z, 100100 for A, 111101 for Z, 111110 for @, and 111111 for $. To translate from binary to base 64, we group the binary digits from the right in groups of 6 and use the list of correspondences to replace each six bits by one base-64 digit. To convert from base 64 to binary, we just replace each base-64 digit by its corresponding six bits.

For conversions between octal and base 64, we change the binary strings in our table to octal strings, replacing each 6-bit string by its 2-digit octal equivalent, and then follow the same procedures as above, interchanging base-64 digits and 2-digit strings of octal digits.

22. We can just add and multiply using the grade-school algorithms (working column by column starting at the right), using the addition and multiplication tables in base three (for example, $2 + 1 = 10$ and $2 \cdot 2 = 11$). When a digit-by-digit answer is too large to fit (i.e., greater than 2), we "carry" into the next column. Note that we can check our work by converting everything to decimal numerals (the check is shown in parentheses below). A calculator or computer algebra system makes doing the conversions tolerable. For convenience, we leave off the "3" subscripts throughout.

a) $112 + 210 = 1022$ (decimal: $14 + 21 = 35$)
$112 \cdot 210 = 101{,}220$ (decimal: $14 \cdot 21 = 294$)

b) $2112 + 12021 = 21{,}210$ (decimal: $68 + 142 = 210$)
$2112 \cdot 12021 = 111{,}020{,}122$ (decimal: $68 \cdot 142 = 9656$)

c) $20001 + 1111 = 21{,}112$ (decimal: $163 + 40 = 203$)
$20001 \cdot 1111 = 22{,}221{,}111$ (decimal: $163 \cdot 40 = 6520$)

d) $120021 + 2002 = 122{,}100$ (decimal: $412 + 56 = 468$)
$120021 \cdot 2002 = 1{,}011{,}122{,}112$ (decimal: $412 \cdot 56 = 23{,}072$)

24. We can just add and multiply using the grade-school algorithms (working column by column starting at the right), using the addition and multiplication tables in base sixteen (for example, $7 + 8 = \mathrm{F}$ and $7 \cdot 8 = 38$). When a digit-by-digit answer is too large to fit (i.e., greater than F), we "carry" into the next column. Note that we can check our work by converting everything to decimal numerals (the check is shown in parentheses below). A calculator or computer algebra system makes doing the conversions tolerable, specially if we use built-in functions for doing so. For convenience, we leave off the "16" subscripts throughout.

a) $\mathrm{1AB} + \mathrm{BBC} = \mathrm{D67}$ (decimal: $427 + 3004 = 3431$)
$\mathrm{1AB} \cdot \mathrm{BBC} = 139{,}294$ (decimal: $427 \cdot 3004 = 1{,}282{,}708$)

b) $\mathrm{20CBA} + \mathrm{A01} = \mathrm{21{,}6BB}$ (decimal: $134{,}330 + 2561 = 136{,}891$)
$\mathrm{20CBA} \cdot \mathrm{A01} = \mathrm{14{,}815{,}0BA}$ (decimal: $134{,}330 \cdot 2561 = 344{,}019{,}130$)

c) $\mathrm{ABCDE} + 1111 = \mathrm{AC{,}DEF}$ (decimal: $703{,}710 + 4369 = 708{,}079$)
$\mathrm{ABCDE} \cdot 1111 = \mathrm{B7{,}414{,}8BE}$ (decimal: $703{,}710 \cdot 4369 = 3{,}074{,}508{,}990$)

d) $\mathrm{E0000E} + \mathrm{BAAA} = \mathrm{E0B{,}AB8}$ (decimal: $14{,}680{,}078 + 47{,}786 = 14{,}727{,}864$)
$\mathrm{E0000E} \cdot \mathrm{BAAA} = \mathrm{A{,}354{,}CA3{,}54C}$ (decimal: $14{,}680{,}078 \cdot 47{,}786 = 701{,}502{,}207{,}308$)

26. In effect, this algorithm computes $11 \mathbin{\mathbf{mod}} 645$, $11^2 \mathbin{\mathbf{mod}} 645$, $11^4 \mathbin{\mathbf{mod}} 645$, $11^8 \mathbin{\mathbf{mod}} 645$, $11^{16} \mathbin{\mathbf{mod}} 645$, $\ldots$, and then multiplies (modulo 645) the required values. Since $644 = (1010000100)_2$, we need to multiply together 11^4 **mod** 645, 11^{128} **mod** 645, and 11^{512} **mod** 645, reducing modulo 645 at each step. We compute by repeatedly squaring: 11^2 **mod** $645 = 121$, 11^4 **mod** $645 = 121^2$ **mod** $645 = 14641$ **mod** $645 = 451$, 11^8 **mod** $645 = 451^2$ **mod** $645 = 203401$ **mod** $645 = 226$, 11^{16} **mod** $645 = 226^2$ **mod** $645 = 51076$ **mod** $645 = 121$. At this point we notice that 121 appeared earlier in our calculation, so we have 11^{32} **mod** $645 = 121^2$ **mod** $645 = 451$, 11^{64} **mod** $645 = 451^2$ **mod** $645 = 226$, 11^{128} **mod** $645 = 226^2$ **mod** $645 = 121$, 11^{256} **mod** $645 = 451$, and 11^{512} **mod** $645 = 226$. Thus our final answer will be the product of 451, 121, and 226, reduced modulo 645. We compute these one at a time: $451 \cdot 121$ **mod** $645 = 54571$ **mod** $645 = 391$, and $391 \cdot 226$ **mod** $645 = 88366$ **mod** $645 = 1$. So 11^{644} **mod** $645 = 1$. A computer algebra system will verify this; use the command "`1 &^ 644 mod 645;`" in *Maple*, for example. The ampersand here tells *Maple* to use modular exponentiation, rather than first computing the integer 11^{644}, which has over 600 digits, although it could certainly handle this if asked. The point is that modular exponentiation is much faster and avoids having to deal with such large numbers.

28. In effect this algorithm computes powers 123 **mod** 101, 123^2 **mod** 101, 123^4 **mod** 101, 123^8 **mod** 101, 123^{16} **mod** 101, ..., and then multiplies (modulo 101) the required values. Since $1001 = (1111101001)_2$, we need to multiply together 123 **mod** 101, 123^8 **mod** 101, 123^{32} **mod** 101, 123^{64} **mod** 101, 123^{128} **mod** 101, 123^{256} **mod** 101, and 123^{512} **mod** 101, reducing modulo 101 at each step. We compute by repeatedly squaring: 123 **mod** $101 = 22$, 123^2 **mod** $101 = 22^2$ **mod** $101 = 484$ **mod** $101 = 80$, 123^4 **mod** $101 = 80^2$ **mod** $101 = 6400$ **mod** $101 = 37$, 123^8 **mod** $101 = 37^2$ **mod** $101 = 1369$ **mod** $101 = 56$, 123^{16} **mod** $101 = 56^2$ **mod** $101 = 3136$ **mod** $101 = 5$, 123^{32} **mod** $101 = 5^2$ **mod** $101 = 25$, 123^{64} **mod** $101 = 25^2$ **mod** $101 = 625$ **mod** $101 = 19$, 123^{128} **mod** $101 = 19^2$ **mod** $101 = 361$ **mod** $101 = 58$, 123^{256} **mod** $101 = 58^2$ **mod** $101 = 3364$ **mod** $101 = 31$, and 123^{512} **mod** $101 = 31^2$ **mod** $101 = 961$ **mod** $101 = 52$. Thus our final answer will be the product of 22, 56, 25, 19, 58, 31, and 52. We compute these one at a time modulo 101: $22 \cdot 56$ is 20, $20 \cdot 25$ is 96, $96 \cdot 19$ is 6, $6 \cdot 58$ is 45, $45 \cdot 31$ is 82, and finally $82 \cdot 52$ is 22. So 123^{1001} **mod** $101 = 22$.

30. **a)** $5 = 9 - 3 - 1$ **b)** $13 = 9 + 3 + 1$ **c)** $37 = 27 + 9 + 1$ **d)** $79 = 81 - 3 + 1$

32. The key fact here is that $10 \equiv -1 \pmod{11}$, and so $10^k \equiv (-1)^k \pmod{11}$. Thus 10^k is congruent to 1 if k is even and to -1 if k is odd. Let the decimal expansion of the integer a be given by $(a_{n-1}a_{n-2}\ldots a_3a_2a_1a_0)_{10}$. Thus $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0$. Since $10^k \equiv (-1)^k \pmod{11}$, we have $a \equiv \pm a_{n-1} \mp a_{n-2} + \cdots - a_3 + a_2 - a_1 + a_0 \pmod{11}$, where signs alternate and depend on the parity of n. Therefore $a \equiv 0 \pmod{11}$ if and only if $(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$, which we obtain by collecting the odd and even indexed terms, is congruent to $0 \pmod{11}$. Since being divisible by 11 is the same as being congruent to $0 \pmod{11}$, we have proved that a positive integer is divisible by 11 if and only if the sum of its decimal digits in even-numbered positions minus the sum of its decimal digits in odd-numbered positions is divisible by 11.

34. **a)** Since the binary representation of 22 is 10110, the six bit one's complement representation is 010110.

b) Since the binary representation of 31 is 11111, the six bit one's complement representation is 011111.

c) Since the binary representation of 7 is 111, we complement 000111 to obtain 111000 as the one's complement representation of -7.

d) Since the binary representation of 19 is 10011, we complement 010011 to obtain 101100 as the one's complement representation of -19.

36. Every 1 is changed to a 0, and every 0 is changed to a 1.

38. We just combine the two ideas in Exercises 36 and 37: to form $a - b$, we compute $a + (-b)$, using Exercise 36 to find $-b$ and Exercise 37 to find the sum.

40. Following the definition, we find the two's complement expansion of a positive number simply by representing it in binary, using six bits; and we find the two's complement expansion of a negative number $-x$ by representing $2^5 - x$ in binary using five bits and preceding it with a 1.

a) Since 22 is positive, and its binary expansion is 10110, the answer is 010110.

b) Since 31 is positive, and its binary expansion is 11111, the answer is 011111.

c) Since -7 is negative, we first find the 5-bit binary expansion of $2^5 - 7 = 25$, namely 11001, and precede it by a 1, obtaining 111001.

d) Since -19 is negative, we first find the 5-bit binary expansion of $2^5 - 19 = 13$, namely 01101, and precede it by a 1, obtaining 101101.

42. We can experiment a bit to find a convenient algorithm. We saw in Exercise 40 that the expansion of -7 is 111001, while of course the expansion of 7 is 000111. Apparently to find the expansion of $-m$ from that of m we complement each bit and then add 1, working in base 2. Similarly, the expansion of -8 is 111000, whereas the expansion of 8 is 001000; again $110111 + 1 = 111000$. At the extremes (using six bits) we have 1 represented by 000001, so -1 is represented by $111110 + 1 = 111111$; and 31 is represented by 011111, so -31 is represented by $100000 + 1 = 100001$.

44. We just combine the two ideas in Exercises 42 and 43. To form $a - b$, we compute $a + (-b)$, using Exercise 42 to find $-b$ and Exercise 43 to find the sum.

46. If the number is positive (i.e., the left-most bit is 0), then the expansions are the same. If the number is negative (i.e., the left-most bit is 1), then we take the one's complement representation and add 1, working in base 2. For example, the one's complement representation of -19 using six bits is, from Exercise 34, 101100. Adding 1 we obtain 101101, which is the two's complement representation of -19 using six bits, from Exercise 40.

48. We obtain these expansions from the top down. For example in part **(e)** we compute that $7! > 1000$ but $6! \leq 1000$, so the highest factorial appearing is $6! = 720$. We use the division algorithm to find the quotient and remainder when 1000 is divided by 720, namely 1 and 280, respectively. Therefore the expansion begins $1 \cdot 6!$ and continues with the expansion of 280, which we find in the same manner.

a) $2 = 2!$ **b)** $7 = 3! + 1!$ **c)** $19 = 3 \cdot 3! + 1!$ **d)** $87 = 3 \cdot 4! + 2 \cdot 3! + 2! + 1!$

e) $1000 = 6! + 2 \cdot 5! + 4! + 2 \cdot 3! + 2 \cdot 2!$ **f)** $1000000 = 2 \cdot 9! + 6 \cdot 8! + 6 \cdot 7! + 2 \cdot 6! + 5 \cdot 5! + 4! + 2 \cdot 3! + 2 \cdot 2!$

50. The algorithm is essentially the same as the usual grade-school algorithm for adding. We add from right to left, one column at a time, carrying to the next column if necessary. A carry out of the column representing $i!$ is needed whenever the sum obtained for that column is greater than i, in which case we subtract $i + 1$ from that digit and carry 1 into the next column (since $(i + 1)! = (i + 1) \cdot i!$).

52. The partial products are 11100 and 1110000, namely 1110 shifted one place and three places to the left. We add these two numbers, obtaining 10001100.

54. Subtraction is really just like addition, so the number of bit operations should be comparable, namely $O(n)$. More specifically, if we analyze the algorithm for Exercise 53, we see that the loop is executed n times, and only a few operations are performed during each pass.

56. In the worst case, each bit of a has to be compared to each bit of b, so $O(n)$ comparisons are needed. An exact analysis of the procedure given in the solution to Exercise 55 shows that $n + 1$ comparisons of bits are needed in the worst case, assuming that the logical "and" condition in the **while** loop is evaluated efficiently from left to right (so that a_0 is not compared to b_0 there).

58. A multiplication modulo m consists of multiplying two integers, each at most $\log m$ bits long (since they are less than m), followed by a division by m, which is also $\log m$ bits long. Thus this takes $(\log m)^2$ bit operations by Example 11 and the analysis of Algorithm 4 mentioned in the text. This is what goes on inside the loop of Algorithm 5. The loop is iterated $\log n$ times. Therefore the total number of bit operations is $O((\log m)^2 \log n)$.

SECTION 4.3 Primes and Greatest Common Divisors

2. The numbers 19, 101, 107, and 113 are prime, as we can verify by trial division. The numbers $27 = 3^3$ and $93 = 3 \cdot 31$ are not prime.

4. We obtain the answers by trial division. The factorizations are $39 = 3 \cdot 13$, $81 = 3^4$, $101 = 101$ (prime), $143 = 11 \cdot 13$, $289 = 17^2$, and $899 = 29 \cdot 31$.

6. A 0 appears at the end of a number for every factor of 10 $(= 2 \cdot 5)$ the number has. Now 100! certainly has more factors of 2 than it has factors of 5, so the number of factors of 10 it has is the same as the number of factors of 5. Each of the twenty numbers $5, 10, 15, \ldots, 100$ contributes a factor of 5 to 100!, and in addition the four numbers 25, 50, 75, and 100 contribute one more factor of 5. Therefore there are 24 factors of 5 in 100!, so 100! ends in exactly 24 0's.

8. The input is a positive integer n. We successively look for small factors d (starting with $d = 2$ and incrementing d once we know that d is no longer a factor of what remains), which will necessarily be prime. When we find a factor, we divide out by that factor and keep going. We will print the factors as we find them. (Alternatively, they could be stored in a list of some sort.) We stop when the remaining number is 1 (all factors have been found). The pseudocode below accomplishes this. Notice that we could be a little more sophisticated and use only prime trial divisors, but it hardly seems worth the effort, since it would take time to see which trial divisors are prime. Alternatively, we could handle $d = 2$ by itself and then loop through only odd values of d, starting at 3 and incrementing by 2.

```
procedure factorization(n : positive integer)
d := 2
while n > 1
    if n mod d = 0 then
        print d
        n := n/d
    else
        d := d + 1
```

10. We first establish the identity in the hint. If we let $y = x^k$, then the claimed identity is

$$(y^t + 1) = (y + 1)(y^{t-1} - y^{t-2} + y^{t-3} - \cdots - y + 1),$$

which is easily seen to be true by multiplying out the right-hand side and noticing the "telescoping" that occurs. We want to show that m is a power of 2, i.e., that its only prime factor is 2. Suppose to the contrary that m has an odd prime factor t and write $m = kt$, where k is a positive integer. Letting $x = 2$ in the identity given in the hint, we have $2^m + 1 = (2^k + 1)(\text{the other factor})$. Because $2^k + 1 > 1$ and the prime $2^m + 1$ can have no proper factor greater than 1, we must have $2^m + 1 = 2^k + 1$, so $m = k$ and $t = 1$, contradicting the fact that t is prime. This completes the proof by contradiction.

12. We follow the hint. There are n numbers in the sequence $(n+1)!+2$, $(n+1)!+3$, $(n+1)!+4$, $\ldots$, $(n+1)!+(n+1)$. The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; the third is composite because it is divisible by 4; $\ldots$; the last is composite because it is divisible by $n+1$. This gives us the desired n consecutive composite integers.

14. We must find, by inspection with mental arithmetic, the greatest common divisors of the numbers from 1 to 11 with 12, and list those whose gcd is 1. These are 1, 5, 7, and 11. There are so few since 12 had many factors—in particular, both 2 and 3.

16. Since these numbers are small, the easiest approach is to find the prime factorization of each number and look for any common prime factors.

a) Since $21 = 3 \cdot 7$, $34 = 2 \cdot 17$, and $55 = 5 \cdot 11$, these are pairwise relatively prime.

b) Since $85 = 5 \cdot 17$, these are not pairwise relatively prime.

c) Since $25 = 5^2$, 41 is prime, $49 = 7^2$, and $64 = 2^6$, these are pairwise relatively prime.

d) Since 17, 19, and 23 are prime and $18 = 2 \cdot 3^2$, these are pairwise relatively prime.

18. **a)** Since $6 = 1+2+3$, and these three summands are the only proper divisors of 6, we conclude that 6 is perfect. Similarly $28 = 1+2+4+7+14$.

b) We need to find all the proper divisors of $2^{p-1}(2^p-1)$. Certainly all the numbers 1, 2, 4, 8, $\ldots$, 2^{p-1} are proper divisors, and their sum is $2^p - 1$ (this is a geometric series). Also each of these divisors times $2^p - 1$ is also a divisor, and all but the last is proper. Again adding up this geometric series we find a sum of $(2^p-1)(2^{p-1}-1)$. There are no other other proper divisors. Therefore the sum of all the divisors is $(2^p-1)+(2^p-1)(2^{p-1}-1) = (2^p-1)(1+2^{p-1}-1) = (2^p-1)2^{p-1}$, which is our original number. Therefore this number is perfect.

20. We need to find a factor if there is one, or else check all possible prime divisors up to the square root of the given number to verify that there is no nontrivial divisor.

a) $2^7 - 1 = 127$. Division by 2, 3, 5, 7, and 11 shows that these are not factors. Since $\sqrt{127} < 13$, we are done; 127 is prime.

b) $2^9 - 1 = 511 = 7 \cdot 73$, so this number is not prime.

c) $2^{11} - 1 = 2047 = 23 \cdot 89$, so this number is not prime.

d) $2^{13} - 1 = 8191$. Division by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, and 89 (phew!) shows that these are not factors. Since $\sqrt{8191} < 97$, we are done; 8191 is prime.

22. Certainly if n is prime, then all the integers from 1 to $n-1$ are less than or equal to n and relatively prime to n, but no others are, so $\phi(n) = n-1$. Conversely, suppose that n is not prime. If $n=1$, then we have $\phi(1) = 1 \neq 1-1$. If $n > 1$, then $n = ab$ with $1 < a < n$ and $1 < b < n$. Note that neither a nor b is relatively prime to n. Therefore the number of positive integers less than or equal to n and relatively prime to n is at most $n-3$ (since a, b, and n are not in this collection), so $\phi(n) \neq n-1$.

24. We form the greatest common divisors by finding the minimum exponent for each prime factor.

a) $2^2 \cdot 3^3 \cdot 5^2$ **b)** $2 \cdot 3 \cdot 11$ **c)** 17 **d)** 1 **e)** 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7$

26. We form the least common multiples by finding the maximum exponent for each prime factor.

a) $2^5 \cdot 3^3 \cdot 5^5$ **b)** $2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$ **c)** 17^{17} **d)** $2^2 \cdot 5^3 \cdot 7 \cdot 13$

e) undefined (0 is not a positive integer) **f)** $2 \cdot 3 \cdot 5 \cdot 7$

28. We have $1000 = 2^3 \cdot 5^3$ and $625 = 5^4$, so $\gcd(1000, 625) = 5^3 = 125$, and $\operatorname{lcm}(1000, 625) = 2^3 \cdot 5^4 = 5000$. As expected, $125 \cdot 5000 = 625000 = 1000 \cdot 625$.

30. By Exercise 31 we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11})/(2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$.

32. To apply the Euclidean algorithm, we divide the larger number by the smaller, replace the larger by the smaller and the smaller by the remainder of this division, and repeat this process until the remainder is 0. At that point, the smaller number is the greatest common divisor.

a) $\gcd(1,5) = \gcd(1,0) = 1$ **b)** $\gcd(100,101) = \gcd(100,1) = \gcd(1,0) = 1$

c) $\gcd(123,277) = \gcd(123,31) = \gcd(31,30) = \gcd(30,1) = \gcd(1,0) = 1$

d) $\gcd(1529,14039) = \gcd(1529,278) = \gcd(278,139) = \gcd(139,0) = 139$

e) $\gcd(1529,14038) = \gcd(1529,277) = \gcd(277,144) = \gcd(144,133) = \gcd(133,11) = \gcd(11,1) = \gcd(1,0)$ $= 1$

f) $\gcd(11111,111111) = \gcd(11111,1) = \gcd(1,0) = 1$

34. We need to divide successively by 34, 21, 13, 8, 5, 3, 2, and 1, so eight divisions are required.

36. The statement we are asked to prove involves the result of dividing $2^a - 1$ by $2^b - 1$. Let us actually carry out that division algebraically—long division of these expressions. The leading term in the quotient is 2^{a-b} (as long as $a \geq b$), with a remainder at that point of $2^{a-b} - 1$. If now $a - b \geq b$ then the next step in the long division produces the next summand in the quotient, 2^{a-2b}, with a remainder at this stage of $2^{a-2b} - 1$. This process of long division continues until the remainder at some stage is less than the divisor, i.e., $2^{a-kb} - 1 < 2^b - 1$. But then the remainder is $2^{a-kb} - 1$, and clearly $a - kb$ is exactly a **mod** b. This completes the proof.

38. By Exercise 37, $2^a - 1$ and $2^b - 1$ are relatively prime precisely when $2^{\gcd(a,b)} - 1 = 1$, which happens if and only if $\gcd(a,b) = 1$. Thus it is enough to check here that 35, 34, 33, 31, 29, and 23 are relatively prime. This is clear, since the prime factorizations are, respectively, 35, $2 \cdot 17$, $3 \cdot 11$, 31, 29, and 23.

40. **a)** In order to find the coefficients s and t such that $9s + 11t = \gcd(9,11)$, we carry out the steps of the Euclidean algorithm.

$$11 = 9 + 2$$
$$9 = 4 \cdot 2 + 1$$

Then we work up from the bottom, expressing the greatest common divisor (which we have just seen to be 1) in terms of the numbers involved in the algorithm, namely 11, 9, and 2. In particular, the last equation tells us that $1 = 9 - 4 \cdot 2$, so that we have expressed the gcd as a linear combination of 9 and 2. But now the first equation tells us that $2 = 11 - 9$; we plug this into our previous equation and obtain

$$1 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11\,.$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 9 and 11, namely $\gcd(9,11) = 5 \cdot 9 - 4 \cdot 11$.

b) Again, we carry out the Euclidean algorithm. Since $44 = 33 + 11$, and $11 \mid 33$, we know that $\gcd(33,44) = 11$. From the equation shown here, we can immediately write $11 = (-1) \cdot 33 + 44$.

c) The calculation of the greatest common divisor takes several steps:

$$78 = 2 \cdot 35 + 8$$
$$35 = 4 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 2 + 1$$

Then we need to work our way back up, successively plugging in for the remainders determined in this calculation:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\ &= 3 \cdot (35 - 4 \cdot 8) - 8 = 3 \cdot 35 - 13 \cdot 8 \\ &= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) = 29 \cdot 35 - 13 \cdot 78 \end{aligned}$$

d) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned} 55 &= 2 \cdot 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (55 - 2 \cdot 21) = 21 \cdot 21 - 8 \cdot 55 \end{aligned}$$

e) We compute the greatest common divisor in one step: $203 = 2 \cdot 101 + 1$. Therefore we have $1 = (-2) \cdot 101 + 203$.

f) We compute the greatest common divisor using the Euclidean algorithm:

$$\begin{aligned} 323 &= 2 \cdot 124 + 75 \\ 124 &= 75 + 49 \\ 75 &= 49 + 26 \\ 49 &= 26 + 23 \\ 26 &= 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (23 - 7 \cdot 3) = 8 \cdot 3 - 23 \\ &= 8 \cdot (26 - 23) - 23 = 8 \cdot 26 - 9 \cdot 23 \\ &= 8 \cdot 26 - 9 \cdot (49 - 26) = 17 \cdot 26 - 9 \cdot 49 \\ &= 17 \cdot (75 - 49) - 9 \cdot 49 = 17 \cdot 75 - 26 \cdot 49 \\ &= 17 \cdot 75 - 26 \cdot (124 - 75) = 43 \cdot 75 - 26 \cdot 124 \\ &= 43 \cdot (323 - 2 \cdot 124) - 26 \cdot 124 = 43 \cdot 323 - 112 \cdot 124 \end{aligned}$$

g) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}
2339 &= 2002 + 337\\
2002 &= 5 \cdot 337 + 317\\
337 &= 317 + 20\\
317 &= 15 \cdot 20 + 17\\
20 &= 17 + 3\\
17 &= 5 \cdot 3 + 2\\
3 &= 2 + 1
\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
1 &= 3 - 2\\
&= 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17\\
&= 6 \cdot (20 - 17) - 17 = 6 \cdot 20 - 7 \cdot 17\\
&= 6 \cdot 20 - 7 \cdot (317 - 15 \cdot 20) = 111 \cdot 20 - 7 \cdot 317\\
&= 111 \cdot (337 - 317) - 7 \cdot 317 = 111 \cdot 337 - 118 \cdot 317\\
&= 111 \cdot 337 - 118 \cdot (2002 - 5 \cdot 337) = 701 \cdot 337 - 118 \cdot 2002\\
&= 701 \cdot (2339 - 2002) - 118 \cdot 2002 = 701 \cdot 2339 - 819 \cdot 2002
\end{aligned}$$

h) The procedure is the same:

$$\begin{aligned}
4669 &= 3457 + 1212\\
3457 &= 2 \cdot 1212 + 1033\\
1212 &= 1033 + 179\\
1033 &= 5 \cdot 179 + 138\\
179 &= 138 + 41\\
138 &= 3 \cdot 41 + 15\\
41 &= 2 \cdot 15 + 11\\
15 &= 11 + 4\\
11 &= 2 \cdot 4 + 3\\
4 &= 3 + 1
\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
1 &= 4 - 3\\
&= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11\\
&= 3 \cdot (15 - 11) - 11 = 3 \cdot 15 - 4 \cdot 11\\
&= 3 \cdot 15 - 4 \cdot (41 - 2 \cdot 15) = 11 \cdot 15 - 4 \cdot 41\\
&= 11 \cdot (138 - 3 \cdot 41) - 4 \cdot 41 = 11 \cdot 138 - 37 \cdot 41\\
&= 11 \cdot 138 - 37 \cdot (179 - 138) = 48 \cdot 138 - 37 \cdot 179\\
&= 48 \cdot (1033 - 5 \cdot 179) - 37 \cdot 179 = 48 \cdot 1033 - 277 \cdot 179\\
&= 48 \cdot 1033 - 277 \cdot (1212 - 1033) = 325 \cdot 1033 - 277 \cdot 1212\\
&= 325 \cdot (3457 - 2 \cdot 1212) - 277 \cdot 1212 = 325 \cdot 3457 - 927 \cdot 1212\\
&= 325 \cdot 3457 - 927 \cdot (4669 - 3457) = 1252 \cdot 3457 - 927 \cdot 4669
\end{aligned}$$

i) The procedure is the same:

$$\begin{aligned}13422 &= 10001 + 3421\\ 10001 &= 2 \cdot 3421 + 3159\\ 3421 &= 3159 + 262\\ 3159 &= 12 \cdot 262 + 15\\ 262 &= 17 \cdot 15 + 7\\ 15 &= 2 \cdot 7 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}1 &= 15 - 2 \cdot 7\\ &= 15 - 2 \cdot (262 - 17 \cdot 15) = 35 \cdot 15 - 2 \cdot 262\\ &= 35 \cdot (3159 - 12 \cdot 262) - 2 \cdot 262 = 35 \cdot 3159 - 422 \cdot 262\\ &= 35 \cdot 3159 - 422 \cdot (3421 - 3159) = 457 \cdot 3159 - 422 \cdot 3421\\ &= 457 \cdot (10001 - 2 \cdot 3421) - 422 \cdot 3421 = 457 \cdot 10001 - 1336 \cdot 3421\\ &= 457 \cdot 10001 - 1336 \cdot (13422 - 10001) = 1793 \cdot 10001 - 1336 \cdot 13422\end{aligned}$$

42. We take $a = 356$ and $b = 252$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 104$, $q_2 = 2$, $r_3 = 44$, $q_3 = 2$, $r_4 = 16$, $q_4 = 2$, $r_5 = 12$, $q_5 = 1$, $r_6 = 4$, $q_6 = 3$. Note that $n = 6$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1$, $t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$
$s_3 = s_1 - q_2 s_2 = 0 - 2 \cdot 1 = -2$, $t_3 = t_1 - q_2 t_2 = 1 - 2 \cdot (-1) = 3$
$s_4 = s_2 - q_3 s_3 = 1 - 2 \cdot (-2) = 5$, $t_4 = t_2 - q_3 t_3 = -1 - 2 \cdot 3 = -7$
$s_5 = s_3 - q_4 s_4 = -2 - 2 \cdot 5 = -12$, $t_5 = t_3 - q_4 t_4 = 3 - 2 \cdot (-7) = 17$
$s_6 = s_4 - q_5 s_5 = 5 - 1 \cdot (-12) = 17$, $t_6 = t_4 - q_5 t_5 = -7 - 1 \cdot 17 = -24$

Thus we have $s_6 a + t_6 b = 17 \cdot 356 + (-24) \cdot 252 = 4$, which is $\gcd(356, 252)$.

44. We take $a = 100001$ and $b = 1001$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 99$, $r_2 = 902$, $q_2 = 1$, $r_3 = 99$, $q_3 = 9$, $r_4 = 11$, $q_4 = 9$. Note that $n = 4$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 99 \cdot 0 = 1$, $t_2 = t_0 - q_1 t_1 = 0 - 99 \cdot 1 = -99$
$s_3 = s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1$, $t_3 = t_1 - q_2 t_2 = 1 - 1 \cdot (-99) = 100$
$s_4 = s_2 - q_3 s_3 = 1 - 9 \cdot (-1) = 10$, $t_4 = t_2 - q_3 t_3 = -99 - 9 \cdot 100 = -999$

Thus we have $s_4 a + t_4 b = 10 \cdot 100001 + (-999) \cdot 1001 = 11$, which is $\gcd(100001, 1001)$.

46. The number of (positive) factors that a positive integer n has can be determined from the prime factorization of n. If we write this prime factorization as $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then there are $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$ different factors. This follows from the ideas in Chapter 6. Specifically, in choosing a factor we can choose 0, 1, 2, $\ldots$, e_1 of the p_1 factors, a total of $e_1 + 1$ choices; for each of these there are $e_2 + 1$ choices as to how many p_2 factors to include, and so on. If we don't want to go through the analysis using the ideas given below, we could simply compute the number of factors for each n, starting at 1 (perhaps using a computer program), and thereby obtain the answers by "brute force."

a) If an integer is to have exactly three different factors (we assume "positive factors" is intended here), then n must be the square of a prime number; that is the only way to make $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1) = 3$. The smallest prime number is 2. So the smallest positive integer with exactly three factors is $2^2 = 4$.

b) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=4$. We can do this with $r=1$ and $e_1=3$, or with $r=2$ and $e_1=e_2=1$. The smallest numbers obtainable in these ways are $2^3=8$ and $2\cdot 3=6$, respectively. So the smallest number with four factors is 6.

c) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=5$. We can do this only with $r=1$ and $e_1=4$, so the smallest such number is $2^4=16$.

d) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=6$. We can do this with $r=1$ and $e_1=5$, or with $r=2$ and $e_1=2$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^5=32$ and $2^2\cdot 3=12$, respectively. So the smallest number with six factors is 12.

e) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=10$. We can do this with $r=1$ and $e_1=9$, or with $r=2$ and $e_1=4$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^9=512$ and $2^4\cdot 3=48$, respectively. So the smallest number with ten factors is 48.

48. Obviously there are no definitive answers to these problems, but we present below a reasonable and satisfying rule for forming the sequence in each case.

a) All the entries are primes. In fact, the n^{th} term is the smallest prime number greater than or equal to n.

b) Here we see that the sequence jumps at the prime locations. We can state this succinctly by saying that the n^{th} term is the number of prime numbers not exceeding n.

c) There are 0s in the prime locations and 1s elsewhere. In other words, the n^{th} term of the sequence is 0 if n is a prime number and 1 otherwise.

d) This sequence is actually important in number theory. The n^{th} term is -1 if n is prime, 0 if n has a repeated prime factor (for example, $12=2^2\cdot 3$, so 2 is a repeated prime factor of 12 and therefore the twelfth term is 0), and 1 otherwise (if n is not prime but is square-free).

e) The n^{th} term is 0 if n has two or more distinct prime factors, and is 1 otherwise. In other words the n^{th} term is 1 if n is a power of a prime number.

f) The n^{th} term is the square of the n^{th} prime.

50. From $a\equiv b \pmod{m}$ we know that $b=a+sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a=b-sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a,m)=\gcd(b,m)$.

52. We compute the first several of these: $2+1=3$ (which is prime), $2\cdot3+1=7$ (which is prime), $2\cdot3\cdot5+1=31$ (which is prime), $2\cdot3\cdot5\cdot7+1=211$ (which is prime), $2\cdot3\cdot5\cdot7\cdot11+1=2311$ (which is prime). However, $2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031=59\cdot509$, so the conjecture is false. Notice, however, that the prime factors in this last case were necessarily different from the primes being multiplied.

54. Suppose by way of contradiction that q_1, q_2, ..., q_n are the only primes of the form $3k+2$. Notice that this list necessarily includes 2. Let $Q=3q_1q_2\cdots q_n-1$. Notice that neither 3 nor any prime of the form $3k+2$ is a factor of Q. But $Q\ge 3\cdot2-1=5>1$, so it must have prime factors. Therefore all of its prime factors are of the form $3k+1$. However, the product of numbers of the form $3k+1$ is again of that form, because $(3k+1)(3l+1)=3(3kl+k+l)+1$. Patently Q is not of that form, and we have a contradiction, which completes the proof.

56. Define the function f as suggested from the positive rational numbers to the positive integers. This is a one-to-one function, because if we are given the value of $f(p/q)$, we can immediately recover p and q uniquely by writing $f(p/q)$ in base eleven and noting what appears to the left of the one and only A in the expansion and what appears to the right (and interpret these as numerals in base ten). Thus we have a one-to-one correspondence between the set of positive rational numbers and an infinite subset of the natural numbers, which is countable; therefore the set of positive rational numbers is countable.

SECTION 4.4 Solving Congruences

2. We need to show that $13 \cdot 937 \equiv 1 \pmod{2436}$, or in other words, that $13 \cdot 937 - 1 = 12180$ is divisible by 2436. A calculator shows that it is, since $12180 = 2436 \cdot 5$.

4. We need a number that when multiplied by 2 gives a number congruent to 1 modulo 17. Since $18 \equiv 1 \pmod{17}$ and $2 \cdot 9 = 18$, it follows that 9 is an inverse of 2 modulo 17.

6. **a)** The first step of the procedure in Example 1 yields $17 = 8 \cdot 2 + 1$, which means that $17 - 8 \cdot 2 = 1$, so -8 is an inverse. We can also report this as 9, because $-8 \equiv 9 \pmod{17}$.

b) We need to find s and t such that $34s + 89t = 1$. Then s will be the desired inverse, since $34s \equiv 1 \pmod{89}$ (i.e., $34s - 1 = -89t$ is divisible by 89). To do so, we proceed as in Example 2. First we go through the Euclidean algorithm computation that $\gcd(34, 89) = 1$:

$$\begin{aligned}
89 &= 2 \cdot 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34
\end{aligned}$$

Thus $s = -34$, so an inverse of 34 modulo 89 is -34, which can also be written as 55.

c) We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Example 2. In fact, once we get to a certain point below, all the work was already done in part **(b)**. First we go through the

Euclidean algorithm computation that $\gcd(144, 233) = 1$:

$$\begin{aligned}
233 &= 144 + 89 \\
144 &= 89 + 55 \\
89 &= 55 + 34 \\
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\
&= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\
&= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233
\end{aligned}$$

Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

d) The first step in the Euclidean algorithm calculation is $1001 = 5 \cdot 200 + 1$. Thus $-5 \cdot 200 + 1001 = 1$, and -5 (or 996) is the desired inverse.

8. If x is an inverse of a modulo m, then by definition $ax - 1 = tm$ for some integer t. If a and m in this equation both have a common divisor greater than 1, then 1 must also have this same common divisor, since $1 = ax - tm$. This is absurd, since the only positive divisor of 1 is 1. Therefore no such x exists.

10. We know from Exercise 6 that 9 is an inverse of 2 modulo 17. Therefore if we multiply both sides of this equation by 9 we will get $x \equiv 9 \cdot 7 \pmod{17}$. Since 63 **mod** $17 = 12$, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that $2 \cdot 12 = 24 \equiv 7 \pmod{17}$. This answer can also be stated as all integers of the form $12 + 17k$ for $k \in \mathbf{Z}$.

12. In each case we multiply both sides of the congruence by the inverse found in Exercise 6 and simplify. Our answers are not unique, of course—anything in the same congruence class works just as well.

a) We found that 55 is an inverse of 34 modulo 89, so $x \equiv 77 \cdot 55 = 4235 \equiv 52 \pmod{89}$. Check: $34 \cdot 52 = 1768 \equiv 77 \pmod{89}$.

b) We found that 89 is an inverse of 144 modulo 233, so $x \equiv 4 \cdot 89 = 356 \equiv 123 \pmod{233}$. Check: $144 \cdot 123 = 17712 \equiv 4 \pmod{233}$.

c) We found that -5 is an inverse of 200 modulo 1001, so $x \equiv 13 \cdot (-5) = -65 \equiv 936 \pmod{1001}$. (We could also leave the answer as -65.) Check: $200 \cdot 936 = 187200 \equiv 13 \pmod{1001}$.

14. Adding 12 to both sides of the congruence yields $12x^2+25x+12 \equiv 0 \pmod{11}$. (We chose something to add that would make the left-hand side easily factorable and the right-hand side equal to 0.) This is equivalent to $(3x+4)(4x+3) \equiv 0 \pmod{11}$. Because there are no non-zero divisors of 0 modulo 11, this congruence is true if and only if either $3x+4 \equiv 0 \pmod{11}$ or $4x+3 \equiv 0 \pmod{11}$. (This would have been more complicated modulo a non-prime modulus, because there would be nonzero divisors of 0.) We solve these linear congruences by inspection (guess and check) or using the Euclidean algorithm to find inverses of 3 and 4 (or using computer algebra software), to yield $x=6$ or $x=2$. In fact, typing "`msolve(12^2+25x=10,11)`" into *Maple* produces this solution set.

16. **a)** We can find inverses using the technique shown in Example 2. With a little work (or trial and error, which is actually faster in this case), we find that $2\cdot 6 \equiv 1 \pmod{11}$, $3\cdot 4 \equiv 1 \pmod{11}$, $5\cdot 9 \equiv 1 \pmod{11}$, and $7\cdot 8 \equiv 1 \pmod{11}$. Actually, the problem does not ask us to show these pairs explicitly, only to show that they exist. The general argument given in Exercise 18 shows this.
b) In this specific case we can compute $10! = 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10 = 1\cdot(2\cdot6)\cdot(3\cdot4)\cdot(5\cdot9)\cdot(7\cdot8)\cdot10 \equiv 1\cdot1\cdot1\cdot1\cdot10 = 10 \equiv -1 \pmod{11}$. Alternatively, we can use the proof in Exercise 18.

18. **a)** Every positive integer less than p has an inverse modulo p, and by Exercise 7 this inverse is unique among positive integers less than p. This follows from Theorem 1, since every number less than p must be relatively prime to p (because p is prime it has no smaller divisors). We can group each positive integer less than p with its inverse. The only issue is whether some numbers are their own inverses, in which case this grouping does not produce pairs. By Exercise 17 only 1 and -1 (which is the same as $p-1$ modulo p) are their own inverses. Therefore all the other positive integers less than p can be grouped into pairs consisting of inverses of each other, and there are clearly $(p-1-2)/2 = (p-3)/2$ such pairs.
b) When we compute $(p-1)!$, we can write the product by grouping the pairs of inverses modulo p. Each such pair produces the product 1 modulo p, so modulo p the entire product is the same as the product of the only unpaired elements, namely $1\cdot(p-1) = p-1$. Since this equals -1 modulo p, our proof is complete.
c) By the contrapositive of what we have just proved, we can conclude that if $(n-1)! \not\equiv -1 \pmod{n}$ then n is not prime.

20. Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $3\cdot4\cdot5 = 60$. Using the notation in the text, we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1,2,3$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm (as in Example 2); we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2\cdot20\cdot2 + 1\cdot15\cdot3 + 3\cdot12\cdot3 = 233 \equiv 53 \pmod{60}$. So the solutions are all integers of the form $53+60k$, where k is an integer.

22. By definition, the first congruence can be written as $x = 6t+3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t+3 \equiv 4 \pmod{7}$, which can easily be solved to show that $t \equiv 6 \pmod{7}$. From this we can write $t = 7u+6$ for some integer u. Thus $x = 6t+3 = 6(7u+6)+3 = 42u+39$. Thus our answer is all numbers congruent to 39 modulo 42. We check our answer by confirming that $39 \equiv 3 \pmod{6}$ and $39 \equiv 4 \pmod{7}$.

24. By definition, the first congruence can be written as $x = 2t+1$ where t is an integer. Substituting this expression for x into the second congruence tells us that $2t+1 \equiv 2 \pmod{3}$, which can easily be solved to show that $t \equiv 2 \pmod{3}$. From this we can write $t = 3u+2$ for some integer u. Thus $x = 2t+1 = 2(3u+2)+1 = 6u+5$. Next we have $6u+5 \equiv 3 \pmod{5}$, which we solve to get $u \equiv 3 \pmod{5}$, so $u = 5v+3$. Thus $x = 6(5v+3)+5 = 30v+23$. For the last congruence we have $30v+23 \equiv 4 \pmod{11}$; solving this is a little harder but trial and error or the applying the methods of Example 2 to get an inverse and then Example 3 shows that $v \equiv 10 \pmod{11}$. Therefore $x = 30(11w + 10) + 23 = 330w + 323$. So our solution is all integers congruent to 323 modulo 330. We check our answer by confirming that $323 \equiv 1 \pmod 2$, $323 \equiv 2 \pmod 3$, $323 \equiv 3 \pmod 5$, and $323 \equiv 4 \pmod{11}$.

26. We cannot apply the Chinese remainder theorem directly, since the moduli are not pairwise relatively prime. However, we can, using the Chinese remainder theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 5 \pmod 6$, we must have $x \equiv 5 \equiv 1 \pmod 2$ and $x \equiv 5 \equiv 2 \pmod 3$. Similarly, from the second congruence we must have $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 5$; and from the third congruence we must have $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$. These can be solved using the Chinese remainder theorem (see Example 5) to yield $x \equiv 23 \pmod{30}$. Therefore the solutions are all integers of the form $23 + 30k$, where k is an integer.

28. This is just a restatement of the Chinese remainder theorem. Given any such a we can certainly compute $a \textbf{ mod } m_1$, $a \textbf{ mod } m_2$, $\ldots$, $a \textbf{ mod } m_n$ to represent it. The Chinese remainder theorem says that there is only one nonnegative integer less than m yielding each n-tuple, so the representation is unique.

30. We follow the hint and suppose that there are two solutions to the set of congruences. Thus suppose that $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ for each i. We want to show that these solutions are the same modulo m; this will guarantee that there is only one nonnegative solution less than m. The assumption certainly implies that $x \equiv y \pmod{m_i}$ for each i. But then Exercise 29 tells us that $x \equiv y \pmod m$, as desired.

32. We are asked to solve $x \equiv 0 \pmod 5$ and $x \equiv 1 \pmod 3$. We know from the Chinese remainder theorem that there is a unique answer modulo 15. It is probably quickest just to look for it by dividing each multiple of 5 by 3, and we see immediately that $x = 10$ satisfies the condition. Thus the solutions are all integers congruent to 10 modulo 15. If the numbers involved were larger, then we could use the technique implicit in the proof of Theorem 2 (see Exercise 53).

34. Fermat's little theorem tells us that $23^{40} \equiv 1 \pmod{41}$. Therefore $23^{1002} = (23^{40})^{25} \cdot 23^2 \equiv 1^{25} \cdot 529 = 529 \equiv 37 \pmod{41}$.

36. By Exercise 35, an inverse of 5 modulo 41 is 5^{39}. We can stop there, but presumably we'd like a simpler answer. This could be calculated using modular exponentiation (or, from a practical point of view, with computer algebra software). The simplest form of this is 33, and it is easy to check that $5 \cdot 33 = 165 \equiv 1 \pmod{41}$.

38. **a)** By Fermat's little theorem we know that $3^4 \equiv 1 \pmod 5$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod 5$, so $3^{302} \textbf{ mod } 5 = 4$. Similarly, $3^6 \equiv 1 \pmod 7$; therefore $3^{300} = (3^6)^{50} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod 7$, so $3^{302} \textbf{ mod } 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \textbf{ mod } 11 = 9$.

b) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This was a particularly trivial application of the Chinese remainder theorem.)

40. Note that the prime factorization of 42 is $2 \cdot 3 \cdot 7$. So it suffices to show that $2 \mid n^7 - n$, $3 \mid n^7 - n$, and $7 \mid n^7 - n$. The first is trivial ($n^7 - n$ is either "odd minus odd" or "even minus even," both of which are even), and each of the other two follows immediately from Fermat's little theorem, because $n^7 - n \equiv (n^2)^3 \cdot n - n \equiv 1 \cdot n - n = 0 \pmod 3$ and $n^7 - n \equiv n - n = 0 \pmod 7$.

42. To decide whether $2^{13}-1=8191$ is prime, we need only look for a prime factor not exceeding $\sqrt{8191}\approx 90.5$. By Exercise 41 every such prime divisor must be of the form $26k+1$. The only candidates are therefore 53 and 79. We easily check that neither is a divisor, and so we conclude that 8191 is prime.

We can take the same approach for $2^{23}-1=8{,}388{,}607$, but we might worry that there will be far too many potential divisors to test, since we must go as far as 2896. By Exercise 41 every prime divisor of $2^{23}-1$ must be of the form $46k+1$. The first candidate divisor is therefore 47. Luckily $47\mid 8{,}388{,}607$, so we conclude that this Mersenne number is not prime.

44. Let $x_k=b^{(n-1)/2^k}=b^{2^{s-k}t}$, for $k=0,1,2,\ldots,s$. Because n is prime and $n\nmid b$, Fermat's little theorem tells us that $x_0=b^{n-1}\equiv 1 \pmod n$. By Exercise 17, because $x_1^2=(b^{(n-1)/2})^2=x_0\equiv 1\pmod n$, either $x_1\equiv -1\pmod n$ or $x_1\equiv 1\pmod n$. If $x_1\equiv 1\pmod n$, because $x_2^2=x_1\equiv 1\pmod n$, either $x_2\equiv -1\pmod n$ or $x_2\equiv 1\pmod n$. In general, if we have found that $x_0\equiv x_1\equiv x_2\equiv\cdots\equiv x_k\equiv 1\pmod n$, with $k<s$, then, because $x_{k+1}^2=x_k\equiv 1\pmod n$, we know that either $x_{k+1}\equiv -1\pmod n$ or $x_{k+1}\equiv 1\pmod n$. Continuing this procedure for $k=1,2,\ldots,s$, we find that either $x_s=b^t\equiv 1\pmod n$, or $x_k\equiv -1\pmod n$ for some integer k with $0\le k\le s$. Hence, n passes Miller's test for the base b.

46. This follows from Exercise 49, taking $m=1$. Alternatively, we can argue directly as follows. Factor $1729=7\cdot 13\cdot 19$. We must show that this number meets the definition of Carmichael number, namely that $b^{1728}\equiv 1\pmod{1729}$ for all b relatively prime to 1729. Note that if $\gcd(b,1729)=1$, then $\gcd(b,7)=\gcd(b,13)=\gcd(b,19)=1$. Using Fermat's little theorem we find that $b^6\equiv 1\pmod 7$, $b^{12}\equiv 1\pmod{13}$, and $b^{18}\equiv 1\pmod{19}$. It follows that $b^{1728}=(b^6)^{288}\equiv 1\pmod 7$, $b^{1728}=(b^{12})^{144}\equiv 1\pmod{13}$, and $b^{1728}=(b^{18})^{96}\equiv 1\pmod{19}$. By Exercise 29 (or the Chinese remainder theorem) it follows that $b^{1728}\equiv 1\pmod{1729}$, as desired.

48. Let b be a positive integer with $\gcd(b,n)=1$. The $\gcd(b,p_j)=1$ for $j=1,2,\ldots,k$, and hence, by Fermat's little theorem, $b^{p_j-1}\equiv 1\pmod{p_j}$ for $j=1,2,\ldots,k$. Because $p_j-1\mid n-1$, there are integers t_j with $t_j(p_j-1)=n-1$. Hence for each j we know that $b^{n-1}=b^{(p_j-1)t_j}=(b^{(p_j-1)})^{t_j}\equiv 1\pmod{p_j}$. Therefore $b^{n-1}\equiv 1\pmod n$, as desired.

50. We could use the technique shown in the proof of Theorem 2 to solve each part, or use the approach in our solution to Exercise 32, but since there are so many to do here, it is simpler just to write out all the representations of 0 through 27 and find those given in each part. This task is easily done, since the pattern is clear:

$0=(0,0)$	$7=(3,0)$	$14=(2,0)$	$21=(1,0)$
$1=(1,1)$	$8=(0,1)$	$15=(3,1)$	$22=(2,1)$
$2=(2,2)$	$9=(1,2)$	$16=(0,2)$	$23=(3,2)$
$3=(3,3)$	$10=(2,3)$	$17=(1,3)$	$24=(0,3)$
$4=(0,4)$	$11=(3,4)$	$18=(2,4)$	$25=(1,4)$
$5=(1,5)$	$12=(0,5)$	$19=(3,5)$	$26=(2,5)$
$6=(2,6)$	$13=(1,6)$	$20=(0,6)$	$27=(3,6)$

Now we can read off the answers.

a) 0 **b)** 21 **c)** 1 **d)** 22 **e)** 2 **f)** 24 **g)** 14 **h)** 19 **i)** 27

52. To add 4 and 7 we first find that 4 is represented by $(1,4)$ and that 7 is represented by $(1,2)$. Adding coordinate-wise, we see that the sum is represented by $(1+1,4+2)=(2,6)=(2,1)$; we are working modulo 5 in the second coordinate. Then we find $(2,1)$ in the table and see that it represents 11. Therefore we conclude that $4+7=11$. Note that we can only compute answers less than $3\cdot 5=15$ using this method.

54. We calculate 2^i **mod** 19 for $i = 1, 2, \ldots, 18$ and see that we get 18 different values. The values are 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1.

56. The proof is the same as the proof for the corresponding identity for the real numbers. To show that $\log_r(ab) \equiv \log_r a + \log_r b \pmod{p-1}$, it suffices (by definition) to show that $r^{\log_r a + \log_r b} \equiv ab \pmod{p-1}$. But $r^{\log_r a + \log_r b} = r^{\log_r a} \cdot r^{\log_r b} \equiv a \cdot b \pmod{p-1}$.

58. We square the first five positive integers and reduce modulo 11, obtaining 1, 4, 9, 5, 3. The squares of the next five are necessarily the same set of numbers modulo 11, since $(-x)^2 = x^2$, so we are done. Therefore the quadratic residues modulo 11 are all integers congruent to 1, 3, 4, 5, or 9 modulo 11.

60. Consider the list x^2 **mod** p as x runs from 1 to $p-1$ inclusive. This gives us $p-1$ numbers between 1 and $p-1$ inclusive. By Exercise 59 every a that appears in this list appears exactly twice. Therefore exactly half of the $p-1$ numbers must appear in the list (i.e., be quadratic residues).

62. First assume that $\left(\frac{a}{p}\right) = 1$. Then the congruence $x^2 \equiv a \pmod{p}$ has a solution, say $x = s$. By Fermat's little theorem $a^{(p-1)/2} = (s^2)^{(p-1)/2} = s^{p-1} \equiv 1 \pmod{p}$, as desired. Next consider the case $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \pmod{p}$ has no solution. Let i be an integer between 1 and $p-1$, inclusive. By Theorem 1, i has an inverse i' modulo p, and therefore there is an integer j, namely $i'a$, such that $ij \equiv a \pmod{p}$. Furthermore, since the congruence $x^2 \equiv a \pmod{p}$ has no solution, $j \neq i$. Thus we can group the integers from 1 to $p-1$ into $(p-1)/2$ pairs each with the product a. Multiplying these pairs together, we find that $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$. But now Wilson's theorem (see Exercise 18) tells us that this latter value is -1, again as desired.

64. If $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is even, so the right-hand side of the equivalence in Exercise 62 with $a = -1$ is $+1$, that is, -1 is a quadratic residue. Conversely, if $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd, so the right-hand side of the equivalence in Exercise 62 with $a = -1$ is -1, that is, -1 is not a quadratic residue.

66. We follow the hint. Working modulo 3, we want to solve $x^2 \equiv 16 \equiv 1$. It is easy to see that there are exactly two solutions modulo 3, namely $x = 1$ and $x = 2$. Similarly we find the solutions $x = 1$ and $x = 4$ to $x^2 \equiv 16 \equiv 1 \pmod{5}$; and the solutions $x = 3$ and $x = 4$ to $x^2 \equiv 16 \equiv 2 \pmod{7}$. Therefore we want to find values of x modulo $3 \cdot 5 \cdot 7 = 105$ such that $x \equiv 1$ or $2 \pmod{3}$, $x \equiv 1$ or $4 \pmod{5}$ and $x \equiv 3$ or $4 \pmod{7}$. We can do this by applying the Chinese remainder theorem (as in Example 5) eight times, for the eight combinations of these values. For example, to solve $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, and $x \equiv 3 \pmod{7}$, we find that $m = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$, $y_1 = 2$, $y_2 = 1$, $y_3 = 1$, so $x \equiv 1 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 136 \equiv 31 \pmod{105}$. Doing the similar calculation with the other seven possibilities yields the other solutions modulo 105: $x = 4$, $x = 11$, $x = 46$, $x = 59$, $x = 74$, $x = 94$ and $x = 101$.

SECTION 4.5 Applications of Congruences

2. In each case we need to compute k **mod** 101 by dividing by 101 and finding the remainders. This can be done with a calculator that keeps 13 digits of accuracy internally. Just divide the number by 101, subtract off the integer part of the answer, and multiply the fraction that remains by 101. The result will be almost exactly an integer, and that integer is the answer.

a) 58 **b)** 60 **c)** 52 **d)** 3

4. We compute as follows: $h(k_1) = 1524$; $h(k_2) = 578$; $h(k_3) = 578$, which collides, $h(k_3, 1) = 2505$, so k_3 is assigned memory location 2505; $h(k_4) = 2376$; $h(k_5) = 3960$; $h(k_6) = 1526$; $h(k_7) = 2854$; $h(k_8) = 1526$, which collides, $h(k_8, 1) = 4927$, so k_8 is assigned memory location 4927; $h(k_9) = 3960$, which collides, $h(k_9, 1) = 6100 \equiv 1131 \pmod{4969}$, so k_9 is assigned memory location 1131; $h(k_{10}) = 3960$, which collides, $h(k_{10}, 1) = 4702$, so k_{10} is assigned memory location 4702. Notice that we never had to go above $i = 1$ in the probing sequence.

6. We just calculate using the formula. We are given $x_0 = 3$. Then $x_1 = (4 \cdot 3 + 1) \textbf{ mod } 7 = 13 \textbf{ mod } 7 = 6$; $x_2 = (4 \cdot 6 + 1) \textbf{ mod } 7 = 25 \textbf{ mod } 7 = 4$; $x_3 = (4 \cdot 4 + 1) \textbf{ mod } 7 = 17 \textbf{ mod } 7 = 3$. At this point the sequence must continue to repeat $3, 6, 4, 3, 6, 4, \ldots$ forever.

8. We assume that the input to this procedure consists of a modulus ($m \geq 2$), a multiplier (a), an increment (c), a seed (x_0), and the number (n) of pseudorandom numbers desired. The output will be the sequence $\{x_i\}$.

> **procedure** *pseudorandom*$(m, a, c, x_0, n$: nonnegative integers)
> **for** $i := 1$ **to** n
> $x_i := (ax_{i-1} + c) \textbf{ mod } m$

10. We follow the instructions. Because $3792^2 = 14379264$, the middle four digits are 3792, which is the number we started with. So this sequence is not random at all—it's constant! Similarly, $2916^2 = 08503056$, $5030^2 = 25300900$, $3009^2 = 09054081$, and $0540^2 = 00291600$, which gives us back the number we started with, so this sequence degenerates into a repeating sequence with period 4.

12. We are told to apply the formula $x_{n+1} = x_n^2 \textbf{ mod } 11$, starting with $x_0 = 3$. Thus $x_1 = 3^2 \textbf{ mod } 11 = 9$, $x_3 = 9^2 \textbf{ mod } 11 = 4$, $x_4 = 4^2 \textbf{ mod } 11 = 5$, $x_5 = 5^2 \textbf{ mod } 11 = 3$, and we are back where we started. The sequence generated here is $3, 9, 4, 5, 3, 9, 4, 5, \ldots$.

14. If a string contains an odd number of errors, then the number of 1's in the string with its check bit will differ by an odd number from what it should be, which means it will be an odd number, rather than the expected even number, and we will know that there is an error. If the string contains an even number of errors, then the number of 1's in the string with its check bit will differ by an even number from what it should be, which means it will be an even number, as expected, and we will not know that anything is wrong.

16. We know that $1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot Q + 9 \cdot 1 + 10 \cdot 8 \equiv 0 \pmod{11}$. This simplifies to $130 + 8Q \equiv 0 \pmod{11}$. We subtract 130 from both sides and simplify to $8Q \equiv 2 \pmod{11}$, since $-130 = -12 \cdot 11 + 2$. It is now a simple matter to use trial and error (or the methods of Section 4.4) to find that $Q = 3$ (since $24 \equiv 2 \pmod{11}$).

18. In each case we just have to compute $x_1 + x_2 + \cdots + x_{10} \textbf{ mod } 9$ The easiest way to do this by hand is to "cast out nines," i.e., throw away sums of 9 as we come to them.

a) $7 + 5 + 5 + 5 + 6 + 1 + 8 + 8 + 7 + 3 \textbf{ mod } 9 = 1$ **b)** 5 **c)** 2 **d)** 0

20. In each case we want to solve the equation $x_1 + x_2 + \cdots + x_{10} \equiv x_{11} \pmod 9$ for the missing digit, which is easily done by inspection (one can throw away 9's).

a) $Q+1+2+2+3+1+3+9+7+8 \equiv 4 \pmod 9 \Rightarrow Q \equiv 4 \pmod 9 \Rightarrow Q = 4$

b) $6+7+0+2+1+2+0+Q+9+8 \equiv 8 \pmod 9 \Rightarrow Q+8 \equiv 8 \pmod 9 \Rightarrow Q \equiv 0 \pmod 9$. There are two single-digit numbers Q that makes this true: $Q = 0$ and $Q = 9$, so it is impossible to know for sure what the smudged digit was.

c) $2+7+Q+4+1+0+0+7+7+3 \equiv 4 \pmod 9 \Rightarrow Q+4 \equiv 4 \pmod 9 \Rightarrow Q \equiv 0 \pmod 9$. There are two single-digit numbers Q that makes this true: $Q = 0$ and $Q = 9$, so it is impossible to know for sure what the smudged digit was.

d) $2+1+3+2+7+9+0+3+2+Q \equiv 1 \pmod 9 \Rightarrow Q+2 \equiv 1 \pmod 9 \Rightarrow Q \equiv 8 \pmod 9 \Rightarrow Q = 8$

22. If one digit is changed to a value not congruent to it modulo 9, then the modular equivalence implied by the equation in the preamble will no longer hold. Therefore all single digit errors are detected except for the substitution of a 9 for a 0 or vice versa.

24. In each case we want to solve the equation $3x_1 + x_2 + 3x_3 + x_4 + \cdots + 3x_{11} + x_{12} \equiv 0 \pmod{10}$ for x_{12}, which can be done mentally, because we need to keep track of only the last digit.

a) $3\cdot 7+3+3\cdot 2+3+3\cdot 2+1+3\cdot 8+4+3\cdot 4+3+3\cdot 4+x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 5$

b) $3\cdot 6+3+3\cdot 6+2+3\cdot 3+9+3\cdot 9+1+3\cdot 3+4+3\cdot 6+x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 2$

c) $3\cdot 0+4+3\cdot 5+8+3\cdot 7+3+3\cdot 2+0+3\cdot 7+2+3\cdot 0+x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 0$

d) $3\cdot 9+3+3\cdot 7+6+3\cdot 4+3+3\cdot 2+3+3\cdot 3+4+3\cdot 1+x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 3$

26. Yes. Any single digit error will change, say, x to y, and one side of the congruence given in Example 5 will differ by either $x-y$ or $3(x-y)$ from its true value. Because $x-y \not\equiv 0$ and $3(x-y) \not\equiv 0 \pmod{10}$ (since 3 is relatively prime to 10), the congruence will no longer hold.

28. In each case we need to compute the remainder of the given 14-digit number upon division by 7.

a) $10237424413392 \textbf{ mod } 7 = 1$ **b)** $00032781811234 \textbf{ mod } 7 = 4$

c) $00611232134231 \textbf{ mod } 7 = 5$ **d)** $00193222543435 \textbf{ mod } 7 = 5$

30. A change in the digit in the n^{th} column from the right in the 14-digit number formed by the first 14 digits of the airline ticket identification number (with $n = 0$ corresponding to the units digit), say from x to y, will cause this 14-digit number to differ from its correct value by $(x-y)10^n$. If this equals 0 modulo 7, then the error will not be detected. Because 7 and 10 are relatively prime, that will happen if and only if $|x-y| = 7$; therefore we can detect errors except $0 \leftrightarrow 7$, $1 \leftrightarrow 8$, $2 \leftrightarrow 9$. The same reasoning applies to the check digit (although of course 7, 8, and 9 are invalid digits for the check digit anyway).

32. It follows from the preamble that we need to compute $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \textbf{ mod } 11$ in order to determine the check digit d_8.

a) $3\cdot 1+4\cdot 5+5\cdot 7+6\cdot 0+7\cdot 8+8\cdot 6+9\cdot 8 \textbf{ mod } 11 = 3$

b) $3\cdot 1+4\cdot 5+5\cdot 5+6\cdot 3+7\cdot 7+8\cdot 3+9\cdot 4 \textbf{ mod } 11 = 10$, so the check digit is X.

c) $3\cdot 1+4\cdot 0+5\cdot 8+6\cdot 9+7\cdot 7+8\cdot 0+9\cdot 8 \textbf{ mod } 11 = 9$

d) $3\cdot 1+4\cdot 3+5\cdot 8+6\cdot 3+7\cdot 8+8\cdot 1+9\cdot 1 \textbf{ mod } 11 = 3$

34. Yes. Any single digit error will change, say, x to y, and one side of the congruence given in the preamble will differ by $a(x-y)$, for some $a \in \{1,3,4,5,6,7,8,9\}$, from its true value. Each of those values of a is relatively prime to 11, so $a(x-y) \not\equiv 0 \pmod{11}$ and the congruence will no longer hold.

SECTION 4.6 Cryptography

2. These are straightforward arithmetical calculations, as in Exercise 1.
a) WXST TSPPYXMSR **b)** NOJK KJHHPODJI **c)** QHAR RABBYHCAJ

4. We just need to "subtract 3" from each letter. For example, E goes down to B, and B goes down to Y.
a) BLUE JEANS **b)** TEST TODAY **c)** EAT DIM SUM

6. Under these assumptions we guess that the plaintext E became the ciphertext X. Since the number for E is 4 and the number for X is 23, $k = 23 - 4 = 19$.

8. Because of the word JVVU we guess that the ciphertext V might be the plaintext E or O. If it is the former, then the shift would have to be $21 - 4 = 17$. Applying the inverse of that shift to the message yields MEN LOVE TO WONDER, AND THAT IS THE SEED OF SCIENCE.

10. If the enciphering function is $f(p) = (p+k) \mathbf{~mod~} 26$, then the deciphering function is $f^{-1}(p) = (p-k) \mathbf{~mod~} 26$. Thus we seek a k such that $k \equiv -k \pmod{26}$, and the unique solution is $k = 13$.

12. If $\overline{a}$ is the inverse of a modulo 26, then the decryption function for the encryption function $c = (ap+b) \mathbf{~mod~} 26$ is $p = \overline{a}(c-b) \mathbf{~mod~} 26 = (\overline{a}c - \overline{a}b) \mathbf{~mod~} 26$. Clearly two different pairs (a, b) cannot give the same encryption function, so we need to solve the system of congruences $\overline{a} \equiv a \pmod{26}$ and $b \equiv -\overline{a}b \pmod{26}$. Only 1 and -1 (which is the same as 25) are their own multiplicative inverses modulo 26 (this can be verified by asking a computer algebra system to compute all the inverses), so there are two cases. If $a = 1$, then the second congruence becomes $b \equiv -b \pmod{26}$, whose solutions are $b = 0$ and $b = 13$. This says that the identity function $c = p \mathbf{~mod~} 26$ satisfies the given condition (although that was obvious and not very interesting), and so does $c = (p + 13) \mathbf{~mod~} 26$. If $a = -1$, then the second congruence becomes $b \equiv b \pmod{26}$, which is satisfied by all values of b. Therefore all encryption functions of the form $c = (-p + b) \mathbf{~mod~} 26$ also have themselves as the corresponding decryption function. The answer to the question phrased in terms of pairs is $(1, 0)$, $(1, 13)$, and $(-1, b)$ (or, equivalently, $(25, b)$) for all b.

14. Within each block of five letters (GRIZZ LYBEA RSXXX) we send the first letter to the third letter, the second letter to the fifth letter, and so on. So the encrypted message is IZGZR BELAY XXRXS.

16. One method, using technology, would be to try all possibilities. For $n = 2, 3, 4, \ldots$, have the computer go through all $n!$ permutations of $\{1, 2, 3, \ldots, n\}$ and for each one permute blocks of n letters of the ciphertext, printing out the resulting plaintext on the computer screen. You, a human, can look at them and figure out which ones make sense as a message.

18. The plaintext string in numbers is 18-13-14-22-5-0-11-11. We add the string for the key repeated twice, 1-11-20-4-1-11-20-4, to obtain the string 19-24-8-0-6-11-5-15, which in letters is TYIAGLFP.

20. A cryptosystem is a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, as explained in Definition 1. We follow the discussion of Example 7. As there, $\mathcal{P}$ and $\mathcal{C}$ are strings of elements of $\mathbf{Z}_{26}$. The set of keys is the set of strings over $\mathbf{Z}_{26}$ as well. The set of encryption functions is the set of functions described in the preamble to Exercise 18. The set of decryption functions is the same, because decrypting with the string a-b-c-$\ldots$ is the same as encrypting with the string $(-a)$-$(-b)$-$(-c)$-$\ldots$

22. Suppose the length of the key string is l. We can apply the frequency method, explained in Example 5 and the preceding discussion, to the letters in positions 1, $1 + l$, $1 + 2l$, $\ldots$ to determine the first letter of the key string (viewed as a number from 0 to 25), then do the same for the second letter, and so on up to the l^{th} letter.

24. Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C = P^{13}$ **mod** 2537 for $P = 19$, $P = 1900$, and $P = 210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.

26. First we find d, the inverse of $e = 17$ modulo $52 \cdot 60$. A computer algebra system tells us that $d = 2753$. Next we have the CAS compute c^d **mod** n for each of the four given numbers: 3185^{2753} **mod** $3233 = 1816$ (which are the letters SQ), 2038^{2753} **mod** $3233 = 2008$ (which are the letters UI), 2460^{2753} **mod** $3233 = 1717$ (which are the letters RR), and 2550^{2753} **mod** $3233 = 0411$ (which are the letters EL). The message is SQUIRREL.

28. If $M \equiv 0 \pmod{n}$, then $C \equiv M^e \equiv 0 \pmod{n}$ and so $C^d \equiv 0 \equiv M \pmod{n}$. Otherwise, $\gcd(M,p) = p$ and $\gcd(M,q) = 1$, or $\gcd(M,p) = 1$ and $\gcd(M,q) = q$. By symmetry it suffices to consider the first case, where $M \equiv 0 \pmod{p}$. We have $C^d \equiv (M^e)^d \equiv (0^e)^d \equiv 0 \equiv M \pmod{p}$. As in the case considered in the text, $de = 1 + k(p-1)(q-1)$ for some integer k, so

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot M^{(q-1)^{k(p-1)}} \equiv M \cdot 1 \equiv M \pmod{q}$$

by Fermat's little theorem. Thus by the Chinese remainder theorem, $C^d \equiv M \pmod{pq}$.

30. We follow the steps given in the text, with $p = 101$, $a = 2$, $k_1 = 7$, and $k_2 = 9$. Using *Maple*, we verify that 2 is a primitive root modulo 101, by noticing that 2^k as k runs from 0 to 99 produce distinct values (and of course 2^{100} **mod** $101 = 1$). We find that 2^7 **mod** $101 = 27$. So in Step (2), Alice sends 27 to Bob. Similarly, in Step (3), Bob sends 2^9 **mod** $101 = 7$ to Alice. In Step (4) Alice computes 7^7 **mod** $101 = 90$, and in Step (5) Bob computes 27^9 **mod** $101 = 90$. These are the same, of course, and thus 90 is the shared key.

32. When broken into blocks and translated into numbers the message is 0120 2413 1422. Alice applies her decryption transformation $D_{(2867,7)}(x) = x^{1183}$ **mod** 2867 to each block, which we compute with a CAS to give 1665 1728 2123. Next she applies Bob's encryption transformation $E_{(3127,21)}(x) = x^{21}$ **mod** 3127 to each block, which we compute with a CAS to give 2806 1327 0412. She sends that to Bob. Only Bob can read it, which he does by first applying his decryption transformation $D_{(3127,21)}(x) = x^{1149}$ **mod** 3127 to each block, recovering 1665 1728 2123, and then applying Alice's encryption transformation $E_{(2867,7)}(x) = x^7$ **mod** 2867 to each of these blocks, recovering the original 0120 2413 1422, BUY NOW.

SUPPLEMENTARY EXERCISES FOR CHAPTER 4

2. **a)** Each week consists of seven days. Therefore to find how many (whole) weeks there are in n days, we need to see how many 7's there are in n. That is exactly what n **div** 7 tells us.

b) Each day consists of 24 hours. Therefore to find how many (whole) days there are in n hours, we need to see how many 24's there are in n. That is exactly what n **div** 24 tells us.

4. Let $q = \left\lceil \dfrac{a}{d} - \dfrac{1}{2} \right\rceil$ and $r = a - dq$. Then we have forced $a = dq + r$, so it remains to prove that $-d/2 < r \le d/2$. Now since $q - 1 < \dfrac{a}{d} - \dfrac{1}{2} \le q$, we have (by multiplying through by d and adding $d/2$) $dq - \dfrac{d}{2} < a \le dq + \dfrac{d}{2}$, so $-\dfrac{d}{2} < a - dq \le \dfrac{d}{2}$, as desired.

6. By Exercise 38 in Section 4.1, the square of an integer is congruent to either 0 or 1 modulo 4, where obviously the odd integers have squares congruent to 1 modulo 4. The sum of two of these is therefore congruent to 2 modulo 4, so cannot be a square.

8. If there were integer solutions to this equation, then by definition we would have $x^2 \equiv 2 \pmod{5}$. However we easily compute (as in Exercise 40 in Section 4.1) that the square of an integer of the form $5k$ is congruent to 0 modulo 5; the square of an integer of the form $5k+1$ is congruent to 1 modulo 5; the square of an integer of the form $5k+2$ is congruent to 4 modulo 5; the square of an integer of the form $5k+3$ is congruent to 4 modulo 5; and the square of an integer of the form $5k+4$ is congruent to 1 modulo 5. This is a contradiction, so no solutions exist.

10. The number 3 plays the same role in base two that the number 11 plays in base ten (essentially because $(11)_2 = 3$). The divisibility test for 11 in base ten is that $d_n d_{n-1} \ldots d_2 d_1 d_0$ is divisible by 11 if and only if the alternating sum $d_0 - d_1 + d_2 - \cdots + (-1)^n d_n$ is divisible by 11. The corresponding rule here is that $(d_n d_{n-1} \ldots d_2 d_1 d_0)_2$ is divisible by 3 if and only if the alternating sum $d_0 - d_1 + d_2 - \cdots + (-1)^n d_n$ is divisible by 3. For example, $27 = (11011)_2$ is divisible by 3 because $1 - 1 + 0 - 1 + 1 = 0$ is divisible by 3. The proof follows from the fact that $2^n - 1 \equiv 0 \pmod{3}$ if n is even and $2^n + 1 \equiv 0 \pmod{3}$ if n is odd. Thus we have

$$\begin{aligned}(d_n d_{n-1} \ldots d_2 d_1 d_0)_2 &= d_0 + 2d_1 + 2^2 d_2 + 2^3 d_3 + \cdots 2^n d_n \\ &= d_0 + (3k_1 - 1)d_1 + (3k_2 + 1)d_2 + (3k_3 - 1)d_3 + \cdots + (3k_n + (-1)^n)d_n \\ &= [d_0 - d_1 + d_2 - \cdots + (-1)^n d_n] + [3(k_1 d_1 + k_2 d_2 + k_3 d_3 + \cdots + k_n d_n)]\end{aligned}$$

for integers $k_1 = 1$, $k_2 = 1$, $k_3 = 3$, $k_4 = 5$, $k_5 = 11$, ... The second bracketed expression is always divisible by 3, so the entire number is divisible by 3 if and only if the alternating sum is.

12. As we see from Exercise 11, at most n questions (guesses) are needed. Furthermore, at least this many yes/no questions are needed as well, since if we asked fewer questions, then by the pigeonhole principle, two numbers would produce the same set of answers and we would be unable to guess the number accurately. Thus the complexity is n questions. (The case $n = 0$ is not included, since in that case no questions are needed.) We are assuming throughout this exercise and the previous one that the inclusive sense of "between" was intended.

14. First note that since both a and b must be greater than 1, the sequences $\lfloor ka \rfloor$ and $\lfloor kb \rfloor$ do not list any positive integer twice. The issue is whether any positive integer is listed in both sequences, or whether some positive integer is omitted altogether. Let $N(x,n)$ denote the number of positive integers in the set $\{\, \lfloor kx \rfloor \mid k \text{ is a positive integer} \,\}$ that are less than or equal to n. Then it is enough to prove that $N(a,n) + N(b,n) = n$ for all positive integers n. (That way no positive integer could be left out or appear twice when we consider all the numbers $\lfloor ka \rfloor$ and $\lfloor kb \rfloor$.) Now $N(a,n)$ is the number of positive integers k for which $\lfloor ka \rfloor \le n$, which is just the number of positive integers k for which $ka < n+1$, since a is irrational, and this is clearly $\lfloor (n+1)/a \rfloor$. We have a similar result for b. Let $f(x)$ denote the fractional part of x (i.e., $f(x) = x - \lfloor x \rfloor$). Then we have

$$N(a,n) + N(b,n) = \left\lfloor \frac{n+1}{a} \right\rfloor + \left\lfloor \frac{n+1}{b} \right\rfloor = \frac{n+1}{a} - f\left(\frac{n+1}{a}\right) + \frac{n+1}{b} - f\left(\frac{n+1}{b}\right).$$

But the sum of the first and third terms of the right-hand side here is $n+1$, since we are given that $(1/a) + (1/b) = 1$. The second and fourth terms are each fractions strictly between 0 and 1, and the entire expression is an integer, so they must sum to 1. Therefore the displayed value is $n + 1 - 1 = n$, as desired.

16. The first few of these are $Q_1 = 2$, $Q_2 = 3$, $Q_3 = 7$, $Q_4 = 25$, and $Q_5 = 121$. Although the first three are prime, the next two are not. In fact, a CAS tells us that Q_4 through $Q_{10} = 3{,}628{,}801 = 11 \cdot 329{,}891$ are all not prime. The only other primes among the first 100 are Q_{11}, Q_{27}, Q_{37}, Q_{41}, Q_{73}, and Q_{77}.

18. We can give a nice proof by contraposition here, by showing that if n is not prime, then the sum of its divisors is not $n+1$. There are two cases. If $n = 1$, then the sum of the divisors is $1 \ne 1+1$. Otherwise n is composite, so can be written as $n = ab$, where both a and b are divisors of n different from 1 and from n

(although it might happen that $a = b$). Then n has at least the three distinct divisors 1, a, and n, and their sum is clearly not equal to $n+1$. This completes the proof by contraposition. One should also observe that the converse of this statement is also true: if n is prime, then the sum of its divisors is $n+1$ (since its only divisors are 1 and itself).

20. This question is asking for the smallest pair of primes that differ by 6. Looking at a table of prime numbers tells us that these are 23 and 29, so the five smallest consecutive composite integers are 24, 25, 26, 27, and 28.

22. Using a computer algebra system, such as *Maple* with its ability to loop and its built-in primeness tester, is the only reasonable way to solve this problem. The answer is 7, 37, 67, 97, 127, 157 (i.e., the common difference is 30). The analogous question for seven primes has common difference 150. A search for a string of eight primes in arithmetic progression found one with starting value 17 and common difference 6930.

24. There is one 0 at the end of this number for every factor of 2 in all of the numbers from 1 to 100. We count them as follows. All the even numbers have a factor of 2, and there are $100/2 = 50$ of these. All the multiples of 4 have another factor of 2, and there are $100/4 = 25$ of these. All the multiples of 8 have another factor of 2, and there are $\lfloor 100/8 \rfloor = 12$ of these, and so on. Thus the answer is $50+25+12+6+3+1 = 97$.

26. We need to divide successively by 233, 144, 89, 55, 34, 21, 13, 8, 5, 3, 2, and 1, a total of 12 divisions.

28. **a)** The first statement is clear. For the second, if a and b are both even, then certainly 2 is a factor of their greatest common divisor, and the complementary factor must be the greatest common divisor of the numbers obtained by dividing out this 2. For the third statement, if a is even and b is odd, then the factor of 2 in a will not appear in the greatest common divisor, so we can ignore it. Finally, the last statement follows from Lemma 1 in Section 4.3, taking $q = 1$ (despite the notation, nothing in Lemma 1 required q to be the quotient).

b) All the steps involved in implementing part **(a)** as an algorithm require only comparisons, subtractions, and divisions of even numbers by 2. Since division by 2 is a shift of one bit to the right, only the operations mentioned here are used. (Note that the algorithm needs two more reductions: if a is odd and b is even, then $\gcd(a,b) = \gcd(a, b/2)$, and if $a < b$, then interchange a and b.)

c) We show the operation of the algorithm as a string of equalities; each equation is one step.

$$\begin{aligned}
\gcd(1202,4848) &= \gcd(4848,1202) = 2\gcd(2424,601) = 2\gcd(1212,601) = 2\gcd(606,601)\\
&= 2\gcd(303,601) = 2\gcd(601,303) = 2\gcd(298,303) = 2\gcd(303,298)\\
&= 2\gcd(303,149) = 2\gcd(154,149) = 2\gcd(77,149) = 2\gcd(149,77)\\
&= 2\gcd(72,77) = 2\gcd(77,72) = 2\gcd(77,36) = 2\gcd(77,18)\\
&= 2\gcd(77,9) = 2\gcd(68,9) = 2\gcd(34,9) = 2\gcd(17,9)\\
&= 2\gcd(8,9) = 2\gcd(9,8) = 2\gcd(9,4) = 2\gcd(9,2)\\
&= 2\gcd(9,1) = 2\gcd(8,1) = 2\gcd(4,1) = 2\gcd(2,1)\\
&= 2\gcd(1,1) = 2
\end{aligned}$$

30. Let's try the strategy used in the proof of Theorem 3 in Section 4.3. Suppose that p_1, p_2, ..., p_n are the only primes of the form $3k+1$. Notice that the product of primes of this form is again of this form, because $(3k_1+1)(3k_2+1) = 9k_1k_2 + 3k_1 + 3k_2 + 1 = 3(3k_1k_2 + k_1 + k_2) + 1$. We could try looking at $3p_1p_2\cdots p_n + 1$, which is again of this form. By the fundamental theorem of arithmetic, it has prime factors, and clearly no p_i is a factor. Unfortunately, we cannot be guaranteed that any of its prime factors are of the form $3k+1$, because the product of two primes not of this form, namely of the form $3k+2$, is of the form $3k+1$; indeed, $(3k_1+2)(3k_2+2) = 9k_1k_2 + 6k_1 + 6k_2 + 4 = 3(3k_1k_2 + 2k_1 + 2k_2 + 1) + 1$. Thus the proof breaks down at this point.

32. We give a proof by contradiction. Suppose that $p > \sqrt[3]{n}$, where p is the smallest prime factor of n, but n/p is not prime and not equal to 1. Then $p^3 > n$, so $p^2 > n/p$. By our assumption, $n/p = a \cdot b$, where $a, b > 1$. Because $a \cdot b < p^2$, at least one of a and b is less than p; assume without loss of generality that it is a. Then a is a divisor of n smaller than p, so any prime factor of a is a prime divisor of n smaller than p, in contradiction to our assumptions.

34. We need to arrange that every pair of the four numbers has a factor in common. There are six such pairs, so let us use the first six prime numbers as the common factors. Call the numbers a, b, c, and d. We will give a and b a common factor of 2; a and c a common factor of 3; a and d a common factor of 5; b and c a common factor of 7; b and d a common factor of 11; and c and d a common factor of 13. The simplest way to accomplish this is to let $a = 2\cdot 3\cdot 5 = 30$; $b = 2\cdot 7\cdot 11 = 154$; $c = 3\cdot 7\cdot 13 = 273$; and $d = 5\cdot 11\cdot 13 = 715$. The numbers are mutually relatively prime, since no number is a factor of all of them (indeed, each prime is a factor of only two of them). Many other examples are possible, of course.

36. If $x \equiv 3 \pmod 9$, then $x = 3 + 9t$ for some integer t. In particular this equation tells us that $3 \mid x$. On the other hand the first congruence says that $x = 2 + 6s = 2 + 3\cdot(2s)$ for some integer s, which implies that the remainder when x is divided by 3 is 2. Obviously these two conclusions are inconsistent, so there is no simultaneous solution to the two congruences.

38. **a)** There are two things to prove here. First suppose that $\gcd(m_1, m_2) \mid a_1 - a_2$; say $a_1 - a_2 = k \cdot \gcd(m_1, m_2)$. By Theorem 6 in Section 4.3, there are integers s and t such that $\gcd(m_1, m_2) = sm_1 + tm_2$. Multiplying both sides by k and substituting into our first equation we have $a_1 - a_2 = ksm_1 + ktm_2$, which can be rewritten as $a_1 - ksm_1 = a_2 + ktm_2$. This common value is clearly congruent to a_1 modulo m_1 and congruent to a_2 modulo m_2, so it is a solution to the given system. Conversely, suppose that there is a solution x to the system. Then $x = a_1 + sm_1 = a_2 + tm_2$ for some integers s and t. This says that $a_1 - a_2 = tm_2 - sm_1$. But $\gcd(m_1, m_2)$ divides both m_1 and m_2 and therefore divides the right-hand side of this last equation. Therefore it also divides the left-hand side, $a_1 - a_2$, as desired.

b) We follow the idea sketched in Exercises 29 and 30 of Section 4.4. First we show that if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, then $a \equiv b \pmod{\operatorname{lcm}(m_1, m_2)}$. The first hypothesis says that $m_1 \mid a - b$; the second says that $m_2 \mid a - b$. Therefore $a - b$ is a common multiple of m_1 and m_2. If $a - b$ were not also a multiple of $\operatorname{lcm}(m_1, m_2)$, then $(a-b) \mathbin{\mathbf{mod}} \operatorname{lcm}(m_1, m_2)$ would be a common multiple as well, contradicting the definition of $\operatorname{lcm}(m_1, m_2)$. Therefore $a - b$ is a multiple of $\operatorname{lcm}(m_1, m_2)$, i.e., $a \equiv b \pmod{\operatorname{lcm}(m_1, m_2)}$. Now suppose that there were two solutions to the given system of congruences. By what we have just proved, since these two solutions are congruent modulo m_1 (since they are both congruent to a_1) and congruent modulo m_2 (since they are both congruent to a_2), they must be congruent to each other modulo $\operatorname{lcm}(m_1, m_2)$. That is precisely what we wanted to prove.

40. Note that the prime factorization of 35 is $5\cdot 7$. So it suffices to show that $5 \mid n^{12} - 1$ and $7 \mid n^{12} - 1$ for integers n relatively prime to 5 and 7. For such integers, Fermat's little theorem tells us that $n^4 \equiv 1 \pmod 5$ and $n^6 \equiv 1 \pmod 7$. Then we have $n^{12} - 1 \equiv (n^4)^3 - 1 \equiv 1^3 - 1 = 0 \pmod 5$ and $n^{12} - 1 \equiv (n^6)^2 - 1 \equiv 1^2 - 1 = 0 \pmod 7$.

42. In each case we just compute $(a_1 + a_3 + \cdots + a_{13}) + 3(a_2 + a_4 + \cdots + a_{12}) \mathbin{\mathbf{mod}} 10$ to make sure that it equals 0.

a) $(9+8+0+3+0+7+1)+3(7+0+7+2+6+9)$ **mod** $10=1$; invalid
b) $(9+8+4+4+4+2+1)+3(7+0+5+2+5+1)$ **mod** $10=2$; invalid
c) $(9+8+1+1+8+1+0)+3(7+3+6+4+4+0)$ **mod** $10=0$; valid
d) $(9+8+2+1+0+7+9)+3(7+0+0+1+1+9)$ **mod** $10=0$; valid

44. If two digits in odd locations, or two digits in even locations, are transposed, then the sum is the same, so this error will not be detected.

46. Because 3, 7, and 1 are all relatively prime to 10, changing a single digit to a different value will change the sum modulo 10 and the congruence will no longer hold. Transposition errors involving just d_1, d_4, and d_7 (and similarly for transpositions within $\{d_2, d_5, d_8\}$ or within $\{d_3, d_6, d_9\}$) clearly cannot be detected. If a transposition error occurs between two digits in different groups, it will be detected if the difference between the transposed values is not 5 but will not be detected if it is (i.e., transposing a 1 with a 6, or a 2 with a 7, and so on). To see why this is true in one case (the other cases are similar), suppose that $d_1 = x$ and $d_2 = y$ are interchanged. Then the sum is increased by $3(y-x)+7(x-y)=4(x-y)$. This will be 0 modulo 10 if and only if $4(x-y)$ is not a multiple of 10, which is equivalent to $x-y$ not being a multiple of 5.

48. **a)** The seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned 13 (N); add this to O (14) to get 1 (B), so the next character of the ciphertext is B. We continue in this manner, producing the encrypted message KBK A LAL XBUQ XH RHGKLH.
b) Again the seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned K (10); add this to O (14) to get 24 (Y), so the next character of the ciphertext is Y. We continue in this manner, producing the encrypted message KYU CU NUY RZLP IW ZDFNQU.

CHAPTER 5
Induction and Recursion

SECTION 5.1 Mathematical Induction

Important note about notation for proofs by mathematical induction: *In performing the inductive step, it really does not matter what letter we use. We see in the text the proof of* $P(k) \rightarrow P(k+1)$*; but it would be just as valid to prove* $P(n) \rightarrow P(n+1)$*, since the* k *in the first case and the* n *in the second case are just dummy variables. We will use both notations in this* Guide*; in particular, we will use* k *for the first few exercises but often use* n *afterwards.*

2. We can prove this by mathematical induction. Let $P(n)$ be the statement that the golfer plays hole n. We want to prove that $P(n)$ is true for all positive integers n. For the basis step, we are told that $P(1)$ is true. For the inductive step, we are told that $P(k)$ implies $P(k+1)$ for each $k \geq 1$. Therefore by the principle of mathematical induction, $P(n)$ is true for all positive integers n.

4. a) Plugging in $n = 1$ we have that $P(1)$ is the statement $1^3 = [1 \cdot (1+1)/2]^2$.

b) Both sides of $P(1)$ shown in part **(a)** equal 1.

c) The inductive hypothesis is the statement that

$$1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2 .$$

d) For the inductive step, we want to show for each $k \geq 1$ that $P(k)$ implies $P(k+1)$. In other words, we want to show that assuming the inductive hypothesis (see part **(c)**) we can prove

$$[1^3 + 2^3 + \cdots + k^3] + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2 .$$

e) Replacing the quantity in brackets on the left-hand side of part **(d)** by what it equals by virtue of the inductive hypothesis, we have

$$\left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 = (k+1)^2\left(\frac{k^2}{4} + k + 1\right) = (k+1)^2\left(\frac{k^2+4k+4}{4}\right) = \left(\frac{(k+1)(k+2)}{2}\right)^2 ,$$

as desired.

f) We have completed both the basis step and the inductive step, so by the principle of mathematical induction, the statement is true for every positive integer n.

6. The basis step is clear, since $1 \cdot 1! = 2! - 1$. Assuming the inductive hypothesis, we then have

$$\begin{aligned} 1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! + (k+1) \cdot (k+1)! &= (k+1)! - 1 + (k+1) \cdot (k+1)! \\ &= (k+1)!(1 + k + 1) - 1 = (k+2)! - 1 , \end{aligned}$$

as desired.

8. The proposition to be proved is $P(n)$:

$$2 - 2 \cdot 7 + 2 \cdot 7^2 - \cdots + 2 \cdot (-7)^n = \frac{1 - (-7)^{n+1}}{4}.$$

In order to prove this for all integers $n \geq 0$, we first prove the basis step $P(0)$ and then prove the inductive step, that $P(k)$ implies $P(k+1)$. Now in $P(0)$, the left-hand side has just one term, namely 2, and the right-hand side is $(1-(-7)^1)/4 = 8/4 = 2$. Since $2 = 2$, we have verified that $P(0)$ is true. For the inductive step, we *assume* that $P(k)$ is true (i.e., the displayed equation above), and derive from it the truth of $P(k+1)$, which is the equation

$$2 - 2\cdot 7 + 2\cdot 7^2 - \cdots + 2\cdot(-7)^k + 2\cdot(-7)^{k+1} = \frac{1-(-7)^{(k+1)+1}}{4}.$$

To prove an equation like this, it is usually best to start with the more complicated side and manipulate it until we arrive at the other side. In this case we start on the left. Note that all but the last term constitute precisely the left-hand side of $P(k)$, and therefore by the inductive hypothesis, we can replace it by the right-hand side of $P(k)$. The rest is algebra:

$$\begin{aligned}
[2 - 2\cdot 7 + 2\cdot 7^2 - \cdots + 2\cdot(-7)^k] + 2\cdot(-7)^{k+1} &= \frac{1-(-7)^{k+1}}{4} + 2\cdot(-7)^{k+1} \\
&= \frac{1-(-7)^{k+1} + 8\cdot(-7)^{k+1}}{4} \\
&= \frac{1+7\cdot(-7)^{k+1}}{4} \\
&= \frac{1-(-7)\cdot(-7)^{k+1}}{4} \\
&= \frac{1-(-7)^{(k+1)+1}}{4}.
\end{aligned}$$

10. **a)** By computing the first few sums and getting the answers $1/2$, $2/3$, and $3/4$, we guess that the sum is $n/(n+1)$.

b) We prove this by induction. It is clear for $n = 1$, since there is just one term, $1/2$. Suppose that

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}.$$

We want to show that

$$\left[\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{k(k+1)}\right] + \frac{1}{(k+1)(k+2)} = \frac{k+1}{k+2}.$$

Starting from the left, we replace the quantity in brackets by $k/(k+1)$ (by the inductive hypothesis), and then do the algebra

$$\frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k^2+2k+1}{(k+1)(k+2)} = \frac{k+1}{k+2},$$

yielding the desired expression.

12. We proceed by mathematical induction. The basis step ($n = 0$) is the statement that $(-1/2)^0 = (2+1)/(3\cdot 1)$, which is the true statement that $1 = 1$. Assume the inductive hypothesis, that

$$\sum_{j=0}^{k} \left(-\frac{1}{2}\right)^j = \frac{2^{k+1} + (-1)^k}{3\cdot 2^k}.$$

We want to prove that

$$\sum_{j=0}^{k+1} \left(-\frac{1}{2}\right)^j = \frac{2^{k+2} + (-1)^{k+1}}{3\cdot 2^{k+1}}.$$

Split the summation into two parts, apply the inductive hypothesis, and do the algebra:

$$\begin{aligned}\sum_{j=0}^{k+1}\left(-\frac{1}{2}\right)^j &= \sum_{j=0}^{k}\left(-\frac{1}{2}\right)^j + \left(-\frac{1}{2}\right)^{k+1} \\ &= \frac{2^{k+1}+(-1)^k}{3\cdot 2^k} + \frac{(-1)^{k+1}}{2^{k+1}} \\ &= \frac{2^{k+2}+2(-1)^k}{3\cdot 2^{k+1}} + \frac{3(-1)^{k+1}}{3\cdot 2^{k+1}} \\ &= \frac{2^{k+2}+(-1)^{k+1}}{3\cdot 2^{k+1}}\,.\end{aligned}$$

For the last step, we used the fact that $2(-1)^k = -2(-1)^{k+1}$.

14. We proceed by induction. Notice that the letter k has been used in this problem as the dummy index of summation, so we cannot use it as the variable for the inductive step. We will use n instead. For the basis step we have $1\cdot 2^1 = (1-1)2^{1+1}+2$, which is the true statement $2 = 2$. We assume the inductive hypothesis, that

$$\sum_{k=1}^{n} k\cdot 2^k = (n-1)2^{n+1}+2\,,$$

and try to prove that

$$\sum_{k=1}^{n+1} k\cdot 2^k = n\cdot 2^{n+2}+2\,.$$

Splitting the left-hand side into its first n terms followed by its last term and invoking the inductive hypothesis, we have

$$\sum_{k=1}^{n+1} k\cdot 2^k = \left(\sum_{k=1}^{n} k\cdot 2^k\right) + (n+1)2^{n+1} = (n-1)2^{n+1}+2+(n+1)2^{n+1} = 2n\cdot 2^{n+1}+2 = n\cdot 2^{n+2}+2\,,$$

as desired.

16. The basis step reduces to $6 = 6$. Assuming the inductive hypothesis we have

$$\begin{aligned}&1\cdot 2\cdot 3 + 2\cdot 3\cdot 4 + \cdots + k(k+1)(k+2) + (k+1)(k+2)(k+3) \\ &\quad= \frac{k(k+1)(k+2)(k+3)}{4} + (k+1)(k+2)(k+3) \\ &\quad= (k+1)(k+2)(k+3)\left(\frac{k}{4}+1\right) \\ &\quad= \frac{(k+1)(k+2)(k+3)(k+4)}{4}\,.\end{aligned}$$

18. a) Plugging in $n = 2$, we see that $P(2)$ is the statement $2! < 2^2$.
b) Since $2! = 2$, this is the true statement $2 < 4$.
c) The inductive hypothesis is the statement that $k! < k^k$.
d) For the inductive step, we want to show for each $k \geq 2$ that $P(k)$ implies $P(k+1)$. In other words, we want to show that assuming the inductive hypothesis (see part **(c)**) we can prove that $(k+1)! < (k+1)^{k+1}$.
e) $(k+1)! = (k+1)k! < (k+1)k^k < (k+1)(k+1)^k = (k+1)^{k+1}$
f) We have completed both the basis step and the inductive step, so by the principle of mathematical induction, the statement is true for every positive integer n greater than 1.

20. The basis step is $n = 7$, and indeed $3^7 < 7!$, since $2187 < 5040$. Assume the statement for k. Then $3^{k+1} = 3\cdot 3^k < (k+1)\cdot 3^k < (k+1)\cdot k! = (k+1)!$, the statement for $k+1$.

22. A little computation convinces us that the answer is that $n^2 \le n!$ for $n = 0,\ 1$, and all $n \ge 4$. (Clearly the inequality does not hold for $n = 2$ or $n = 3$.) We will prove by mathematical induction that the inequality holds for all $n \ge 4$. The basis step is clear, since $16 \le 24$. Now suppose that $n^2 \le n!$ for a given $n \ge 4$. We must show that $(n+1)^2 \le (n+1)!$. Expanding the left-hand side, applying the inductive hypothesis, and then invoking some valid bounds shows this:

$$\begin{aligned} n^2 + 2n + 1 &\le n! + 2n + 1 \\ &\le n! + 2n + n = n! + 3n \\ &\le n! + n \cdot n \le n! + n \cdot n! \\ &= (n+1)n! = (n+1)! \end{aligned}$$

24. The basis step is clear, since $1/2 \le 1/2$. We assume the inductive hypothesis (the inequality shown in the exercise) and want to prove the similar inequality for $n+1$. We proceed as follows, using the trick of writing $1/(2(n+1))$ in terms of $1/(2n)$ so that we can invoke the inductive hypothesis:

$$\begin{aligned} \frac{1}{2(n+1)} &= \frac{1}{2n} \cdot \frac{2n}{2(n+1)} \\ &\le \frac{1 \cdot 3 \cdot 5 \cdots (2n-1))}{2 \cdot 4 \cdots 2n} \cdot \frac{2n}{2(n+1)} \\ &\le \frac{1 \cdot 3 \cdot 5 \cdots (2n-1))}{2 \cdot 4 \cdots 2n} \cdot \frac{2n+1}{2(n+1)} \\ &= \frac{1 \cdot 3 \cdot 5 \cdots (2n-1) \cdot (2n+1)}{2 \cdot 4 \cdots 2n \cdot 2(n+1)} \end{aligned}$$

26. One can get to the proof of this by doing some algebraic tinkering. It turns out to be easier to think about the given statement as $na^{n-1}(a-b) \ge a^n - b^n$. The basis step ($n = 1$) is the true statement that $a - b \ge a - b$. Assume the inductive hypothesis, that $ka^{k-1}(a-b) \ge a^k - b^k$; we must show that $(k+1)a^k(a-b) \ge a^{k+1} - b^{k+1}$. We have

$$\begin{aligned} (k+1)a^k(a-b) &= k \cdot a \cdot a^{k-1}(a-b) + a^k(a-b) \\ &\ge a(a^k - b^k) + a^k(a-b) \\ &= a^{k+1} - ab^k + a^{k+1} - ba^k\,. \end{aligned}$$

To complete the proof we want to show that $a^{k+1} - ab^k + a^{k+1} - ba^k \ge a^{k+1} - b^{k+1}$. This inequality is equivalent to $a^{k+1} - ab^k - ba^k + b^{k+1} \ge 0$, which factors into $(a^k - b^k)(a-b) \ge 0$, and this is true, because we are given that $a > b$.

28. The base case is $n = 3$. We check that $4^2 - 7 \cdot 4 + 12 = 0$ is nonnegative. Next suppose that $n^2 - 7n + 12 \ge 0$; we must show that $(n+1)^2 - 7(n+1) + 12 \ge 0$. Expanding the left-hand side, we obtain $n^2 + 2n + 1 - 7n - 7 + 12 = (n^2 - 7n + 12) + (2n - 6)$. The first of the parenthesized expressions is nonnegative by the inductive hypothesis; the second is clearly also nonnegative by the assumption that n is at least 3. Therefore their sum is nonnegative, and the inductive step is complete.

30. The statement is true for $n = 1$, since $H_1 = 1 = 2 \cdot 1 - 1$. Assume the inductive hypothesis, that the statement is true for n. Then on the one hand we have

$$\begin{aligned} H_1 + H_2 + \cdots + H_n + H_{n+1} &= (n+1)H_n - n + H_{n+1} \\ &= (n+1)H_n - n + H_n + \frac{1}{n+1} \\ &= (n+2)H_n - n + \frac{1}{n+1}\,, \end{aligned}$$

and on the other hand

$$\begin{aligned}(n+2)H_{n+1}-(n+1) &= (n+2)\left(H_n+\frac{1}{n+1}\right)-(n+1)\\ &= (n+2)H_n+\frac{n+2}{n+1}-(n+1)\\ &= (n+2)H_n+1+\frac{1}{n+1}-n-1\\ &= (n+2)H_n-n+\frac{1}{n+1}\,.\end{aligned}$$

That these two expressions are equal was precisely what we had to prove.

32. The statement is true for the base case, $n=0$, since $3\mid 0$. Suppose that $3\mid(k^3+2k)$. We must show that $3\mid\big((k+1)^3+2(k+1)\big)$. If we expand the expression in question, we obtain $k^3+3k^2+3k+1+2k+2=(k^3+2k)+3(k^2+k+1)$. By the inductive hypothesis, 3 divides k^3+2k, and certainly 3 divides $3(k^2+k+1)$, so 3 divides their sum, and we are done.

34. The statement is true for the base case, $n=0$, since $6\mid 0$. Suppose that $6\mid(n^3-n)$. We must show that $6\mid\big((n+1)^3-(n+1)\big)$. If we expand the expression in question, we obtain $n^3+3n^2+3n+1-n-1=(n^3-n)+3n(n+1)$. By the inductive hypothesis, 6 divides the first term, n^3-n. Furthermore clearly 3 divides the second term, and the second term is also even, since one of n and $n+1$ is even; therefore 6 divides the second term as well. This tells us that 6 divides the given expression, as desired. (Note that here we have, as promised, used n as the dummy variable in the inductive step, rather than k.)

36. It is not easy to stumble upon the trick needed in the inductive step in this exercise, so do not feel bad if you did not find it. The form is straightforward. For the basis step ($n=1$), we simply observe that $4^{1+1}+5^{2\cdot 1-1}=16+5=21$, which is divisible by 21. Then we assume the inductive hypothesis, that $4^{n+1}+5^{2n-1}$ is divisible by 21, and let us look at the expression when $n+1$ is plugged in for n. We want somehow to manipulate it so that the expression for n appears. We have

$$\begin{aligned}4^{(n+1)+1}+5^{2(n+1)-1} &= 4\cdot 4^{n+1}+25\cdot 5^{2n-1}\\ &= 4\cdot 4^{n+1}+(4+21)\cdot 5^{2n-1}\\ &= 4(4^{n+1}+5^{2n-1})+21\cdot 5^{2n-1}\,.\end{aligned}$$

Looking at the last line, we see that the expression in parentheses is divisible by 21 by the inductive hypothesis, and obviously the second term is divisible by 21, so the entire quantity is divisible by 21, as desired.

38. The basis step is trivial, as usual: $A_1\subseteq B_1$ implies that $\bigcup_{j=1}^{1}A_j\subseteq\bigcup_{j=1}^{1}B_j$ because the union of one set is itself. Assume the inductive hypothesis that if $A_j\subseteq B_j$ for $j=1,2,\ldots,k$, then $\bigcup_{j=1}^{k}A_j\subseteq\bigcup_{j=1}^{k}B_j$. We want to show that if $A_j\subseteq B_j$ for $j=1,2,\ldots,k+1$, then $\bigcup_{j=1}^{k+1}A_j\subseteq\bigcup_{j=1}^{k+1}B_j$. To show that one set is a subset of another we show that an arbitrary element of the first set must be an element of the second set. So let $x\in\bigcup_{j=1}^{k+1}A_j=\left(\bigcup_{j=1}^{k}A_j\right)\cup A_{k+1}$. Either $x\in\bigcup_{j=1}^{k}A_j$ or $x\in A_{k+1}$. In the first case we know by the inductive hypothesis that $x\in\bigcup_{j=1}^{k}B_j$; in the second case, we know from the given fact that $A_{k+1}\subseteq B_{k+1}$ that $x\in B_{k+1}$. Therefore in either case $x\in\left(\bigcup_{j=1}^{k}B_j\right)\cup B_{k+1}=\bigcup_{j=1}^{k+1}B_j$.

This is really easier to do directly than by using the principle of mathematical induction. For a noninductive proof, suppose that $x\in\bigcup_{j=1}^{n}A_j$. Then $x\in A_j$ for some j between 1 and n, inclusive. Since $A_j\subseteq B_j$, we know that $x\in B_j$. Therefore by definition, $x\in\bigcup_{j=1}^{n}B_j$.

40. If $n=1$ there is nothing to prove, and the $n=2$ case is the distributive law (see Table 1 in Section 2.2). Those take care of the basis step. For the inductive step, assume that

$$(A_1\cap A_2\cap\cdots\cap A_n)\cup B=(A_1\cup B)\cap(A_2\cup B)\cap\cdots\cap(A_n\cup B)\,;$$

we must show that

$$(A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}) \cup B = (A_1 \cup B) \cap (A_2 \cup B) \cap \cdots \cap (A_n \cup B) \cap (A_{n+1} \cup B)\,.$$

We have

$$\begin{aligned}(A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}) \cup B &= ((A_1 \cap A_2 \cap \cdots \cap A_n) \cap A_{n+1}) \cup B \\ &= ((A_1 \cap A_2 \cap \cdots \cap A_n) \cup B) \cap (A_{n+1} \cup B) \\ &= (A_1 \cup B) \cap (A_2 \cup B) \cap \cdots \cap (A_n \cup B) \cap (A_{n+1} \cup B)\,.\end{aligned}$$

The second line follows from the distributive law, and the third line follows from the inductive hypothesis.

42. If $n = 1$ there is nothing to prove, and the $n = 2$ case says that $(A_1 \cap \overline{B}) \cap (A_2 \cap \overline{B}) = (A_1 \cap A_2) \cap \overline{B}$, which is certainly true, since an element is in each side if and only if it is in all three of the sets A_1, A_2, and $\overline{B}$. Those take care of the basis step. For the inductive step, assume that

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) = (A_1 \cap A_2 \cap \cdots \cap A_n) - B\,;$$

we must show that

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) \cap (A_{n+1} - B) = (A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}) - B\,.$$

We have

$$\begin{aligned}&(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) \cap (A_{n+1} - B) \\ &\qquad = ((A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B)) \cap (A_{n+1} - B) \\ &\qquad = ((A_1 \cap A_2 \cap \cdots \cap A_n) - B) \cap (A_{n+1}) - B) \\ &\qquad = (A_1 \cap A_2 \cap \cdots \cap A_n \cap A_{n+1}) - B\,.\end{aligned}$$

The third line follows from the inductive hypothesis, and the fourth line follows from the $n = 2$ case.

44. If $n = 1$ there is nothing to prove, and the $n = 2$ case says that $(A_1 \cap \overline{B}) \cup (A_2 \cap \overline{B}) = (A_1 \cup A_2) \cap \overline{B}$, which is the distributive law (see Table 1 in Section 2.2). Those take care of the basis step. For the inductive step, assume that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) = (A_1 \cup A_2 \cup \cdots \cup A_n) - B\,;$$

we must show that

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) \cup (A_{n+1} - B) = (A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}) - B\,.$$

We have

$$\begin{aligned}&(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) \cup (A_{n+1} - B) \\ &\qquad = ((A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B)) \cup (A_{n+1} - B) \\ &\qquad = ((A_1 \cup A_2 \cup \cdots \cup A_n) - B) \cup (A_{n+1}) - B) \\ &\qquad = (A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}) - B\,.\end{aligned}$$

The third line follows from the inductive hypothesis, and the fourth line follows from the $n = 2$ case.

46. This proof will be similar to the proof in Example 10. The basis step is clear, since for $n = 3$, the set has exactly one subset containing exactly three elements, and $3(3-1)(3-2)/6 = 1$. Assume the inductive hypothesis, that a set with n elements has $n(n-1)(n-2)/6$ subsets with exactly three elements; we want to prove that a set S with $n+1$ elements has $(n+1)n(n-1)/6$ subsets with exactly three elements. Fix an element a in S, and let T be the set of elements of S other than a. There are two varieties of subsets of S containing exactly three elements. First there are those that do not contain a. These are precisely the three-element subsets of T, and by the inductive hypothesis, there are $n(n-1)(n-2)/6$ of them. Second, there are those that contain a together with two elements of T. Therefore there are just as many of these subsets as there are two-element subsets of T. By Exercise 45, there are exactly $n(n-1)/2$ such subsets of T; therefore there are also $n(n-1)/2$ three-element subsets of S containing a. Thus the total number of subsets of S containing exactly three elements is $(n(n-1)(n-2)/6) + n(n-1)/2$, which simplifies algebraically to $(n+1)n(n-1)/6$, as desired.

48. We will show that any minimum placement of towers can be transformed into the placement produced by the algorithm. Although it does not strictly have the form of a proof by mathematical induction, the spirit is the same. Let $s_1 < s_2 < \cdots < s_k$ be an optimal locations of the towers (i.e., so as to minimize k), and let $t_1 < t_2 < \cdots < t_l$ be the locations produced by the algorithm from Exercise 47. In order to serve the first building, we must have $s_1 \le x_1 + 1 = t_1$. If $s_1 \ne t_1$, then we can move the first tower in the optimal solution to position t_1 without losing cell service for any building. Therefore we can assume that $s_1 = t_1$. Let x_j be smallest location of a building out of range of the tower at s_1; thus $x_j > s_1 + 1$. In order to serve that building there must be a tower s_i such that $s_i \le x_j + 1 = t_2$. If $i > 2$, then towers at positions s_2 through s_{i-1} are not needed, a contradiction. As before, it then follows that we can move the second tower from s_2 to t_2. We continue in this manner for all the towers in the given minimum solution; thus $k = l$. This proves that the algorithm produces a minimum solution.

50. When $n = 1$ the left-hand side is 1, and the right-hand side is $(1 + \frac{1}{2})^2/2 = 9/8$. Thus the basis step was wrong.

52. We prove by mathematical induction that a function $f : A \to \{1, 2, \ldots, n\}$ where $|A| > n$ cannot be one-to-one. For the basis step, $n = 1$ and $|A| > 1$. Let x and y be distinct elements of A. Because the codomain has only one element, we must have $f(x) = f(y)$, so by definition f is not one-to-one. Assume the inductive hypothesis that no function from any A to $\{1, 2, \ldots, n\}$ with $|A| > n$ is one-to-one, and let f be a function from A to $\{1, 2, \ldots, n, n+1\}$, where $|A| > n + 1$. There are three cases. If $n + 1$ is not in the range of f, then the inductive hypothesis tells us that f is not one-to-one. If $f(x) = n + 1$ for more than one value of $x \in A$, then by definition f is not one-to-one. The only other case has $f(a) = n + 1$ for exactly one element $a \in A$. Let $A' = A - \{a\}$, and consider the function f' defined as f restricted to A'. Since $|A'| > n$, by the inductive hypothesis f' is not one-to-one, and therefore neither is f.

54. The base case is $n = 1$. If we are given a set of two elements from $\{1, 2\}$, then indeed one of them divides the other. Assume the inductive hypothesis, and consider a set A of $n + 2$ elements from $\{1, 2, \ldots, 2n, 2n + 1, 2n+2\}$. We must show that at least one of these elements divides another. If as many as $n+1$ of the elements of A are less than $2n + 1$, then the desired conclusion follows immediately from the inductive hypothesis. Therefore we can assume that both $2n + 1$ and $2n + 2$ are in A, together with n smaller elements. If $n + 1$ is one of these smaller elements, then we are done, since $n + 1 \mid 2n + 2$. So we can assume that $n + 1 \notin A$. Now apply the inductive hypothesis to $B = A - \{2n + 1, 2n + 2\} \cup \{n + 1\}$. Since B is a collection of $n + 1$ numbers from $\{1, 2, \ldots, 2n\}$, the inductive hypothesis guarantees that one element of B divides another. If $n + 1$ is not one of these two numbers, then we are done. So we can assume that $n + 1$ is one of these two numbers. Certainly $n + 1$ can't be the divisor, since its smallest multiple is too big to be in B, so there is some $k \in B$ that divides $n+1$. But now k and $2n+2$ are numbers in A, with k dividing $n+2$, and we are done. An alternative proof of this theorem is given in Example 11 of Section 6.2.

56. There is nothing to prove in the base case, $n = 1$, since $\mathbf{A} = \mathbf{A}$. For the inductive step we just invoke the inductive hypothesis and the definition of matrix multiplication:

$$\begin{aligned}\mathbf{A}^{n+1} = \mathbf{A}\mathbf{A}^n &= \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix} \\ &= \begin{bmatrix} a \cdot a^n + 0 \cdot 0 & a \cdot 0 + 0 \cdot b^n \\ 0 \cdot a^n + b \cdot 0 & 0 \cdot 0 + b \cdot b^n \end{bmatrix} = \begin{bmatrix} a^{n+1} & 0 \\ 0 & b^{n+1} \end{bmatrix}\end{aligned}$$

58. The basis step is trivial, since we are already given that $\mathbf{AB} = \mathbf{BA}$. Next we assume the inductive hypothesis, that $\mathbf{AB}^n = \mathbf{B}^n\mathbf{A}$, and try to prove that $\mathbf{AB}^{n+1} = \mathbf{B}^{n+1}\mathbf{A}$. We calculate as follows: $\mathbf{AB}^{n+1} = \mathbf{AB}^n\mathbf{B} = \mathbf{B}^n\mathbf{AB} = \mathbf{B}^n\mathbf{BA} = \mathbf{B}^{n+1}\mathbf{A}$. Note that we used the definition of matrix powers (that $\mathbf{B}^{n+1} = \mathbf{B}^n\mathbf{B}$), the inductive hypothesis, and the basis step.

60. This is identical to Exercise 43, with $\vee$ replacing $\cup$, $\wedge$ replacing $\cap$, and $\neg$ replacing complementation. The basis step is trivial, since it merely says that $\neg p_1$ is equivalent to itself. Assuming the inductive hypothesis, we look at $\neg(p_1 \vee p_2 \vee \cdots \vee p_n \vee p_{n+1})$. By De Morgan's law (grouping all but the last term together) this is the same $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \wedge \neg p_{n+1}$. But by the inductive hypothesis, this equals, $\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n \wedge \neg p_{n+1}$, as desired.

62. The statement is true for $n = 1$, since 1 line separates the plane into 2 regions, and $(1^2 + 1 + 2)/2 = 2$. Assume the inductive hypothesis, that n lines of the given type separate the plane into $(n^2+n+2)/2$ regions. Consider an arrangement of $n+1$ lines. Remove the last line. Then there are $(n^2 + n + 2)/2$ regions by the inductive hypothesis. Now we put the last line back in, drawing it slowly, and see what happens to the regions. As we come in "from infinity," the line separates one infinite region into two (one on each side of it); this separation is complete as soon as the line hits one of the first n lines. Then, as we continue drawing from this first point of intersection to the second, the line again separates one region into two. We continue in this way. Every time we come to another point of intersection between the line we are drawing and the figure already present, we lop off another additional region. Furthermore, once we leave the last point of intersection and draw our line off to infinity again, we separate another region into two. Therefore the number of additional regions we formed is equal to the number of points of intersection plus one. Now there are n points of intersection, since our line must intersect each of the other lines in a distinct point (this is where the geometric assumptions get used). Therefore this arrangement has $n+1$ more points of intersection than the arrangement of n lines, namely $\big((n^2 + n + 2)/2\big) + (n + 1)$, which, after a bit of algebra, reduces to $\big((n + 1)^2 + (n + 1) + 2\big)/2$, exactly as desired.

64. For the base case $n = 1$ there is nothing to prove. Assume the inductive hypothesis, and suppose that we are given $p \mid a_1 a_2 \cdots a_n a_{n+1}$. We must show that $p \mid a_i$ for some i. Let us look at $\gcd(p, a_1 a_2 \cdots a_n)$. Since the only divisors of p are 1 and p, this is either 1 or p. If it is 1, then by Lemma 2 in Section 4.3, we have $p \mid a_{n+1}$ (here $a = p$, $b = a_1 a_2 \cdots a_n$, and $c = a_{n+1}$), as desired. On the other hand, if the greatest common divisor is p, this means that $p \mid a_1 a_2 \cdots a_n$. Now by the inductive hypothesis, $p \mid a_i$ for some $i \le n$, again as desired.

66. Suppose that a statement $\forall n P(n)$ has been proved by this method. Let S be the set of counterexamples to P, i.e., let $S = \{\, n \mid \neg P(n) \,\}$. We will show that $S = \emptyset$. If $S \ne \emptyset$, then let n be the minimum element of S (which exists by the well-ordering property). Clearly $n \ne 1$ and $n \ne 2$, by the basis steps of our proof method. But since n is the least element of S and $n \ge 3$, we know that $P(n-1)$ and $P(n-2)$ are true. Therefore by the inductive step of our proof method, we know that $P(n)$ is also true. This contradicts the choice of n. Therefore $S = \emptyset$, as desired.

68. The basis step is $n = 1$ and $n = 2$. If there is one guest present, then he or she is vacuously a celebrity, and no questions are needed; this is consistent with the value of $3(n-1)$. If there are two guests, then it is certainly true that we can determine who the celebrity is (or determine that neither of them is) with three questions. In fact, two questions suffice (ask each one if he or she knows the other). Assume the inductive hypothesis that if there are k guests present ($k \ge 2$), then we can determine whether there is a celebrity with at most $3(k-1)$ questions. We want to prove the statement for $k+1$, namely, if there are $k+1$ at the party, then we can find the celebrity (or determine that there is none) using $3k$ questions. Let Alex and Britney be two of the guests. Ask Alex whether he knows Britney. If he says yes, then we know that he is not a celebrity. If he says no, then we know that Britney is not a celebrity. Without loss of generality, assume that we have eliminated Alex as a possible celebrity. Now invoke the inductive hypothesis on the k guests excluding Alex, asking $3(k-1)$ questions. If there is no celebrity, then we know that there is no celebrity at our party. If there is, suppose that it is person x (who might be Britney or might be someone else). We then ask two more questions to determine whether x is in fact a celebrity; namely ask Alex whether he knows x, and ask x whether s/he knows Alex. Based on the answers, we will now know whether x is a celebrity for the whole party or there is no celebrity present. We have asked a total of at most $1+3(k-1)+2=3k$ questions. Note that in fact we did a little better than $3(n-1)$; because only two questions were needed for $n=2$, only $3(n-1)-1=3n-4$ questions are needed in the general case for $n \geq 2$.

70. We prove this by mathematical induction. The basis step, $G(4)=2\cdot 4-4=4$ was proved in Exercise 69. For the inductive step, suppose that when there are k callers, $2k-4$ calls suffice; we must show that when there are $k+1$ callers, $2(k+1)-4$ calls suffice, that is, two more calls. It is clear from the hint how to proceed. For the first extra call, have the $(k+1)^{\text{st}}$ person exchange information with the k^{th} person. Then use $2k-4$ calls for the first k people to exchange information. At that point, each of them knows all the gossip. Finally, have the $(k+1)^{\text{st}}$ person again call the k^{th} person, at which point he will learn the rest of the gossip.

72. We follow the hint. If the statement is true for some value of n, then it is also true for all smaller values of n, because we can use the same arrangement among those smaller numbers. Thus is suffices to prove the statement when n is a power of 2. We use mathematical induction to prove the result for 2^k. If $k=0$ or $k=1$, there is nothing to prove. Notice that the arrangement 1324 works for $k=2$. Assume that we can arrange the positive integers from 1 to 2^k so that the average of any two of these numbers never appears between them. Arrange the numbers from 1 to 2^{k+1} by taking the given arrangement of 2^k numbers, replacing each number by its double, and then following this sequence with the sequence of 2^k numbers obtained from these 2^k even numbers by subtracting 1. Thus for $k=3$ we use the sequence 1324 to form the sequence 26481537. This clearly is a list of the numbers from 1 to 2^{k+1}. The average of an odd number and an even number is not an integer, so it suffices to shows that the average of two even numbers and the average of two odd numbers in our list never appears between the numbers being averaged. If the average of two even numbers, say $2a$ and $2b$, whose average is $a+b$, appears between the numbers being averaged, then by the way we constructed the sequence, there would have been a similar violation in the 2^k list, namely, $(a+b)/2$ would have appeared between a and b. Similarly, if the average of two odd numbers, say $2c-1$ and $2d-1$, whose average is $c+d-1$, appears between the numbers being averaged, then there would have been a similar violation in the 2^k list, namely, $(c+d)/2$ would have appeared between c and d.

74. **a)** The basis step works, because for $n=1$ the statement $1/2 < 1/\sqrt{3}$ is true. The inductive step would require proving that

$$\frac{1}{\sqrt{3n}}\cdot\frac{2n+1}{2n+2} < \frac{1}{\sqrt{3(n+1)}}\,.$$

Squaring both sides and clearing fractions, we see that this is equivalent to $4n^2+4n+1 < 4n^2+4n$, which of course is not true.

b) The basis step works, because the statement $3/8 < 1/\sqrt{7}$ is true. The inductive step this time requires proving that

$$\frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2} < \frac{1}{\sqrt{3(n+1)+1}}\,.$$

A little algebraic manipulation shows that this is equivalent to

$$12n^3+28n^2+19n+4 < 12n^3+28n^2+20n+4\,,$$

which is true.

76. The upper left 4×4 quarter of the figure given in the solution to Exercise 77 gives such a tiling.

78. **a)** Every $3 \times 2k$ board can be covered in an obvious way: put two pieces together to form a 3×2 rectangle, then lay the rectangles edge to edge. In particular, for all $n \geq 1$ the 3×2^n rectangle can be covered.

b) This is similar to part **(a)**. For all $k \geq 1$ it is easy to cover the $6 \times 2k$ board, using two coverings of the $3 \times 2k$ board from part **(a)**, laid side by side.

c) A little trial and error shows that the $3^1 \times 3^1$ board cannot be covered. Therefore not all such boards can be covered.

d) All boards of this shape can be covered for $n \geq 1$, using reasoning similar to parts **(a)** and **(b)**.

80. This is too complicated to discuss here. For a solution, see the article by I. P. Chu and R. Johnsonbaugh, "Tiling Deficient Boards with Trominoes," *Mathematics Magazine* **59** (1986) 34–40. (Notice the variation in the spelling of this made-up word.)

82. In order to explain this argument, we label the squares in the 5×5 checkerboard 11, 12, ..., 15, 21, ..., 25, ..., 51, ..., 55, where the first digit stands for the row number and the second digit stands for the column number. Also, in order to talk about the right triomino (L-shaped tile), think of it positioned to look like the letter L; then we call the square on top the head, the square in the lower right the tail, and the square in the corner the corner. We claim that the board with square 12 removed cannot be tiled. First note that in order to cover square 11, the position of one piece is fixed. Next we consider how to cover square 13. There are three possibilities. If we put a head there, then we are forced to put the corner of another piece in square 15. If we put a corner there, then we are forced to put the tail of another piece in 15, and if we put a tail there, then square 15 cannot be covered at all. So we conclude that squares 13, 14, 15, 23, 24, and 25 will have to be covered by two more pieces. By symmetry, the same argument shows that two more pieces must cover squares 31, 41, 51, 32, 42, and 52. This much has been forced, and now we are left with the 3×3 square in the lower left part of the checkerboard to cover with three more pieces. If we put a corner in 33, then we immediately run into an impasse in trying to cover 53 and 35. If we put a head in 33, then 53 cannot be covered; and if we put a tail in 33, then 35 cannot be covered. So we have reached a contradiction, and the desired covering does not exist.

SECTION 5.2 Strong Induction and Well-Ordering

Important note about notation for proofs by mathematical induction: *In performing the inductive step, it really does not matter what letter we use. We see in the text the proof of* $(\forall j{\le}k\, P(j)) \rightarrow P(k+1)$*; but it would be just as valid to prove* $(\forall j{\le}n\, P(j)) \rightarrow P(n+1)$*, since the* k *in the first case and the* n *in the second case are just dummy variables. Furthermore, we could also take the inductive hypothesis to be* $\forall j{<}n\, P(j)$ *and then prove* $P(n)$*. We will use all three notations in this* Guide.

2. Let $P(n)$ be the statement that the n^{th} domino falls. We want to prove that $P(n)$ is true for all positive integers n. For the basis step we note that the given conditions tell us that $P(1)$, $P(2)$, and $P(3)$ are true. For the inductive step, fix $k \geq 3$ and assume that $P(j)$ is true for all $j \leq k$. We want to show that $P(k+1)$ is true. Since $k \geq 3$, $k-2$ is a positive integer less than or equal to k, so by the inductive hypothesis we know that $P(k-2)$ is true. That is, we know that the $(k-2)^{\text{nd}}$ domino falls. We were told that "when a domino falls, the domino three farther down in the arrangement also falls," so we know that the domino in position $(k-2)+3 = k+1$ falls. This is $P(k+1)$.

Note that we didn't use strong induction exactly as stated in the text. Instead, we considered all the cases $n = 1$, $n = 2$, and $n = 3$ as part of the basis step. We could have more formally included $n = 2$ and $n = 3$ in the inductive step as a special case. Writing our proof this way, the basis step is just to note that the first domino falls, so $P(1)$ is true. For the inductive step, if $k = 1$ or $k = 2$, then we are already told that the second and third domino fall, so $P(k+1)$ is true in those cases. If $k > 2$, then the inductive hypothesis tells us that the $(k-2)^{\text{nd}}$ domino falls, so the domino in position $(k-1)+2 = k+1$ falls.

4. **a)** $P(18)$ is true, because we can form 18 cents of postage with one 4-cent stamp and two 7-cent stamps. $P(19)$ is true, because we can form 19 cents of postage with three 4-cent stamps and one 7-cent stamp. $P(20)$ is true, because we can form 20 cents of postage with five 4-cent stamps. $P(21)$ is true, because we can form 20 cents of postage with three 7-cent stamps.

b) The inductive hypothesis is the statement that using just 4-cent and 7-cent stamps we can form j cents postage for all j with $18 \le j \le k$, where we assume that $k \ge 21$.

c) In the inductive step we must show, assuming the inductive hypothesis, that we can form $k+1$ cents postage using just 4-cent and 7-cent stamps.

d) We want to form $k+1$ cents of postage. Since $k \ge 21$, we know that $P(k-3)$ is true, that is, that we can form $k-3$ cents of postage. Put one more 4-cent stamp on the envelope, and we have formed $k+1$ cents of postage, as desired.

e) We have completed both the basis step and the inductive step, so by the principle of strong induction, the statement is true for every integer n greater than or equal to 18.

6. **a)** We can form the following amounts of postage as indicated: $3 = 3$, $6 = 3+3$, $9 = 3+3+3$, $10 = 10$, $12 = 3+3+3+3$, $13 = 10+3$, $15 = 3+3+3+3+3$, $16 = 10+3+3$, $18 = 3+3+3+3+3+3$, $19 = 10+3+3+3$, $20 = 10+10$. By having considered all the combinations, we know that the gaps in this list cannot be filled. We claim that we can form all amounts of postage greater than or equal to 18 cents using just 3-cent and 10-cent stamps.

b) Let $P(n)$ be the statement that we can form n cents of postage using just 3-cent and 10-cent stamps. We want to prove that $P(n)$ is true for all $n \ge 18$. The basis step, $n = 18$, is handled above. Assume that we can form k cents of postage (the inductive hypothesis); we will show how to form $k+1$ cents of postage. If the k cents included two 10-cent stamps, then replace them by seven 3-cent stamps ($7 \cdot 3 = 2 \cdot 10 + 1$). Otherwise, k cents was formed either from just 3-cent stamps, or from one 10-cent stamp and $k-10$ cents in 3-cent stamps. Because $k \ge 18$, there must be at least three 3-cent stamps involved in either case. Replace three 3-cent stamps by one 10-cent stamp, and we have formed $k+1$ cents in postage ($10 = 3 \cdot 3 + 1$).

c) $P(n)$ is the same as in part **(b)**. To prove that $P(n)$ is true for all $n \ge 18$, we note for the basis step that from part **(a)**, $P(n)$ is true for $n = 18, 19, 20$. Assume the inductive hypothesis, that $P(j)$ is true for all j with $18 \le j \le k$, where k is a fixed integer greater than or equal to 20. We want to show that $P(k+1)$ is true. Because $k-2 \ge 18$, we know that $P(k-2)$ is true, that is, that we can form $k-2$ cents of postage. Put one more 3-cent stamp on the envelope, and we have formed $k+1$ cents of postage, as desired. In this proof our inductive hypothesis included all values between 18 and k inclusive, and that enabled us to jump back three steps to a value for which we knew how to form the desired postage.

8. Since both 25 and 40 are multiples of 5, we cannot form any amount that is not a multiple of 5. So let's determine for which values of n we can form $5n$ dollars using these gift certificates, the first of which provides 5 copies of \$5, and the second of which provides 8 copies. We can achieve the following values of n: $5 = 5$, $8 = 8$, $10 = 5+5$, $13 = 8+5$, $15 = 5+5+5$, $16 = 8+8$, $18 = 8+5+5$, $20 = 5+5+5+5$, $21 = 8+8+5$, $23 = 8+5+5+5$, $24 = 8+8+8$, $25 = 5+5+5+5+5$, $26 = 8+8+5+5$, $28 = 8+5+5+5+5$, $29 = 8+8+8+5$, $30 = 5+5+5+5+5+5$, $31 = 8+8+5+5+5$, $32 = 8+8+8+8$. By having considered all the combinations, we know that the gaps in this list cannot be filled. We claim that we can form total amounts of the form $5n$ for all $n \geq 28$ using these gift certificates. (In other words, \$135 is the largest multiple of \$5 that we cannot achieve.)

To prove this by strong induction, let $P(n)$ be the statement that we can form $5n$ dollars in gift certificates using just 25-dollar and 40-dollar certificates. We want to prove that $P(n)$ is true for all $n \geq 28$. From our work above, we know that $P(n)$ is true for $n = 28, 29, 30, 31, 32$. Assume the inductive hypothesis, that $P(j)$ is true for all j with $28 \leq j \leq k$, where k is a fixed integer greater than or equal to 32. We want to show that $P(k+1)$ is true. Because $k-4 \geq 28$, we know that $P(k-4)$ is true, that is, that we can form $5(k-4)$ dollars. Add one more \$25-dollar certificate, and we have formed $5(k+1)$ dollars, as desired.

10. We claim that it takes exactly $n-1$ breaks to separate a bar (or any connected piece of a bar obtained by horizontal or vertical breaks) into n pieces. We use strong induction. If $n = 1$, this is trivially true (one piece, no breaks). Assume the strong inductive hypothesis, that the statement is true for breaking into k or fewer pieces, and consider the task of obtaining $k+1$ pieces. We must show that it takes exactly k breaks. The process must start with a break, leaving two smaller pieces. We can view the rest of the process as breaking one of these pieces into $i+1$ pieces and breaking the other piece into $k-i$ pieces, for some i between 0 and $k-1$, inclusive. By the inductive hypothesis it will take exactly i breaks to handle the first piece and $k-i-1$ breaks to handle the second piece. Therefore the total number of breaks will be $1 + i + (k-i-1) = k$, as desired.

12. The basis step is to note that $1 = 2^0$. Notice for subsequent steps that $2 = 2^1$, $3 = 2^1 + 2^0$, $4 = 2^2$, $5 = 2^2 + 2^0$, and so on. Indeed this is simply the representation of a number in binary form (base two). Assume the inductive hypothesis, that every positive integer up to k can be written as a sum of distinct powers of 2. We must show that $k+1$ can be written as a sum of distinct powers of 2. If $k+1$ is odd, then k is even, so 2^0 was not part of the sum for k. Therefore the sum for $k+1$ is the same as the sum for k with the extra term 2^0 added. If $k+1$ is even, then $(k+1)/2$ is a positive integer, so by the inductive hypothesis $(k+1)/2$ can be written as a sum of distinct powers of 2. Increasing each exponent by 1 doubles the value and gives us the desired sum for $k+1$.

14. We prove this using strong induction. It is clearly true for $n = 1$, because no splits are performed, so the sum computed is 0, which equals $n(n-1)/2$ when $n = 1$. Assume the strong inductive hypothesis, and suppose that our first splitting is into piles of i stones and $n-i$ stones, where i is a positive integer less than n. This gives a product $i(n-i)$. The rest of the products will be obtained from splitting the piles thus formed, and so by the inductive hypothesis, the sum of the products will be $i(i-1)/2 + (n-i)(n-i-1)/2$. So we must show that

$$i(n-i) + \frac{i(i-1)}{2} + \frac{(n-i)(n-i-1)}{2} = \frac{n(n-1)}{2}$$

no matter what i is. This follows by elementary algebra, and our proof is complete.

16. We follow the hint to show that there is a winning strategy for the first player in Chomp played on a $2 \times n$ board that starts by removing the rightmost cookie in the bottom row. Note that this leaves a board with n cookies in the top row and $n-1$ cookies in the bottom row. It suffices to prove by strong induction on n that a player presented with such a board will lose if his opponent plays properly. We do this by showing how the opponent can return the board to this form following any nonfatal move this player might make. The basis step is $n = 1$, and in that case only the poisoned cookie remains, so the player loses. Assume the inductive hypothesis (that the statement is true for all smaller values of n). If the player chooses a nonpoisoned cookie in the top row, then that leaves another board with two rows of equal length, so again the opponent chooses the rightmost cookie in the bottom row, and we are back to the hopeless situation, for some board with fewer than n cookies in the top row. If the player chooses the cookie in the m^{th} column from the left in the bottom row (where necessarily $m < n$), then the opponent chooses the cookie in the $(m+1)^{\text{st}}$ column from the left in the top row, and once again we are back to the hopeless situation, with m cookies in the top row.

18. We prove something slightly stronger: If a convex n-gon whose vertices are labeled consecutively as v_m, v_{m+1}, $\ldots$, v_{m+n-1} is triangulated, then the triangles can be numbered from m to $m+n-3$ so that v_i is a vertex of triangle i for $i = m, m+1, \ldots, m+n-3$. (The statement we are asked to prove is the case $m = 1$.) The basis step is $n = 3$, and there is nothing to prove. For the inductive step, assume the inductive hypothesis that the statement is true for polygons with fewer than n vertices, and consider any triangulation of a convex n-gon whose vertices are labeled consecutively as v_m, v_{m+1}, $\ldots$, v_{m+n-1}. One of the diagonals in the triangulation must have either v_{m+n-1} or v_{m+n-2} as an endpoint (otherwise, the region containing v_{m+n-1} would not be a triangle). So there are two cases. If the triangulation uses diagonal $v_k v_{m+n-1}$, then we apply the inductive hypothesis to the two polygons formed by this diagonal, renumbering v_{m+n-1} as v_{k+1} in the polygon that contains v_m. This gives us the desired numbering of the triangles, with numbers v_m through v_{k-1} in the first polygon and numbers v_k through v_{m+n-3} in the second polygon. If the triangulation uses diagonal $v_k v_{m+n-2}$, then we apply the inductive hypothesis to the two polygons formed by this diagonal, renumbering v_{m+n-2} as v_{k+1} and v_{m+n-1} as v_{k+2} in the polygon that contains v_{m+n-1}, and renumbering all the vertices by adding 1 to their indices in the other polygon. This gives us the desired numbering of the triangles, with numbers v_m through v_k in the first polygon and numbers v_{k+1} through v_{m+n-3} in the second polygon. Note that we did not need the convexity of our polygons.

20. The proof takes several pages and can be found in an article entitled "Polygons Have Ears" by Gary H. Meisters in *The American Mathematical Monthly* **82** (1975) 648–651.

22. The basis step for this induction is no problem, because for $n = 3$, there can be no diagonals and therefore there are two vertices that are not endpoints of the diagonals. (Note, though, that $Q(3)$ is not true.) For $n = 4$, there can be at most one diagonal, and the two vertices that are not its endpoints satisfy the requirements for both $P(4)$ and $Q(4)$. We look at the inductive steps.

a) The proof would presumably try to go something like this. Given a polygon with its set of nonintersecting diagonals, think of one of those diagonals as splitting the polygon into two polygons, each of which then has a set of nonintersecting diagonals. By the inductive hypothesis, each of the two polygons has at least two vertices that are not endpoints of any of these diagonals. We would hope that these two vertices would be the vertices we want. However, one or both of them in each case might actually be endpoints of that separating diagonal, which is a side, not a diagonal, of the smaller polygons. Therefore we have no guarantee that *any* of the points we found do what we want them to do in the original polygon.

b) As in part **(a)**, given a polygon with its set of nonintersecting diagonals, think of one of those diagonals—let's call it uv—as splitting the polygon into two polygons, each of which then has a set of nonintersecting diagonals. By the inductive hypothesis, each of the two polygons has at least two nonadjacent vertices that are not endpoints of any of these diagonals. Furthermore, the two vertices in each case cannot both be u and v, because u and v are adjacent. Therefore there is a vertex w in one of the smaller polygons and a vertex x in the other that differ from u and v and are not endpoints of any of the diagonals. Clearly w and x do what we want them to do in the original polygon—they are not adjacent and they are not the endpoints of any of the diagonals.

24. Call a suitee w and a suitor m "possible" for each other if there exists a stable assignment in which m and w are paired. We will prove that if a suitee w rejects a suitor m, then w is impossible for m. Since the suitors propose in their preference order, the desired conclusion follows. The proof is by induction on the round in which the rejection happens. We will let m be Bob and w be Alice in our discussion. If it is the first round, then say that Bob and Ted both propose to Alice (necessarily the first choice of each of them), and Alice rejects Bob because she prefers Ted. There can be no stable assignment in which Bob is paired with Alice, because then Alice and Ted would form an unstable pair (Alice prefers Ted to Bob, and Ted prefers Alice to everyone else so in particular prefers her to his mate). So assume the inductive hypothesis, that every suitor who has been rejected so far is impossible for every suitee who has rejected him. At this point Bob proposes to Alice and Alice rejects him in favor of, say, Ted. The reason that Ted has proposed to Alice is that she is his favorite among everyone who has not already rejected him; but by the inductive hypothesis, all the suitees who have rejected him are impossible for him. But now there can be no stable assignment in which Bob and Alice are paired, because such an assignment would again leave Alice and Ted unhappy—Alice because she prefers Ted to Bob, and Ted because he prefers Alice to the person he ended up with (remember that by the inductive hypothesis, he cannot have ended up with anyone he prefers to Alice). This completes the inductive step.

For more information, see the seminal article on this topic ("College Admissions and the Stability of Marriage" by David Gale and Lloyd S. Shapley in *The American Mathematical Monthly* **69** (1962) 9–15) or a definitive book (*The Stable Marriage Problem: Structure and Algorithms* by Dan Gusfield and Robert W. Irving (MIT Press, 1989)).

26. **a)** Clearly these conditions tell us that $P(n)$ is true for the even values of n, namely, 0, 2, 4, 6, 8, $\ldots$. Also, it is clear that there is no way to be sure that $P(n)$ is true for other values of n.

b) Clearly these conditions tell us that $P(n)$ is true for the values of n that are multiples of 3, namely, 0, 3, 6, 9, 12, $\ldots$. Also, it is clear that there is no way to be sure that $P(n)$ is true for other values of n.

c) These conditions are sufficient to prove by induction that $P(n)$ is true for all nonnegative integers n.

d) We immediately know that $P(0)$, $P(2)$, and $P(3)$ are true, and clearly there is no way to be sure that $P(1)$ is true. Once we have $P(2)$ and $P(3)$, the inductive step $P(n) \rightarrow P(n+2)$ gives us the truth of $P(n)$ for all $n \geq 2$.

28. We prove by strong induction on n that $P(n)$ is true for all $n \geq b$. The basis step is $n = b$, which is true by the given conditions. For the inductive step, fix an integer $k \geq b$ and assume the inductive hypothesis that if $P(j)$ is true for all j with $b \leq j \leq k$, then $P(k+1)$ is true. There are two cases. If $k+1 \leq b+j$, then $P(k+1)$ is true by the given conditions. On the other hand, if $k+1 > b+j$, then the given conditional statement has its antecedent true by the inductive hypothesis and so again $P(k+1)$ follows.

30. The flaw comes in the inductive step, where we are implicitly assuming that $k \geq 1$ in order to talk about a^{k-1} in the denominator (otherwise the exponent is not a nonnegative integer, so we cannot apply the inductive hypothesis). Our basis step was $n = 0$, so we are not justified in assuming that $k \geq 1$ when we try to prove the statement for $k+1$ in the inductive step. Indeed, it is precisely at $n = 1$ that the proposition breaks down.

32. The proof is invalid for $k = 4$. We cannot increase the postage from 4 cents to 5 cents by either of the replacements indicated, because there is no 3-cent stamp present and there is only one 4-cent stamp present. There is also a minor flaw in the inductive step, because the condition that $j \geq 3$ is not mentioned.

34. We use the technique from part **(b)** of Exercise 33. We are thinking of k as fixed and using induction on n. If $n = 1$, then the sum contains just one term, which is just $k!$, and the right-hand side is also $k!$, so the proposition is true in this case. Next we assume the inductive hypothesis,

$$\sum_{j=1}^{n} j(j+1)(j+2)\cdots(j+k-1) = \frac{n(n+1)(n+2)\cdots(n+k)}{k+1},$$

and prove the statement for $n+1$, namely,

$$\sum_{j=1}^{n+1} j(j+1)(j+2)\cdots(j+k-1) = \frac{(n+1)(n+2)\cdots(n+k)(n+k+1)}{k+1}.$$

We have

$$\begin{aligned}\sum_{j=1}^{n+1} j(j+1)(j+2)\cdots(j+k-1) &= \left(\sum_{j=1}^{n} j(j+1)(j+2)\cdots(j+k-1)\right) + (n+1)(n+2)\cdots(n+k) \\ &= \frac{n(n+1)(n+2)\cdots(n+k)}{k+1} + (n+1)(n+2)\cdots(n+k) \\ &= (n+1)(n+2)\cdots(n+k)\left(\frac{n}{k+1}+1\right) \\ &= (n+1)(n+2)\cdots(n+k)\cdot\frac{n+k+1}{k+1},\end{aligned}$$

as desired.

36. **a)** That S is nonempty is trivial, since letting $s=1$ and $t=1$ gives $a+b$, which is certainly a positive integer in S.

b) The well-ordering property asserts that every nonempty set of positive integers has a least element. Since we just showed that S is a nonempty set of positive integers, it has a least element, which we will call c.

c) If d is a divisor of a and of b, then it is also a divisor of as and bt, and hence of their sum. Since c is such a sum, d is a divisor of c.

d) This is the hard part. By symmetry it is enough to show one of these, say that $c\,|\,a$. Assume (for a proof by contradiction) that $c \nmid a$. Then by the division algorithm (Section 4.1), we can write $a = qc + r$, where $0 < r < c$. Now $c = as + bt$ (for appropriate choices of s and t), since $c \in S$, so we can compute that $r = a - qc = a - q(as+bt) = a(1-qs) + b(-qt)$. This expresses the positive integer r as a linear combination with integer coefficients of a and b and hence tells us that $r \in S$. But since $r < c$, this contradicts the choice of c. Therefore our assumption that $c \nmid a$ is wrong, and $c\,|\,a$, as desired.

e) We claim that the c found in this exercise is the greatest common divisor of a and b. Certainly by part **(d)** it is a common divisor of a and b. On the other hand, part **(c)** tells us that every common divisor of a and b is a divisor of (and therefore no greater than) c. Thus c is a greatest common divisor of a and b. Of course the greatest common divisor is unique, since one cannot have two numbers, each of which is greater than the other.

38. In Exercise 46 of Section 1.8, we found a closed path that snakes its way around an 8×8 checkerboard to cover all the squares, and using that we were able to prove that when one black and one white square are removed, the remaining board can be covered with dominoes. The same reasoning works for any size board, so it suffices to show that any board with an even number of squares has such a snaking path. Note that a board with an even number of squares must have either an even number of rows or an even number of columns, so without loss of generality, assume that it has an even number of rows, say $2n$ rows and m columns. Number the squares in the usual manner, so that the first row contains squares 1 to m from left to right, the second row contains squares $m+1$ to $2m$ from left to right, and so on, with the final row containing squares $(2n-1)m+1$ to $2nm$ from left to right.

We will prove the stronger statement that any such board contains a path that includes the top row traversed from left to right. The basis step is $n=1$, and in that case the path is simply $1,\ 2,\ \ldots,\ m,\ 2m,\ 2m-1,\ \ldots,\ m+1,\ 1$. Assume the inductive hypothesis and consider a board with $2n+2$ rows. By the inductive hypothesis, the board obtained by deleting the top two rows has a closed path that includes its top row from left to right (i.e., $2m+1,\ 2m+2,\ \ldots,\ 3m$). Replace this subsequence by $2m+1,\ m+1,\ 1,\ 2,\ \ldots,\ m,\ 2m,\ 2m-1,\ \ldots,\ m+2,\ 2m+2,\ \ldots,\ 3m$, and we have the desired path.

40. If $x < y$ then $y - x$ is a positive real number, and its reciprocal $1/(y-x)$ is a positive real number, so we can choose a positive integer $A > 1/(y-x)$. (Technically this is the Archimedean property of the real numbers; see Appendix 1.) Now look at $\lfloor x \rfloor + (j/A)$ for positive integers j. Each of these is a rational number. Choose j to be the least positive integer such that this number is greater than x. Such a j exists by the well-ordering property, since clearly if j is large enough, then $\lfloor x \rfloor + (j/A)$ exceeds x. (Note that $j = 0$ results in a value not greater than x.) So we have $r = \lfloor x \rfloor + (j/A) > x$ but $\lfloor x \rfloor + ((j-1)/A) = r - (1/A) \le x$. From this last inequality, substituting $y - x$ for $1/A$ (which only makes the left-hand side smaller) we have $r - (y-x) < x$, whence $r < y$, as desired.

42. The strong induction principle clearly implies ordinary induction, for if one has shown that $P(k) \to P(k+1)$, then it automatically follows that $[P(1) \wedge \cdots \wedge P(k)] \to P(k+1)$; in other words, strong induction can always be invoked whenever ordinary induction is used.

Conversely, suppose that $P(n)$ is a statement that one can prove using strong induction. Let $Q(n)$ be $P(1) \wedge \cdots \wedge P(n)$. Clearly $\forall n P(n)$ is logically equivalent to $\forall n Q(n)$. We show how $\forall n Q(n)$ can be proved using ordinary induction. First, $Q(1)$ is true because $Q(1) = P(1)$ and $P(1)$ is true by the basis step for the proof of $\forall n P(n)$ by strong induction. Now suppose that $Q(k)$ is true, i.e., $P(1) \wedge \cdots \wedge P(k)$ is true. By the proof of $\forall n P(n)$ by strong induction it follow that $P(k+1)$ is true. But $Q(k) \wedge P(k+1)$ is just $Q(k+1)$. Thus we have proved $\forall n Q(n)$ by ordinary induction.

SECTION 5.3 Recursive Definitions and Structural Induction

2. **a)** $f(1) = -2f(0) = -2 \cdot 3 = -6$, $f(2) = -2f(1) = -2 \cdot (-6) = 12$, $f(3) = -2f(2) = -2 \cdot 12 = -24$, $f(4) = -2f(3) = -2 \cdot (-24) = 48$, $f(5) = -2f(4) = -2 \cdot 48 = -96$

b) $f(1) = 3f(0) + 7 = 3 \cdot 3 + 7 = 16$, $f(2) = 3f(1) + 7 = 3 \cdot 16 + 7 = 55$, $f(3) = 3f(2) + 7 = 3 \cdot 55 + 7 = 172$, $f(4) = 3f(3) + 7 = 3 \cdot 172 + 7 = 523$, $f(5) = 3f(4) + 7 = 3 \cdot 523 + 7 = 1576$

c) $f(1) = f(0)^2 - 2f(0) - 2 = 3^2 - 2 \cdot 3 - 2 = 1$, $f(2) = f(1)^2 - 2f(1) - 2 = 1^2 - 2 \cdot 1 - 2 = -3$, $f(3) = f(2)^2 - 2f(2) - 2 = (-3)^2 - 2 \cdot (-3) - 2 = 13$, $f(4) = f(3)^2 - 2f(3) - 2 = 13^2 - 2 \cdot 13 - 2 = 141$, $f(5) = f(4)^2 - 2f(4) - 2 = 141^2 - 2 \cdot 141 - 2 = 19{,}597$

d) First note that $f(1) = 3^{f(0)/3} = 3^{3/3} = 3 = f(0)$. In the same manner, $f(n) = 3$ for all n.

4. **a)** $f(2) = f(1) - f(0) = 1 - 1 = 0$, $f(3) = f(2) - f(1) = 0 - 1 = -1$, $f(4) = f(3) - f(2) = -1 - 0 = -1$, $f(5) = f(4) - f(3) = -1 - 1 = 0$

b) Clearly $f(n) = 1$ for all n, since $1 \cdot 1 = 1$.

c) $f(2) = f(1)^2 + f(0)^3 = 1^2 + 1^3 = 2$, $f(3) = f(2)^2 + f(1)^3 = 2^2 + 1^3 = 5$, $f(4) = f(3)^2 + f(2)^3 = 5^2 + 2^3 = 33$, $f(5) = f(4)^2 + f(3)^3 = 33^2 + 5^3 = 1214$

d) Clearly $f(n) = 1$ for all n, since $1/1 = 1$.

6. **a)** This is valid, since we are provided with the value at $n = 0$, and each subsequent value is determined by the previous one. Since all that changes from one value to the next is the sign, we conjecture that $f(n) = (-1)^n$. This is true for $n = 0$, since $(-1)^0 = 1$. If it is true for $n = k$, then we have $f(k+1) = -f(k+1-1) = -f(k) = -(-1)^k$ by the inductive hypothesis, whence $f(k+1) = (-1)^{k+1}$.

b) This is valid, since we are provided with the values at $n = 0$, 1, and 2, and each subsequent value is determined by the value that occurred three steps previously. We compute the first several terms of the sequence: $1,\ 0,\ 2,\ 2,\ 0,\ 4,\ 4,\ 0,\ 8,\ \ldots$. We conjecture the formula $f(n) = 2^{n/3}$ when $n \equiv 0 \pmod 3$,

$f(n) = 0$ when $n \equiv 1 \pmod 3$, $f(n) = 2^{(n+1)/3}$ when $n \equiv 2 \pmod 3$. To prove this, first note that in the base cases we have $f(0) = 1 = 2^{0/3}$, $f(1) = 0$, and $f(2) = 2 = 2^{(2+1)/3}$. Assume the inductive hypothesis that the formula is valid for smaller inputs. Then for $n \equiv 0 \pmod 3$ we have $f(n) = 2f(n-3) = 2 \cdot 2^{(n-3)/3} = 2 \cdot 2^{n/3} \cdot 2^{-1} = 2^{n/3}$, as desired. For $n \equiv 1 \pmod 3$ we have $f(n) = 2f(n-3) = 2 \cdot 0 = 0$, as desired. And for $n \equiv 2 \pmod 3$ we have $f(n) = 2f(n-3) = 2 \cdot 2^{(n-3+1)/3} = 2 \cdot 2^{(n+1)/3} \cdot 2^{-1} = 2^{(n+1)/3}$, as desired.

c) This is invalid. We are told that $f(2)$ is defined in terms of $f(3)$, but $f(3)$ has not been defined.

d) This is invalid, because the value at $n = 1$ is defined in two conflicting ways—first as $f(1) = 1$ and then as $f(1) = 2f(1-1) = 2f(0) = 2 \cdot 0 = 0$.

e) This appears syntactically to be not valid, since we have conflicting instruction for odd $n \geq 3$. On the one hand $f(3) = f(2)$, but on the other hand $f(3) = 2f(1)$. However, we notice that $f(1) = f(0) = 2$ and $f(2) = 2f(0) = 4$, so these apparently conflicting rules tell us that $f(3) = 4$ on the one hand and $f(3) = 2 \cdot 2 = 4$ on the other hand. Thus we got the same answer either way. Let us show that in fact this definition is valid because the rules coincide.

We compute the first several terms of the sequence: $2, 2, 4, 4, 8, 8, \ldots$. We conjecture the formula $f(n) = 2^{\lceil (n+1)/2 \rceil}$. To prove this inductively, note first that $f(0) = 2 = 2^{\lceil (0+1)/2 \rceil}$. For larger values we have for n odd using the first part of the recursive step that $f(n) = f(n-1) = 2^{\lceil (n-1+1)/2 \rceil} = 2^{\lceil n/2 \rceil} = 2^{\lceil (n+1)/2 \rceil}$, since $n/2$ is not an integer. For $n \geq 2$, whether even or odd, using the second part of the recursive step we have $f(n) = 2f(n-2) = 2 \cdot 2^{\lceil (n-2+1)/2 \rceil} = 2 \cdot 2^{\lceil (n+1)/2 \rceil - 1} = 2 \cdot 2^{\lceil (n+1)/2 \rceil} \cdot 2^{-1} = 2^{\lceil (n+1)/2 \rceil}$, as desired.

8. Many answers are possible.

a) Each term is 4 more than the term before it. We can therefore define the sequence by $a_1 = 2$ and $a_{n+1} = a_n + 4$ for all $n \geq 1$.

b) We note that the terms alternate: $0, 2, 0, 2$, and so on. Thus we could define the sequence by $a_1 = 0$, $a_2 = 2$, and $a_n = a_{n-2}$ for all $n \geq 3$.

c) The sequence starts out $2, 6, 12, 20, 30$, and so on. The differences between successive terms are $4, 6, 8, 10$, and so on. Thus the n^{th} term is $2n$ greater than the term preceding it; in symbols: $a_n = a_{n-1} + 2n$. Together with the initial condition $a_1 = 2$, this defines the sequence recursively.

d) The sequence starts out $1, 4, 9, 16, 25$, and so on. The differences between successive terms are $3, 5, 7, 9$, and so on—the odd numbers. Thus the n^{th} term is $2n - 1$ greater than the term preceding it; in symbols: $a_n = a_{n-1} + 2n - 1$. Together with the initial condition $a_1 = 1$, this defines the sequence recursively.

10. The base case is that $S_m(0) = m$. The recursive part is that $S_m(n+1)$ is the successor of $S_m(n)$ (i.e., the integer that follows $S_m(n)$, namely $S_m(n) + 1$).

12. The basis step ($n = 1$) is clear, since $f_1^2 = f_1 f_2 = 1$. Assume the inductive hypothesis. Then $f_1^2 + f_2^2 + \cdots + f_n^2 + f_{n+1}^2 = f_n f_{n+1} + f_{n+1}^2 = f_{n+1}(f_n + f_{n+1}) = f_{n+1} f_{n+2}$, as desired.

14. The basis step ($n = 1$) is clear, since $f_2 f_0 - f_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1$. Assume the inductive hypothesis. Then we have

$$\begin{aligned} f_{n+2} f_n - f_{n+1}^2 &= (f_{n+1} + f_n) f_n - f_{n+1}^2 \\ &= f_{n+1} f_n + f_n^2 - f_{n+1}^2 \\ &= -f_{n+1}(f_{n+1} - f_n) + f_n^2 \\ &= -f_{n+1} f_{n-1} + f_n^2 \\ &= -(f_{n+1} f_{n-1} - f_n^2) \\ &= -(-1)^n = (-1)^{n+1}. \end{aligned}$$

16. The basis step ($n = 1$) is clear, since $f_0 - f_1 + f_2 = 0 - 1 + 1 = 0$, and $f_1 - 1 = 0$ as well. Assume the inductive hypothesis. Then we have (substituting using the defining relation for the Fibonacci sequence where appropriate)

$$\begin{aligned} f_0 - f_1 + f_2 - \cdots - f_{2n-1} + f_{2n} - f_{2n+1} + f_{2n+2} &= f_{2n-1} - 1 - f_{2n+1} + f_{2n+2} \\ &= f_{2n-1} - 1 + f_{2n} \\ &= f_{2n+1} - 1 \\ &= f_{2(n+1)-1} - 1 . \end{aligned}$$

18. We prove this by induction on n. Clearly $\mathbf{A}^1 = \mathbf{A} = \begin{bmatrix} f_2 & f_1 \\ f_1 & f_0 \end{bmatrix}$. Assume the inductive hypothesis. Then

$$\mathbf{A}^{n+1} = \mathbf{A}\mathbf{A}^n = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} = \begin{bmatrix} f_{n+1} + f_n & f_n + f_{n-1} \\ f_{n+1} & f_n \end{bmatrix} = \begin{bmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{bmatrix},$$

as desired.

20. The max or min of one number is itself; $\max(a_1, a_2) = a_1$ if $a_1 \ge a_2$ and a_2 if $a_1 < a_2$, whereas $\min(a_1, a_2) = a_2$ if $a_1 \ge a_2$ and a_1 if $a_1 < a_2$; and for $n \ge 2$,

$$\max(a_1, a_2, \ldots, a_{n+1}) = \max(\max(a_1, a_2, \ldots, a_n), a_{n+1})$$

and

$$\min(a_1, a_2, \ldots, a_{n+1}) = \min(\min(a_1, a_2, \ldots, a_n), a_{n+1}) .$$

22. Clearly only positive integers can be in S, since 1 is a positive integer, and the sum of two positive integers is again a positive integer. To see that all positive integers are in S, we proceed by induction. Obviously $1 \in S$. Assuming that $n \in S$, we get that $n + 1$ is in S by applying the recursive part of the definition with $s = n$ and $t = 1$. Thus S is precisely the set of positive integers.

24. **a)** Odd integers are obtained from other odd integers by adding 2. Thus we can define this set S as follows: $1 \in S$; and if $n \in S$, then $n + 2 \in S$.

b) Powers of 3 are obtained from other powers of 3 by multiplying by 3. Thus we can define this set S as follows: $3 \in S$ (this is 3^1, the power of 3 using the smallest positive integer exponent); and if $n \in S$, then $3n \in S$.

c) There are several ways to do this. One that is suggested by Horner's method is as follows. We will assume that the variable for these polynomials is the letter x. All integers are in S (this base case gives us all the constant polynomials); if $p(x) \in S$ and n is any integer, then $xp(x) + n$ is in S. Another method constructs the polynomials term by term. Its base case is to let 0 be in S; and its inductive step is to say that if $p(x) \in S$, c is an integer, and n is a nonnegative integer, then $p(x) + cx^n$ is in S.

26. **a)** If we apply each of the recursive step rules to the only element given in the basis step, we see that $(2, 3)$ and $(3, 2)$ are in S. If we apply the recursive step to these we add $(4, 6)$, $(5, 5)$, and $(6, 4)$. The next round gives us $(6, 9)$, $(7, 8)$, $(8, 7)$, and $(9, 6)$. A fourth set of applications adds $(8, 12)$, $(9, 11)$, $(10, 10)$, $(11, 9)$, and $(12, 8)$; and a fifth set of applications adds $(10, 15)$, $(11, 14)$, $(12, 13)$, $(13, 12)$, $(14, 11)$, and $(15, 10)$.

b) Let $P(n)$ be the statement that $5 \mid a + b$ whenever $(a, b) \in S$ is obtained by n applications of the recursive step. For the basis step, $P(0)$ is true, since the only element of S obtained with no applications of the recursive step is $(0, 0)$, and indeed $5 \mid 0 + 0$. Assume the strong inductive hypothesis that $5 \mid a + b$ whenever $(a, b) \in S$ is obtained by k or fewer applications of the recursive step, and consider an element obtained with

$k+1$ applications of the recursive step. Since the final application of the recursive step to an element (a,b) must be applied to an element obtained with fewer applications of the recursive step, we know that $5 \mid a+b$. So we just need to check that this inequality implies $5 \mid a+2+b+3$ and $5 \mid a+3+b+2$. But this is clear, since each is equivalent to $5 \mid a+b+5$, and 5 divides both $a+b$ and 5.

c) This holds for the basis step, since $5 \mid 0+0$. If this holds for (a,b), then it also holds for the elements obtained from (a,b) in the recursive step by the same argument as in part **(b)**.

28. **a)** The simplest elements of S are $(1,2)$ and $(2,1)$. That is the basis step. To get new elements of S from old ones, we need to maintain the parity of the sum, so we either increase the first coordinate by 2, increase the second coordinate by 2, or increase each coordinate by 1. Thus our recursive step is that if $(a,b) \in S$, then $(a+2,b) \in S$, $(a,b+2) \in S$, and $(a+1,b+1) \in S$.

b) The statement here is that b is a multiple of a. One approach is to have an infinite number of base cases to take care of the fact that every element is a multiple of itself. So we have $(n,n) \in S$ for all $n \in \mathbf{Z}^+$. If one objects to having an infinite number of base cases, then we can start with $(1,1) \in S$ and a recursive rule that if $(a,a) \in S$, then $(a+1,a+1) \in S$. Larger multiples of a can be obtained by adding a to a known multiple of a, so our recursive step is that if $(a,b) \in S$, then $(a,a+b) \in S$.

c) The smallest pairs in which the sum of the coordinates is a multiple of 3 are $(1,2)$ and $(2,1)$. So our basis step is $(1,2) \in S$ and $(2,1) \in S$. If we start with a point for which the sum of the coordinates is a multiple of 3 and want to maintain this divisibility condition, then we can add 3 to the first coordinate, or add 3 to the second coordinate, or add 1 to the one of the coordinates and 2 to the other. Thus our recursive step is that if $(a,b) \in S$, then $(a+3,b) \in S$, $(a,b+3) \in S$, $(a+1,b+2) \in S$, and $(a+2,b+1) \in S$.

30. Since we are concerned only with the substrings 01 and 10, all we care about are the changes from 0 to 1 or 1 to 0 as we move from left to right through the string. For example, we view 0011110110100 as a block of 0's followed by a block of 1's followed by a block of 0's followed by a block of 1's followed by a block of 0's followed by a block of 1's followed by a block of 0's. There is one occurrence of 01 or 10 at the start of each block other than the first, and the occurrences alternate between 01 and 10. If the string has an odd number of blocks (or the string is empty), then there will be an equal number of 01's and 10's. If the string has an even number of blocks, then the string will have one more 01 than 10 if the first block is 0's, and one more 10 than 01 if the first block is 1's. (One could also give an inductive proof, based on the length of the string, but a stronger statement is needed: that if the string ends in a 1 then 01 occurs at most one more time than 10, but that if the string ends in a 0, then 01 occurs at most as often as 10.)

32. **a)** $ones(\lambda) = 0$ and $ones(wx) = x + ones(w)$, where w is a bit string and x is a bit (viewed as an integer when being added)

b) The basis step is when $t = \lambda$, in which case we have $ones(s\lambda) = ones(s) = ones(s)+0 = ones(s)+ones(\lambda)$. For the inductive step, write $t = wx$, where w is a bit string and x is a bit. Then we have $ones(s(wx)) = ones((sw)x) = x + ones(sw)$ by the recursive definition, which is $x + ones(s) + ones(w)$ by the inductive hypothesis, which is $ones(s) + (x + ones(w))$ by commutativity and associativity of addition, which finally equals $ones(s) + ones(wx)$ by the recursive definition.

34. **a)** 1010 **b)** 1 1011 **c)** 1110 1001 0001

36. We induct on w_2. The basis step is $(w_1\lambda)^R = w_1^R = \lambda w_1^R = \lambda^R w_1^R$. For the inductive step, assume that $w_2 = w_3x$, where w_3 is a string of length one less than the length of w_2, and x is a symbol (the last symbol of w_2). Then we have $(w_1w_2)^R = (w_1w_3x)^R = x(w_1w_3)^R$ (by the recursive definition given in the solution to Exercise 35). This in turn equals $xw_3^Rw_1^R$ by the inductive hypothesis, which is $(w_3x)^Rw_1^R$ (again by the definition). Finally, this equals $w_2^Rw_1^R$, as desired.

38. There are two types of palindromes, so we need two base cases, namely λ is a palindrome, and x is a palindrome for every symbol x. The recursive step is that if α is a palindrome and x is a symbol, then $x\alpha x$ is a palindrome.

40. The key fact here is that if a bit string of length greater than 1 has more 0's than 1's, then either it is the concatenation of two such strings, or else it is the concatenation of two such strings with one 1 inserted either before the first, between them, or after the last. This can be proved by looking at the running count of the excess of 0's over 1's as we read the string from left to right. Therefore one recursive definition is that 0 is in the set, and if x and y are in the set, then so are xy, $1xy$, $x1y$, and $xy1$.

42. Recall from Exercise 37 the recursive definition of the i^{th} power of a string. We also will use the result of Exercise 36 and the following lemma: $w^{i+1} = w^i w$ for all $i \geq 0$, which is clear (or can be proved by induction on i, using the associativity of concatenation).

Now to prove that $(w^R)^i = (w^i)^R$, we use induction on i. It is clear for $i = 0$, since $(w^R)^0 = \lambda = \lambda^R = (w^i)^R$. Assuming the inductive hypothesis, we have $(w^R)^{i+1} = w^R(w^R)^i = w^R(w^i)^R = (w^i w)^R = (w^{i+1})^R$, as desired.

44. For the basis step we have the tree consisting of just the root, so there is one leaf and there are no internal vertices, and $l(T) = i(T) + 1$ holds. For the recursive step, assume that this relationship holds for T_1 and T_2, and consider the tree with a new root, whose children are the roots of T_1 and T_2. The new root is an internal vertex of T, and every internal vertex in T_1 or T_2 is an internal vertex of T, so $i(T) = i(T_1) + i(T_2) + 1$. Similarly, the leaves of T_1 and T_2 are the leaves of T, so $l(T) = l(T_1) + l(T_2)$. Thus we have $l(T) = l(T_1) + l(T_2) = i(T_1) + 1 + i(T_2) + 1$ by the inductive hypothesis, which equals $(i(T_1) + i(T_2) + 1) + 1 = i(T) + 1$, as desired.

46. The basis step requires that we show that this formula holds when $(m, n) = (1, 1)$. The induction step requires that we show that if the formula holds for all pairs smaller than (m, n) in the lexicographic ordering of $\mathbf{Z}^+ \times \mathbf{Z}^+$, then it also holds for (m, n). For the basis step we have $a_{1,1} = 5 = 2(1+1)+1$. For the inductive step, assume that $a_{m',n'} = 2(m'+n')+1$ whenever (m', n') is less than (m, n) in the lexicographic ordering of $\mathbf{Z}^+ \times \mathbf{Z}^+$. By the recursive definition, if $n = 1$ then $a_{m,n} = a_{m-1,n} + 2$; since $(m-1, n)$ is smaller than (m, n), the induction hypothesis tells us that $a_{m-1,n} = 2(m-1+n)+1$, so $a_{m,n} = 2(m-1+n)+1+2 = 2(m+n)+1$, as desired. Now suppose that $n > 1$, so $a_{m,n} = a_{m,n-1} + 2$. Again we have $a_{m,n-1} = 2(m+n-1)+1$, so $a_{m,n} = 2(m+n-1)+1+2 = 2(m+n)+1$, and the proof is complete.

48. **a)** $A(1, 0) = 0$ by the second line of the definition.
b) $A(0, 1) = 2$ by the first line of the definition.
c) $A(1, 1) = 2$ by the third line of the definition.
d) $A(2, 2) = A(1, A(2, 1)) = A(1, 2) = A(0, A(1, 1)) = A(0, 2) = 4$

50. We prove this by induction on n. It is clear for $n = 1$, since $A(1, 1) = 2 = 2^1$. Assume that $A(1, n) = 2^n$. Then $A(1, n+1) = A(0, A(1, n)) = A(0, 2^n) = 2 \cdot 2^n = 2^{n+1}$, as desired.

52. This is impossible to compute, if by compute we mean write down a nice numeral for the answer. As explained in the solution to Exercise 51, one can show by induction that $A(2, n)$ is equal to $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$, with n 2's in the tower. To compute $A(3, 4)$ we use the definition to write $A(3, 4) = A(2, A(3, 3))$. We saw in the solution to Exercise 51, however, that $A(3, 3) = 65536$, so $A(3, 4) = A(2, 65536)$. Thus $A(3, 4)$ is a tower of 2's with 65536 2's in the tower. There is no nicer way to write or describe this number—it is too big.

54. We use a double induction here, inducting first on m and then on n. The outside base case is $m=0$ (with n arbitrary). Then $A(m,n)=2n$ for all n. Also $A(m+1,n)=2n$ for $n=0$ and $n=1$, and $2n\geq 2n$ in those cases; and $A(m+1,n)=2^n$ for all $n>1$ (by Exercise 50), and in those cases $2^n\geq 2n$ as well. Now we assume the inductive hypothesis, that $A(m+1,t)\geq A(m,t)$ for all t. We will show by induction on n that $A(m+2,n)\geq A(m+1,n)$. For $n=0$ this reduces to $0\geq 0$, and for $n=1$ it reduces to $2\geq 2$. Assume the inner inductive hypothesis, that $A(m+2,n)\geq A(m+1,n)$. Then

$$\begin{aligned}A(m+2,n+1)&=A(m+1,A(m+2,n))\\&\geq A(m+1,A(m+1,n))\quad\text{(using the inductive hypothesis and Exercise 53)}\\&\geq A(m,A(m+1,n))\quad\text{(by the inductive hypothesis on } m)\\&=A(m+1,n+1)\,.\end{aligned}$$

56. Let $P(n)$ be the statement "F is well-defined at n." Then $P(0)$ is true, since $F(0)$ is specified. Assume that $P(n)$ is true. Then F is also well-defined at $n+1$, since $F(n+1)$ is given in terms of $F(n)$. Therefore by mathematical induction, $P(n)$ is true for all n, i.e., F is well-defined as a function on the set of all nonnegative integers.

58. **a)** This would be a proper definition if the recursive part were stated to hold for $n\geq 2$. As it stands, however, $F(1)$ is ambiguous, and $F(0)$ is undefined.

b) This definition makes no sense as it stands; $F(3)$ is not defined, since $F(0)$ isn't. Also, $F(2)$ is ambiguous.

c) For $n=3$, the recursive part makes no sense, since we would have to know $F(3/2)$. Also, $F(2)$ is ambiguous.

d) The definition is ambiguous about $n=1$, since both the second clause and the third clause seem to apply. This would be a valid definition if the third clause applied only to odd $n\geq 3$.

e) We note that $F(1)$ is defined explicitly, $F(2)$ is defined in terms of $F(1)$, $F(4)$ is defined in terms of $F(2)$, and $F(3)$ is defined in terms of $F(8)$, which is defined in terms of $F(4)$. So far, so good. However, let us see what the definition says to do with $F(5)$:

$$F(5)=F(14)=1+F(7)=1+F(20)=1+1+F(10)=1+1+1+F(5)\,.$$

This not only leaves us begging the question as to what $F(5)$ is, but is a contradiction, since $0\neq 3$. (If we replace "$3n-1$" by "$3n+1$" in this problem, then it is an unsolved problem—the Collatz conjecture—as to whether F is well-defined; see Example 23 in Section 1.8.)

60. In each case we will apply the definition. Note that $\log^{(1)} n=\log n$ (for $n>0$). Similarly, $\log^{(2)} n=\log(\log n)$ as long as it is defined (which is when $n>1$), $\log^{(3)} n=\log(\log(\log n))$ as long as it is defined (which is when $n>2$), and so on. Normally the parentheses are understood and omitted.

a) $\log^{(2)} 16=\log\log 16=\log 4=2$, since $2^4=16$ and $2^2=4$

b) $\log^{(3)} 256=\log\log\log 256=\log\log 8=\log 3\approx 1.585$

c) $\log^{(3)} 2^{65536}=\log\log\log 2^{65536}=\log\log 65536=\log 16=4$

d) $\log^{(4)} 2^{2^{65536}}=\log\log\log\log 2^{2^{65536}}=\log\log\log 2^{65536}=4$ by part **(c)**

62. Note that $\log^{(1)} 2=1$, $\log^{(2)} 2^2=1$, $\log^{(3)} 2^{2^2}=1$, $\log^{(4)} 2^{2^{2^2}}=1$, and so on. In general $\log^{(k)} n=1$ when n is a tower of k 2s; once n exceeds a tower of k 2s, $\log^{(k)} n>1$. Therefore the largest n such that $\log^* n=k$ is a tower of k 2s. Here $k=5$, so the answer is $2^{2^{2^{2^2}}}=2^{65536}$. This number overflows most calculators. In order to determine the number of decimal digits it has, we recall that the number of decimal digits of a positive integer x is $\lfloor\log_{10} x\rfloor+1$. Therefore the number of decimal digits of 2^{65536} is $\lfloor\log_{10} 2^{65536}\rfloor+1=\lfloor 65536\log_{10} 2\rfloor+1=19{,}729$.

64. Each application of the function f divides its argument by 2. Therefore iterating this function k times (which is what $f^{(k)}$ does) has the effect of dividing by 2^k. Therefore $f^{(k)}(n) = n/2^k$. Now $f_1^*(n)$ is the smallest k such that $f^{(k)}(n) \le 1$, that is, $n/2^k \le 1$. Solving this for k easily yields $k \ge \log n$, where logarithm is taken to the base 2. Thus $f_1^*(n) = \lceil \log n \rceil$ (we need to take the ceiling function because k must be an integer).

SECTION 5.4 Recursive Algorithms

2. First, we use the recursive step to write $6! = 6 \cdot 5!$. We then use the recursive step repeatedly to write $5! = 5 \cdot 4!$, $4! = 4 \cdot 3!$, $3! = 3 \cdot 2!$, $2! = 2 \cdot 1!$, and $1! = 1 \cdot 0!$. Inserting the value of $0! = 1$, and working back through the steps, we see that $1! = 1 \cdot 1 = 1$, $2! = 2 \cdot 1! = 2 \cdot 1 = 2$, $3! = 3 \cdot 2! = 3 \cdot 2 = 6$, $4! = 4 \cdot 3! = 4 \cdot 6 = 24$, $5! = 5 \cdot 4! = 5 \cdot 24 = 120$, and $6! = 6 \cdot 5! = 6 \cdot 120 = 720$.

4. First, because $n = 10$ is even, we use the **else if** clause to see that

$$mpower(2,10,7) = mpower(2,5,7)^2 \textbf{ mod } 7\,.$$

We next use the **else** clause to see that

$$mpower(2,5,7) = (mpower(2,2,7)^2 \textbf{ mod } 7 \cdot 2 \textbf{ mod } 7) \textbf{ mod } 7\,.$$

Then we use the **else if** clause again to see that

$$mpower(2,2,7) = mpower(2,1,7)^2 \textbf{ mod } 7\,.$$

Using the **else** clause again, we have

$$mpower(2,1,7) = (mpower(2,0,7)^2 \textbf{ mod } 7 \cdot 2 \textbf{ mod } 7) \textbf{ mod } 7\,.$$

Finally, using the **if** clause, we see that $mpower(2,0,7) = 1$. Now we work backward: $mpower(2,1,7) = (1^2 \textbf{ mod } 7 \cdot 2 \textbf{ mod } 7) \textbf{ mod } 7 = 2$, $mpower(2,2,7) = 2^2 \textbf{ mod } 7 = 4$, $mpower(2,5,7) = (4^2 \textbf{ mod } 7 \cdot 2 \textbf{ mod } 7) \textbf{ mod } 7 = 4$, and finally $mpower(2,10,7) = 4^2 \textbf{ mod } 7 = 2$. We conclude that $2^{10} \textbf{ mod } 7 = 2$.

6. With this input, the algorithm uses the **else** clause to find that $\gcd(12,17) = \gcd(17 \textbf{ mod } 12, 12) = \gcd(5,12)$. It uses this clause again to find that $\gcd(5,12) = \gcd(12 \textbf{ mod } 5, 5) = \gcd(2,5)$, then to get $\gcd(2,5) = \gcd(5 \textbf{ mod } 2, 2) = \gcd(1,2)$, and once more to get $\gcd(1,2) = \gcd(2 \textbf{ mod } 1, 1) = \gcd(0,1)$. Finally, to find $\gcd(0,1)$ it uses the first step with $a = 0$ to find that $\gcd(0,1) = 1$. Consequently, the algorithm finds that $\gcd(12,17) = 1$.

8. The sum of the first n positive integers is the sum of the first $n-1$ positive integers plus n. This trivial observation leads to the recursive algorithm shown here.

procedure *sum of first*(n : positive integer)
if $n = 1$ **then return** 1
else return *sum of first*$(n-1) + n$

10. The recursive algorithm works by comparing the last element with the maximum of all but the last. We assume that the input is given as a sequence.

procedure *max*($a_1, a_2, \ldots, a_n$: integers)
if $n = 1$ **then return** a_1
else
    $m := max(a_1, a_2, \ldots, a_{n-1})$
    if $m > a_n$ **then return** m
    else return a_n

12. This is the inefficient method.

> **procedure** *power*$(x, n, m$: positive integers)
> **if** $n = 1$ **then return** x **mod** m
> **else return** $\big(x \cdot \mathit{power}(x, n-1, m)\big)$ **mod** m

14. This is actually quite subtle. The recursive algorithm will need to keep track not only of what the mode actually is, but also of how often the mode appears. We will describe this algorithm in words, rather than in pseudocode. The input is a list $a_1, a_2, \ldots, a_n$ of integers. Call this list L. If $n = 1$ (the base case), then the output is that the mode is a_1 and it appears 1 time. For the recursive case ($n > 1$), form a new list L' by deleting from L the term a_n and all terms in L equal to a_n. Let k be the number of terms deleted. If $k = n$ (in other words, if L' is the empty list), then the output is that the mode is a_n and it appears n times. Otherwise, apply the algorithm recursively to L', obtaining a mode m, which appears t times. Now if $t \geq k$, then the output is that the mode is m and it appears t times; otherwise the output is that the mode is a_n and it appears k times.

16. The sum of the first one positive integer is 1, and that is the answer the recursive algorithm gives when $n = 1$, so the basis step is correct. Now assume that the algorithm works correctly for $n = k$. If $n = k + 1$, then the **else** clause of the algorithm is executed, and $k + 1$ is added to the (assumed correct) sum of the first k positive integers. Thus the algorithm correctly finds the sum of the first $k + 1$ positive integers.

18. We use mathematical induction on n. If $n = 0$, we know that $0! = 1$ by definition, so the **if** clause handles this basis step correctly. Now fix $k \geq 0$ and assume the inductive hypothesis—that the algorithm correctly computes $k!$. Consider what happens with input $k + 1$. Since $k + 1 > 0$, the **else** clause is executed, and the answer is whatever the algorithm gives as output for input k, which by inductive hypothesis is $k!$, multiplied by $k + 1$. But by definition, $k! \cdot (k + 1) = (k + 1)!$, so the algorithm works correctly on input $k + 1$.

20. Our induction is on the value of y. When $y = 0$, the product $xy = 0$, and the algorithm correctly returns that value. Assume that the algorithm works correctly for smaller values of y, and consider its performance on y. If y is even (and necessarily at least 2), then the algorithm computes 2 times the product of x and $y/2$. Since it does the product correctly (by the inductive hypothesis), this equals $2(x \cdot y/2)$, which equals xy by the commutativity and associativity of multiplication. Similarly, when y is odd, the algorithm computes 2 times the product of x and $(y-1)/2$ and then adds x. Since it does the product correctly (by the inductive hypothesis), this equals $2(x \cdot (y-1)/2) + x$, which equals $xy - x + x = xy$, again by the rules of algebra.

22. The largest in a list of one integer is that one integer, and that is the answer the recursive algorithm gives when $n = 1$, so the basis step is correct. Now assume that the algorithm works correctly for $n = k$. If $n = k + 1$, then the **else** clause of the algorithm is executed. First, by the inductive hypothesis, the algorithm correctly sets m to be the largest among the first k integers in the list. Next it returns as the answer either that value or the $(k + 1)$st element, whichever is larger. This is clearly the largest element in the entire list. Thus the algorithm correctly finds the maximum of a given list of integers.

24. We use the hint.

> **procedure** *twopower*$(n$: positive integer, a : real number)
> **if** $n = 1$ **then return** a^2
> **else return** $\mathit{twopower}(n-1, a)^2$

26. We use the idea in Exercise 24, together with the fact that $a^n = (a^{n/2})^2$ if n is even, and $a^n = a \cdot (a^{(n-1)/2})^2$ if n is odd, to obtain the following recursive algorithm. In essence we are using the binary expansion of n implicitly.

> **procedure** *fastpower*(n : positive integer, a : real number)
> **if** $n = 1$ **then return** a
> **else if** n is even **then return** *fastpower*$(n/2, a)^2$
> **else return** $a \cdot$ *fastpower*$((n-1)/2, a)^2$

28. To compute f_7, Algorithm 7 requires $f_8 - 1 = 20$ additions, and Algorithm 8 requires $7 - 1 = 6$ additions.

30. This is essentially just Algorithm 8, with a different operation and different initial conditions.

```
procedure iterative(n : nonnegative integer)
if n = 0 then y := 1
else
        x := 1
        y := 2
        for i := 1 to n − 1
                z := x · y
                x := y
                y := z
return y {the n^th term of the sequence}
```

32. This is very similar to the recursive procedure for computing the Fibonacci numbers. Note that we can combine the three base cases (stopping rules) into one.

> **procedure** *sequence*(n : nonnegative integer)
> **if** $n < 3$ **then return** $n + 1$
> **else return** *sequence*$(n-1)$ + *sequence*$(n-2)$ + *sequence*$(n-3)$

34. The iterative algorithm is much more efficient here. If we compute with the recursive algorithm, we end up computing the small values (early terms in the sequence) over and over and over again (try it for $n = 5$).

36. We obtain the answer by computing $P(m, m)$, where P is the following procedure, which we obtain simply by copying the recursive definition from Exercise 47 in Section 5.3 into an algorithm.

> **procedure** $P(m, n$: positive integers)
> **if** $m = 1$ **then return** 1
> **else if** $n = 1$ **then return** 1
> **else if** $m < n$ **then return** $P(m, m)$
> **else if** $m = n$ **then return** $1 + P(m, m-1)$
> **else return** $P(m, n-1) + P(m-n, n)$

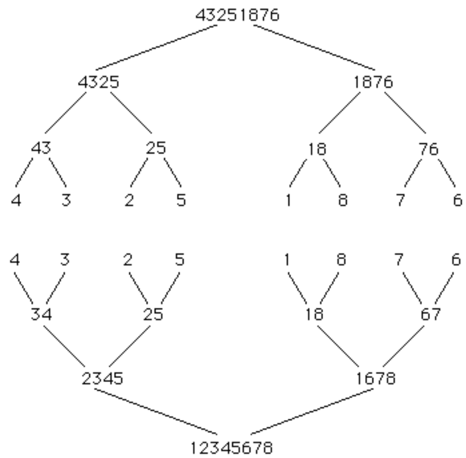
38. The following algorithm practically writes itself.

> **procedure** *power*(w : bit string, i : nonnegative integer)
> **if** $i = 0$ **then return** λ
> **else return** w concatenated with *power*$(w, i-1)$

40. If $i = 0$, then by definition w^i is no copies of w, so it is correct to output the empty string. Inductively, if the algorithm correctly returns the i^{th} power of w, then it correctly returns the $(i+1)^{\text{st}}$ power of w by concatenating one more copy of w.

42. If $n = 3$, then the polygon is already triangulated. Otherwise, by Lemma 1 in Section 5.2, the polygon has a diagonal; draw it. This diagonal splits the polygon into two polygons, each of which has fewer than n vertices. Recursively apply this algorithm to triangulate each of these polygons. The result is a triangulation of the original polygon.

44. The procedure is the same as that given in the solution to Example 9. We will show the tree and inverted tree that indicate how the sequence is taken apart and put back together.



46. From the analysis given before the statement of Lemma 1, it follows that the number of comparisons is $m+n-r$, where the lists have m and n elements, respectively, and r is the number of elements remaining in one list at the point the other list is exhausted. In this exercise $m=n=5$, so the answer is always $10-r$.

a) The answer is $10-1=9$, since the second list has only 1 element when the first list has been emptied.

b) The answer is $10-5=5$, since the second list has 5 elements when the first list has been emptied.

c) The answer is $10-2=8$, since the second list has 2 elements when the first list has been emptied.

48. In each case we need to show that a certain number of comparisons is necessary in the worst case, and then we need to give an algorithm that does the merging with this many comparisons.

a) There are 5 possible outcomes (the element of the first list can be greater than 0, 1, 2, 3, or 4 elements of the second list). Therefore by decision tree theory (see Section 11.2), at least $\lceil \log 5 \rceil = 3$ comparisons are needed. We can achieve this with a binary search: first compare the element of the first list to the second element of the second, and then at most two comparisons are needed to find the correct place for this element.

b) Algorithm 10 merges the lists with 5 comparisons. We must show that 5 are needed in the worst case. Naively applying decision tree theory does not help, since $\lceil \log 15 \rceil = 4$ (there are $C(5+2-1,2)=15$ ways to choose the places among the second list for the elements of the first list to go). Instead, suppose that the lists are a_1, a_2 and b_1, b_2, b_3, b_4, in order. Then without loss of generality assume that the first comparison is a_1 against b_i. If $i \geq 2$ and $a_1 < b_i$, then there are at least 9 outcomes still possible, requiring $\lceil \log 9 \rceil = 4$ more comparisons. If $i=1$ and $a_1 > b_1$, then there are 10 outcomes, again requiring 4 more comparisons.

c) There are $C(5+3-1,3)=35$ outcomes, so at least $\lceil \log 35 \rceil = 6$ comparisons are needed. On the other hand Algorithm 10 uses only 6 comparisons.

d) There are $C(5+4-1,4)=70$ outcomes, so at least $\lceil \log 70 \rceil = 7$ comparisons are needed. On the other hand Algorithm 10 uses only 7 comparisons.

50. On the first pass, we separate the list into two lists, the first being all the elements less than 3 (namely 1 and 2), and the second being all the elements greater than 3, namely $5,7,8,9,4,6$ (in that order). As soon as each of these two lists is sorted (recursively) by quick sort, we are done. We show the entire process in the following sequence of list. The numbers in parentheses are the numbers that are correctly placed by the algorithm on the current level of recursion, and the brackets are those elements that were correctly placed previously. Five levels of recursion are required. 12(3)578946, (1)2[3]4(5)7896, [1](2)[3](4)[5]6(7)89, [1][2][3][4][5](6)[7](8)9, [1][2][3][4][5][6][7][8](9)

52. In practice, this algorithm is coded differently from what we show here, requiring more comparisons but being more efficient because the data structures are simpler (and the sorting is done in place). We denote the list $a_1, a_2, \ldots, a_n$ by a, with similar notations for the other lists. Also, rather than putting a_1 at the end of the first sublist, we put it between the two sublists and do not have to deal with it in either sublist.

```
procedure quick(a_1, a_2, ..., a_n)
b := the empty list
c := the empty list
temp := a_1
for i := 2 to n
        if a_i < a_1 then adjoin a_i to the end of list b
        else adjoin a_i to the end of list c
{notation: m = length(b) and k = length(c)}
if m ≠ 0 then quick(b_1, b_2, ..., b_m)
if k ≠ 0 then quick(c_1, c_2, ..., c_k)
{now put the sorted lists back into a}
for i := 1 to m
        a_i := b_i
a_{m+1} := temp
for i := 1 to k
        a_{m+i+1} := c_i
{the list a is now sorted}
```

54. In the best case, the initial split will require 3 comparisons and result in sublists of length 1 and 2 still to be sorted. These require 0 and 1 comparisons, respectively, and the list has been sorted. Therefore the answer is $3+0+1=4$.

SECTION 5.5 Program Correctness

2. There are two cases. If $x \geq 0$ initially, then nothing is executed, so $x \geq 0$ at the end. If $x < 0$ initially, then x is set equal to 0, so $x = 0$ at the end; hence again $x \geq 0$ at the end.

4. There are three cases. If $x < y$ initially, then min is set equal to x, so $(x \leq y \wedge min = x)$ is true. If $x = y$ initially, then min is set equal to y (which equals x), so again $(x \leq y \wedge min = x)$ is true. Finally, if $x > y$ initially, then min is set equal to y, so $(x > y \wedge min = y)$ is true. Hence in all cases the disjunction $(x \leq y \wedge min = x) \vee (x > y \wedge min = y)$ is true.

6. There are three cases. If $x < 0$, then y is set equal to $-2|x|/x = (-2)(-x)/x = 2$. If $x > 0$, then y is set equal to $2|x|/x = 2x/x = 2$. If $x = 0$, then y is set equal to 2. Hence in all cases $y = 2$ at the termination of this program.

8. We prove that Algorithm 8 in Section 5.4 is correct. It is clearly correct if $n = 0$ or $n = 1$, so we assume that $n \geq 2$. Then the program terminates when the **for** loop terminates, so we concentrate our attention on that loop. Before the loop begins, we have $x = 0$ and $y = 1$. Let the loop invariant p be "$(x = f_{i-1} \wedge y = f_i) \vee (i \text{ is undefined} \wedge x = f_0 \wedge y = f_1)$." This is true at the beginning of the loop, since i is undefined and $f_0 = 0$ and $f_1 = 1$. What we must show now is $p \wedge (1 \leq i < n)\{S\}p$. If $p \wedge (1 \leq i < n)$, then $x = f_{i-1}$ and $y = f_i$. Hence z becomes f_{i+1} by the definition of the Fibonacci sequence. Now x becomes y, namely f_i, and y becomes z, namely f_{i+1}, and i is incremented. Hence for this new (defined) i, $x = f_{i-1}$ and $y = f_i$, as desired. We therefore conclude that upon termination $x = f_{i-1} \wedge y = f_i \wedge i = n$; hence $y = f_n$, as desired.

10. We must show that if p_0 is true before S is executed, then q is true afterwards. Suppose that p_0 is true before S is executed. By the given conditional statement, we know that p_1 is also true. Therefore, since $p_1\{S\}q$, we conclude that q is true after S is executed, as desired.

12. Suppose that the initial assertion is true before the program begins, so that a and d are positive integers. Consider the following loop invariant p: "$a = dq + r$ and $r \geq 0$." This is true before the loop starts, since the equation then states $a = d \cdot 0 + a$, and we are told that a (which equals r at this point) is a positive integer, hence greater than or equal to 0. Now we must show that if p is true and $r \geq d$ before some pass through the loop, then it remains true after the pass. Certainly we still have $r \geq 0$, since all that happened to r was the subtraction of d, and $r \geq d$ to begin this pass. Furthermore, let q' denote the new value of q and r' the new value of r. Then $dq' + r' = d(q+1) + (r-d) = dq + d + r - d = dq + r = a$, as desired. Furthermore, the loop terminates eventually, since one cannot repeated subtract the positive integer d from the positive integer r without r eventually becoming less than d. When the loop terminates, the loop invariant p must still be true, and the condition $r \geq d$ must be false—i.e., $r < d$ must be true. But this is precisely the desired final assertion.

SUPPLEMENTARY EXERCISES FOR CHAPTER 5

2. The proposition is true for $n = 1$, since $1^3 + 3^3 = 28 = 1(1+1)^2(2 \cdot 1^2 + 4 \cdot 1 + 1)$. Assume the inductive hypothesis. Then

$$\begin{aligned} 1^3 + 3^3 + \cdots + (2n+1)^3 + (2n+3)^3 &= (n+1)^2(2n^2+4n+1) + (2n+3)^3 \\ &= 2n^4 + 8n^3 + 11n^2 + 6n + 1 + 8n^3 + 36n^2 + 54n + 27 \\ &= 2n^4 + 16n^3 + 47n^2 + 60n + 28 \\ &= (n+2)^2(2n^2 + 8n + 7) \\ &= (n+2)^2(2(n+1)^2 + 4(n+1) + 1)\,. \end{aligned}$$

4. Our proof is by induction, it being trivial for $n = 1$, since $1/3 = 1/3$. Under the inductive hypothesis

$$\begin{aligned} \frac{1}{1\cdot 3} + \cdots + \frac{1}{(2n-1)(2n+1)} + \frac{1}{(2n+1)(2n+3)} &= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \\ &= \frac{1}{2n+1}\left(n + \frac{1}{2n+3}\right) \\ &= \frac{1}{2n+1}\left(\frac{2n^2+3n+1}{2n+3}\right) \\ &= \frac{1}{2n+1}\left(\frac{(2n+1)(n+1)}{2n+3}\right) = \frac{n+1}{2n+3}\,, \end{aligned}$$

as desired.

6. We prove this statement by induction. The base case is $n = 5$, and indeed $5^2 + 5 = 30 < 32 = 2^5$. Assuming the inductive hypothesis, we have $(n+1)^2 + (n+1) = n^2 + 3n + 2 < n^2 + 4n < n^2 + n^2 = 2n^2 < 2(n^2+n)$, which is less than $2 \cdot 2^n$ by the inductive hypothesis, and this equals 2^{n+1}, as desired.

8. We can let $N = 16$. We prove that $n^4 < 2^n$ for all $n > N$. The base case is $n = 17$, when $17^4 = 83521 < 131072 = 2^{17}$. Assuming the inductive hypothesis, we have $(n+1)^4 = n^4 + 4n^3 + 6n^2 + 4n + 1 < n^4 + 4n^3 + 6n^3 + 4n^3 + 2n^3 = n^4 + 16n^3 < n^4 + n^4 = 2n^4$, which is less than $2 \cdot 2^n$ by the inductive hypothesis, and this equals 2^{n+1}, as desired.

10. If $n = 0$ (base case), then the expression equals $0 + 1 + 8 = 9$, which is divisible by 9. Assume that $n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9. We must show that $(n+1)^3 + (n+2)^3 + (n+3)^3$ is also divisible by 9. The difference of these two expressions is $(n+3)^3 - n^3 = 9n^2 + 27n + 27 = 9(n^2 + 3n + 3)$, a multiple of 9. Therefore since the first expression is divisible by 9, so is the second.

12. We want to prove that 64 divides $9^{n+1} + 56n + 55$ for every positive integer n. For $n = 1$ the expression equals $192 = 64 \cdot 3$. Assume the inductive hypothesis that $64 \mid 9^{n+1} + 56n + 55$ and consider $9^{n+2} + 56(n+1) + 55$. We have $9^{n+2} + 56(n+1) + 55 = 9(9^{n+1} + 56n + 55) - 8 \cdot 56n + 56 - 8 \cdot 55 = 9(9^{n+1} + 56n + 55) - 64 \cdot 7n - 6 \cdot 64$. The first term is divisible by 64 by the inductive hypothesis, and the second and third terms are patently divisible by 64, so our proof by mathematical induction is complete.

14. The two parts are nearly identical, so we do only part **(a)**. Part **(b)** is proved in the same way, substituting multiplication for addition throughout. The basis step is the tautology that if $a_1 \equiv b_1 \pmod{m}$, then $a_1 \equiv b_1 \pmod{m}$. Assume the inductive hypothesis. This tells us that $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m}$. Combining this fact with the fact that $a_{n+1} \equiv b_{n+1} \pmod{m}$, we obtain the desired congruence, $\sum_{j=1}^{n+1} a_j \equiv \sum_{j=1}^{n+1} b_j \pmod{m}$ from Theorem 5 in Section 4.1.

16. After some computation we conjecture that $n + 6 < (n^2 - 8n)/16$ for all $n \geq 28$. (We find that it is not true for smaller values of n.) For the basis step we have $28 + 6 = 34$ and $(28^2 - 8 \cdot 28)/16 = 35$, so the statement is true. Assume that the statement is true for $n = k$. Then since $k > 27$ we have

$$\begin{aligned}\frac{(k+1)^2 - 8(k+1)}{16} = \frac{k^2 - 8k}{16} + \frac{2k-7}{16} &> k + 6 + \frac{2k-7}{16} \quad \text{by the inductive hypothesis}\\ &> k + 6 + \frac{2 \cdot 27 - 7}{16} > k + 6 + 2.9 > (k+1) + 6\,,\end{aligned}$$

as desired.

18. When $n = 1$, we are looking for the derivative of $g(x) = e^{cx}$, which is ce^{cx} by the chain rule, so the statement is true for $n = 1$. Assume that the statement is true for $n = k$, that is, the kth derivative is given by $g^{(k)} = c^k e^{cx}$. Differentiating by the chain rule again (and remembering that c^k is constant) gives us the $(k+1)$st derivative: $g^{(k+1)} = c \cdot c^k e^{cx} = c^{k+1} e^{cx}$, as desired.

20. We look at the first few Fibonacci numbers to see if there is a pattern (all congruences are modulo 3): $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3 \equiv 0$, $f_5 = 5 \equiv 2$, $f_6 = 8 \equiv 2$, $f_7 = 13 \equiv 1$, $f_8 = 21 \equiv 0$, $f_9 = 34 \equiv 1$. We may not see a pattern yet, but note that f_8 and f_9 are the same, modulo 3, as f_0 and f_1. Therefore the sequence must continue to repeat from this point, since the recursive definition gives f_n just in terms of n_{n-1} and f_{n-2}. In particular, $f_{10} \equiv f_2 = 1$, $f_{11} \equiv f_3 = 2$, and so on. Since the pattern has period 8, we can formulate our conjecture as follows:

$$f_n \equiv 0 \pmod{3} \text{ if } n \equiv 0 \text{ or } 4 \pmod{8}$$
$$f_n \equiv 1 \pmod{3} \text{ if } n \equiv 1,\ 2, \text{ or } 7 \pmod{8}$$
$$f_n \equiv 2 \pmod{3} \text{ if } n \equiv 3,\ 5, \text{ or } 6 \pmod{8}$$

To prove this by mathematical induction is tedious. There are two base cases, $n = 0$ and $n = 1$. The conjecture is certainly true in each of them, since $0 \equiv 0 \pmod{8}$ and $f_0 \equiv 0 \pmod{3}$, and $1 \equiv 1 \pmod{8}$ and $f_0 \equiv 1 \pmod{3}$. So we assume the inductive hypothesis and consider a given $n + 1$. There are eight cases to consider, depending on the value of $(n+1)$ **mod** 8. We will carry out one of them; the other seven cases are similar. If $n + 1 \equiv 5 \pmod{8}$, for example, then $n - 1$ and n are congruent to 3 and 4 modulo 8, respectively. By the inductive hypothesis, $f_{n-1} \equiv 2 \pmod{3}$ and $f_n \equiv 0 \pmod{3}$. Therefore f_{n+1}, which is the sum of these two numbers, is equivalent to $2 + 0$, or 2, modulo 3, as desired.

22. There are two base cases: for $n = 0$ we have $f_0 + f_2 = 0 + 1 = 1 = l_1$, and $f_1 + f_3 = 1 + 2 = 3 = l_2$, as desired. Assume the inductive hypothesis, that $f_k + f_{k+2} = l_{k+1}$ for all $k \leq n$ (we are using strong induction here). Then $f_{n+1} + f_{n+3} = f_n + f_{n-1} + f_{n+2} + f_{n+1} = (f_n + f_{n+2}) + (f_{n-1} + f_{n+1}) = l_{n+1} + l_n$ by the inductive hypothesis (with $k = n$ and $k = n - 1$). This last expression equals $l_{n+2} = l_{(n+1)+1}$, however, by the definition of the Lucas numbers, as desired.

24. We follow the hint. Starting with the trivial identity

$$\frac{m+n-1}{n} = \frac{m-1}{n} + 1$$

and multiplying both sides by

$$\frac{m(m+1)\cdots(m+n-2)}{(n-1)!}$$

we obtain the identity given in the hint:

$$\frac{m(m+1)\cdots(m+n-1)}{n!} = \frac{(m-1)m(m+1)\cdots(m+n-2)}{n!} + \frac{m(m+1)\cdots(m+n-2)}{(n-1)!}$$

Now we want to show that the product of any n consecutive positive integers is divisible by $n!$. We prove this by induction on n. The case $n = 1$ is clear, since every integer is divisible by $1!$. Assume the inductive hypothesis, that the statement is true for $n-1$. To prove the statement for n, now, we will give a proof using induction on the starting point of the sequence of n consecutive positive integers. Call this starting point m. The basis step, $m = 1$, is again clear, since the product of the first n positive integers *is* $n!$. Assume the inductive hypothesis that the statement is true for $m-1$. Note that we have two inductive hypotheses active here: the statement is true for $n-1$, and the statement is true also for $m-1$ and n. We are trying to prove the statement true for m and n. At this point we simply stare at the identity given above. The first term on the right-hand side is an integer by the inductive hypothesis about $m-1$ and n. The second term on the right-hand side is an integer by the inductive hypothesis about $n-1$. Therefore the expression is an integer. But the statement that the left-hand side is an integer is precisely what we wanted—that the product of the n positive integers starting with m is divisible by $n!$.

26. The algebra gets very messy here, but the ideas are not advanced. We will use the following standard trigonometric identity, which is proved using the standard formulae for the sine and cosine of sums and differences:

$$\cos A \sin B = \frac{\sin(A+B) - \sin(A-B)}{2}$$

The proof of the identity in this exercise is by induction, of course. The basis step ($n = 1$) is the true statement that

$$\cos x = \frac{\cos x \sin(x/2)}{\sin(x/2)}.$$

Assume the inductive hypothesis:

$$\sum_{j=1}^{n} \cos jx = \frac{\cos((n+1)x/2)\sin(nx/2)}{\sin(x/2)}$$

Now it is clear that the inductive step is equivalent to showing that adding the $(n+1)^{\text{th}}$ term in the sum to the expression on the right-hand side of the last displayed equation yields the same expression with $n+1$ substituted for n. In other words, we must show that

$$\cos(n+1)x + \frac{\cos((n+1)x/2)\sin(nx/2)}{\sin(x/2)} = \frac{\cos((n+2)x/2)\sin((n+1)x/2)}{\sin(x/2)},$$

which can be rewritten without fractions as

$$\sin(x/2)\cos(n+1)x + \cos((n+1)x/2)\sin(nx/2) = \cos((n+2)x/2)\sin((n+1)x/2).$$

But this follows after a little calculation using the trigonometric identity displayed at the beginning of this solution, since both sides equal

$$\frac{\sin((2n+3)x/2) - \sin(x/2)}{2}\,.$$

28. We compute a few terms to get a feel for what is going on: $x_1 = \sqrt{6} \approx 2.45$, $x_2 = \sqrt{\sqrt{6}+6} \approx 2.91$, $x_3 \approx 2.98$, and so on. The values seem to be approaching 3 from below in an increasing manner.

a) Clearly $x_0 < x_1$. Assume that $x_{k-1} < x_k$. Then $x_k = \sqrt{x_{k-1}+6} < \sqrt{x_k+6} = x_{k+1}$, and the inductive step is proved.

b) Since $\sqrt{6} < \sqrt{9} = 3$, the basis step is proved. Assume that $x_k < 3$. Then $x_{k+1} = \sqrt{x_k+6} < \sqrt{3+6} = 3$, and the inductive step is proved.

c) By a result from mathematical analysis, an increasing bounded sequence converges to a limit. If we call this limit L, then we must have $L = \sqrt{L+6}$, by letting $n \to \infty$ in the defining equation. Solving this equation for L yields $L = 3$. (The root $L = -2$ is extraneous, since L is positive.)

30. We first prove that such an expression exists. The basis step will handle all $n < b$. These cases are clear, because we can take $k = 0$ and $a_0 = n$. Assume the inductive hypothesis, that we can express all nonnegative integers less than n in this way, and consider an arbitrary $n \ge b$. By the division algorithm (Theorem 2 in Section 4.1), we can write n as $q \cdot b + r$, where $0 \le r < b$. By the inductive hypothesis, we can write q as $a_k b^k + a_{k-1}b^{k-1} + \cdots + a_1 b + a_0$. This means that $n = (a_k b^k + a_{k-1}b^{k-1} + \cdots + a_1 b + a_0) \cdot b + r = a_k b^{k+1} + a_{k-1}b^k + \cdots + a_1 b^2 + a_0 b + r$, and this is in the desired form.

For uniqueness, suppose that $a_k b^k + a_{k-1}b^{k-1} + \cdots + a_1 b + a_0 = c_k b^k + c_{k-1}b^{k-1} + \cdots + c_1 b + c_0$, where we have added initial terms with zero coefficients if necessary so that each side has the same number of terms; thus we have $0 \le a_i < b$ and $0 \le c_i < b$ for all i. Subtracting the second expansion from both sides gives us $(a_k - c_k)b^k + (a_{k-1} - c_{k-1})b^{k-1} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0$. If the two expressions are different, then there is a smallest integer j such that $a_j \ne c_j$; that means that $a_i = c_i$ for $i = 0, 1, \ldots, j-1$. Hence

$$b^j\big((a_k - c_k)b^{k-j} + (a_{k-1} - c_{k-1})b^{k-j-1} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)\big) = 0\,,$$

so

$$(a_k - c_k)b^{k-j} + (a_{k-1} - c_{k-1})b^{k-j-1} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0\,.$$

Solving for $a_j - c_j$ we have

$$\begin{aligned} a_j - c_j &= (c_k - a_k)b^{k-j} + (c_{k-1} - a_{k-1})b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1})b \\ &= b\big((c_k - a_k)b^{k-j-1} + (c_{k-1} - a_{k-1})b^{k-j-2} + \cdots + (c_{j+1} - a_{j+1})\big)\,. \end{aligned}$$

But this means that b divides $a_j - c_j$. Because both a_j and c_j are between 0 and $b-1$, inclusive, this is possible only if $a_j = b_j$, a contradiction. Thus the expression is unique.

32. For simplicity we will suppress the arguments ("(x)")and just write f' for the derivative of f. We also assume, of course, that denominators are not zero. If $n = 1$ there is nothing to prove, and the $n = 2$ case is just an application of the product rule:

$$\frac{(f_1 f_2)'}{f_1 f_2} = \frac{f_1' f_2 + f_1 f_2'}{f_1 f_2} = \frac{f_1'}{f_1} + \frac{f_2'}{f_2}\,.$$

Assume the inductive hypothesis and consider the situation for $n+1$:

$$\begin{aligned} \frac{(f_1 f_2 \cdots f_n f_{n+1})'}{f_1 f_2 \cdots f_n f_{n+1}} &= \frac{(f_1 f_2 \cdots f_n)' f_{n+1} + (f_1 f_2 \cdots f_n) f_{n+1}'}{(f_1 f_2 \cdots f_n) f_{n+1}} \\ &= \frac{(f_1 f_2 \cdots f_n)'}{(f_1 f_2 \cdots f_n)} + \frac{f_{n+1}'}{f_{n+1}} \\ &= \frac{f_1'}{f_1} + \frac{f_2'}{f_2} + \cdots + \frac{f_n'}{f_n} + \frac{f_{n+1}'}{f_{n+1}}\,. \end{aligned}$$

The first line followed from the product rule, the second line was algebra, and the third line followed from the inductive hypothesis.

34. Call a coloring proper if no two regions that have an edge in common have a common color. For the basis step we can produce a proper coloring if there is only one line by coloring the half of the plane on one side of the line red and the other half blue. Assume that a proper coloring is possible with k lines. If we have $k+1$ lines, remove one of the lines, properly color the configuration produced by the remaining lines, and then put the last line back. Reverse all the colors on one side of the last line. The resulting coloring will be proper.

36. It will be convenient to clear fractions by multiplying both sides by the product of all the x_s's; this makes the desired inequality

$$(x_1^2+1)(x_2^2+1)\cdots(x_n^2+1) \ge (x_1x_2+1)(x_2x_3+1)\cdots(x_{n-1}x_n+1)(x_nx_1+1)\,.$$

The basis step is

$$(x_1^2+1)(x_2^2+1) \ge (x_1x_2+1)(x_2x_1+1)\,.$$

which after algebraic simplification and factoring becomes $(x_1-x_2)^2 \ge 0$ and therefore is correct. For the inductive step, we assume that the inequality is true for n and hope to prove

$$(x_1^2+1)(x_2^2+1)\cdots(x_n^2+1)(x_{n+1}^2+1) \ge (x_1x_2+1)(x_2x_3+1)\cdots(x_{n-1}x_n+1)(x_nx_{n+1}+1)(x_{n+1}x_1+1)\,.$$

Because of the cyclic form of this inequality, we can without loss of generality assume that x_{n+1} is the largest (or tied for the largest) of all the given numbers. By the inductive hypothesis we have

$$(x_1^2+1)(x_2^2+1)\cdots(x_n^2+1)(x_{n+1}^2+1) \ge (x_1x_2+1)(x_2x_3+1)\cdots(x_{n-1}x_n+1)(x_nx_1+1)(x_{n+1}^2+1)\,,$$

so it suffices to show that

$$(x_nx_1+1)(x_{n+1}^2+1) \ge (x_nx_{n+1}+1)(x_{n+1}x_1+1)\,.$$

But after algebraic simplification and factoring, this becomes $(x_{n+1}-x_1)(x_{n+1}-x_n) \ge 0$, which is true by our assumption that x_{n+1} is the largest number in the list.

38. (It will be helpful for the reader to draw a diagram to help in following this proof.) We use induction on n, the number of cities, the result being trivial if $n=1$ or $n=2$. Assume the inductive hypothesis and suppose that we have a country with $k+1$ cities, labeled c_1 through c_{k+1}. Remove c_{k+1} and apply the inductive hypothesis to find a city c that can be reached either directly or with one intermediate stop from each of the other cities among c_1 through c_k. If the one-way road leads from c_{k+1} to c, then we are done, so we can assume that the road leads from c to c_{k+1}. If there are any one-way roads from c_{k+1} to a city with a one-way road to c, then we are also done, so we can assume that each road between c_{k+1} and a city with a one-way road to c leads from such a city to c_{k+1}. Thus c and all the cities with a one-way road to c have a direct road to c_{k+1}. All the remaining cities must have a one-way road from them to a city with a one-way road to c (that was part of the definition of c), and so they have paths of length 2 to c_{k+1}, via some such city. Therefore c_{k+1} satisfies the conditions of the problem, and the proof is complete.

40. We have to assume from the statement of the problem that all the cars get are equally efficient in terms of miles per gallon. We proceed by induction on n, the number of cars in the group. If $n=1$, then the one car has enough fuel to complete the lap. Assume the inductive hypothesis that the statement is true for a group of k cars, and suppose we have a group of $k+1$ cars. It helps to think of the cars as stationary, not moving yet. We claim that at least one car c in the group has enough fuel to reach the next car in the group. If this were not so, then the total amount of fuel in all the cars combined would not cover the full lap (think of each car as traveling as far as it can on its own fuel). So now pretend that the car d just ahead of car c is not present, and instead the fuel in that car is in c's tank. By the inductive hypothesis (we still have the same total amount of fuel), some car in this situation can complete a lap by obtaining fuel from other cars as it travels around the track. Then this same car can complete the lap in the actual situation, because if and when it needs to move from the location of car c to the location of the car d, the amount of fuel it has available without d's fuel that we are pretending c already has will be sufficient for it to reach d, at which time this extra fuel becomes available (because this car made it to c's location and car c has enough fuel to reach d's location).

42. The basis step is $n = 3$. Because the hypotenuse is the longest side of a right triangle, $c > a$ and $c > b$. Therefore

$$c^3 = c \cdot c^2 = c(a^2 + b^2) = c \cdot a^2 + c \cdot b^2 > a \cdot a^2 + b \cdot b^2 = a^3 + b^3 .$$

For the inductive step,

$$c^{k+1} = c \cdot c^k > c(a^k + b^k) = c \cdot a^k + c \cdot b^k > a \cdot a^k + b \cdot b^k = a^{k+1} + b^{k+1} .$$

One can also give a noninductive proof much along the same lines:

$$c^n = c^2 \cdot c^{n-2} = (a^2 + b^2) \cdot c^{n-2} = a^2 \cdot c^{n-2} + b^2 \cdot c^{n-2} > a^2 \cdot a^{n-2} + b^2 \cdot b^{n-2} = a^n + b^n$$

44. **a)** The basis step is to prove the statement that this algorithm terminates for all fractions of the form $1/q$. Since this fraction is already a unit fraction, there is nothing more to prove.

b) For the inductive step, assume that the algorithm terminates for all proper positive fractions with numerators smaller than p, suppose that we are starting with the proper positive fraction p/q, and suppose that the algorithm selects $1/n$ as the first step in the algorithm. Note that necessarily $n > 1$. Therefore we can write $p/q = p'/q' + 1/n$. If $p/q = 1/n$, we are done, so assume that $p/q > 1/n$. By finding a common denominator and subtracting, we see that we can take $p' = np - q$ and $q' = nq$. We claim that $p' < p$, which algebraically is easily seen to be equivalent to $p/q < 1/(n-1)$, and this is true by the choice of n such that $1/n$ is the largest unit fraction not exceeding p/q. Therefore by the inductive hypothesis we can write p'/q' as the sum of distinct unit fractions with increasing denominators, and thereby have written p/q as the sum of unit fractions. The only thing left to check is that $p'/q' < 1/n$, so that the algorithm will not try to choose $1/n$ again for p'/q'. But if this were not the case, then $p/q \geq 2/n$, and combining this with the inequality $p/q < 1/(n-1)$ given above, we would have $2/n < 1/(n-1)$, which would mean that $n = 1$, a contradiction.

46. What we really need to show is that the definition "terminates" for every n. It is conceivable that trying to apply the definition gets us into some kind of infinite loop, using the second line; we need to show that this is not the case. We will give a very strange kind of proof by mathematical induction. First, following the hint, we will show that the definition tells us that $M(n) = 91$ for all positive integers $n \leq 101$. We do this by backwards induction, starting with $n = 101$ and going down toward $n = 1$. There are 11 base cases: $n = 101$, 100, 99, $\ldots$, 91. The first line of the definition tells us immediately that $M(101) = 101 - 10 = 91$. To compute $M(100)$ we have

$$\begin{aligned} M(100) &= M(M(100 + 11)) = M(M(111)) \\ &= M(111 - 10) = M(101) = 91 . \end{aligned}$$

The last equality came from the fact that we had already computed $M(101)$. Similarly,

$$\begin{aligned} M(99) &= M(M(99 + 11)) = M(M(110)) \\ &= M(110 - 10) = M(100) = 91 , \end{aligned}$$

and so on down to

$$\begin{aligned} M(91) &= M(M(91 + 11)) = M(M(102)) \\ &= M(102 - 10) = M(92) = 91 . \end{aligned}$$

In each case the final equality comes from the previously computed value. Now assume the inductive hypothesis, that $M(k) = 91$ for all k from $n+1$ through 101 (i.e., if $n+1 \le k \le 101$); we must prove that $M(n) = 91$, where n is some fixed positive integer less than 91. To compute $M(n)$, we have

$$M(n) = M(M(n+11)) = M(91) = 91$$

where the next to last equality comes from the fact that $n+11$ is between $n+1$ and 101. Thus we have proved that $M(n) = 91$ for all $n \le 101$. The first line of the definition takes care of values of n greater than 101, so the entire function is well-defined.

48. We proceed by induction on n. The case $n=2$ is just the definition of symmetric difference. Assume that the statement is true for $n-1$; we must show that it is true for n. By definition $R_n = R_{n-1} \oplus A_n$. We must show that an element x is in R_n if and only if it belongs to an odd number of the sets $A_1, A_2, \ldots, A_n$. The inductive hypothesis tells us that x is in R_{n-1} if and only if x belongs to an odd number of the sets $A_1, A_2, \ldots, A_{n-1}$. There are four cases. Suppose first that $x \in R_{n-1}$ and $x \in A_n$. Then x belongs to an odd number of the sets $A_1, A_2, \ldots, A_{n-1}$ and therefore belongs to an even number of the sets $A_1, A_2, \ldots, A_n$; thus $x \notin R_n$, which is correct by the definition of $\oplus$. Next suppose that $x \in R_{n-1}$ and $x \notin A_n$. Then x belongs to an odd number of the sets $A_1, A_2, \ldots, A_{n-1}$ and therefore belongs to an odd number of the sets $A_1, A_2, \ldots, A_n$; thus $x \in R_n$, which is again correct by the definition of $\oplus$. For the third case, suppose that $x \notin R_{n-1}$ and $x \in A_n$. Then x belongs to an even number of the sets $A_1, A_2, \ldots, A_{n-1}$ and therefore belongs to an odd number of the sets $A_1, A_2, \ldots, A_n$; thus $x \in R_n$, which is again correct by the definition of $\oplus$. The last case ($x \notin R_{n-1}$ and $x \notin A_n$) is similar.

50. This problem is similar to and uses the result of Exercise 62 in Section 5.1. The lemma we need is that if there are n planes meeting the stated conditions, then adding one more plane, which intersects the original figure in the manner described, results in the addition of $(n^2+n+2)/2$ new regions. The reason for this is that the pattern formed on the new plane by all the lines of intersection of this plane with the planes already present has, by Exercise 62 in Section 5.1, $(n^2+n+2)/2$ regions; and each of these two-dimensional regions separates the three-dimensional region through which it passes into two three-dimensional regions. Therefore the proof by induction of the present exercise reduces to noting that one plane separates space into $(1^3+5\cdot 1+6)/6 = 2$ regions, and verifying the algebraic identity

$$\frac{n^3+5n+6}{6} + \frac{n^2+n+2}{2} = \frac{(n+1)^3+5(n+1)+6}{6}\,.$$

52. **a)** This set is not well ordered, since the set itself has no least element (the negative integers get smaller and smaller).

b) This set is well ordered—the problem inherent in part **(a)** is not present here because the entire set has -99 as its least element. Every subset also has a least element.

c) This set is not well ordered. The entire set, for example, has no least element, since the numbers of the form $1/n$ for n a positive integer get smaller and smaller.

d) This set is well ordered. The situation is analogous to part **(b)**.

54. In the preamble to Exercise 42 in Section 4.3, an algorithm was described for writing the greatest common divisor of two positive integers as a linear combination of these two integer (see also Theorem 6 and Example 17 in that section). We can use that algorithm, together with the result of Exercise 53, to solve this problem. For $n=1$ there is nothing to do, since $a_1 = a_1$, and we already have an algorithm for $n=2$. For $n>2$, we can write $\gcd(a_{n-1}, a_n)$ as a linear combination of a_{n-1} and a_n, say as

$$\gcd(a_{n-1}, a_n) = c_{n-1}a_{n-1} + c_n a_n\,.$$

Then we apply the algorithm recursively to the numbers a_1, a_2, $\ldots$, a_{n-2}, $\gcd(a_{n-1}, a_n)$. This gives us the following equation:

$$\gcd(a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n)) = c_1a_1 + c_2a_2 + \cdots + c_{n-2}a_{n-2} + Q \cdot \gcd(a_{n-1}, a_n)$$

Plugging in from the previous display, we have the desired linear combination:

$$\begin{aligned}\gcd(a_1, a_2, \ldots, a_n) &= \gcd(a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n)) \\ &= c_1a_1 + c_2a_2 + \cdots + c_{n-2}a_{n-2} + Q(c_{n-1}a_{n-1} + c_na_n) \\ &= c_1a_1 + c_2a_2 + \cdots + c_{n-2}a_{n-2} + Qc_{n-1}a_{n-1} + Qc_na_n\end{aligned}$$

56. The following definition works. The empty string is in the set, and if x and y are in the set, then so are xy, $1x00$, $00x1$, and $0x1y0$. One way to see this is to think of graphing, for a string in this set, the quantity (number of 0's) $-\, 2 \cdot$ (number of 1's) as a function of the position in the string. This graph must start and end at the horizontal axis. If it contains another point on the axis, then we can split the string into xy where x and y are both in the set. If the graph stays above the axis, then the string must be of the form $00x1$, and if it stays below the axis, then it must be of the form $1x00$. The only other case is that in which the graph crosses the axis at a 1 in the string, without landing on the axis. In this case, the string must look like $0x1y0$.

58. **a)** The set contains three strings of length 3, and each of them gives us four more strings of length 6, using the fourth through seventh rules, except that there is a bit of overlap, so that in fact there are only 13 strings in all. The strings are *abc*, *bac*, *acb*, *abcabc*, *ababcc*, *aabcbc*, *abcbac*, *abbacc*, *abacbc*, *bacabc*, *abcacb*, *aacbbc*, and *acbabc*.

b) We prove this by induction on the length of the string. The basis step is vacuously true, since there are no strings in the set of length 0 (and it is trivially true anyway, since 0 is a multiple of 3). Assume the inductive hypothesis that the statement is true for shorter strings, and let y be a string in S. If $y \in S$ by one of the first three rules, then y has length 3. If $y \in S$ by one of the last four rules, then the length of y is equal to 3 plus the length of x. By the inductive hypothesis, the length of x is a multiple of 3, so the length of y is also a multiple of 3.

60. By applying the recursive rules we get the following list: ((())), (()()), ()()(), ()(()), (())().

62. We use induction on the length of the string x of balanced parentheses. If $x = \lambda$, then the statement is true since $0 = 0$. Otherwise $x = (a)$ or $x = ab$, where a and b are shorter balanced strings of parentheses. In the first case, the number of parentheses of each type in x is one more than the corresponding number in a, so by the inductive hypothesis these numbers are equal. In the second case, the number of parentheses of each type in x is the sum of the corresponding numbers in a and b, so again by the inductive hypothesis these numbers are equal.

64. We prove the "only if" part by induction on the length of the balanced string w. If $w = \lambda$, then there is nothing to prove. If $w = (x)$, then we have by the inductive hypothesis that $N(x) = 0$ and that $N(a) \geq 0$ if a is a prefix of x. Then $N(w) = 1 + 0 + (-1) = 0$; and $N(b) \geq 1 \geq 0$ if b is a nonempty prefix of w, since $b = (a$. If $w = xy$, then we have by the inductive hypothesis that $N(x) = N(y) = 0$; and $N(a) \geq 0$ if a is a prefix of x or y. Then $N(w) = 0 + 0 = 0$; and $N(b) \geq 0$ if b is a prefix of w, since either b is a prefix of x or $b = xa$ where a is a prefix of y.

We also prove the "if" part by induction on the length of the string w. Suppose that w satisfies the condition. If $w = \lambda$, then $w \in B$. Otherwise w must begin with a parenthesis, and it must be a left parenthesis, since otherwise the prefix of length 1 would give us $N\big()\big) = -1$. Now there are two cases: either $w = ab$, where $N(a) = N(b) = 0$ and $a \neq \lambda \neq b$, or not. If so, then a and b are balanced strings of parentheses by the inductive hypothesis (noting that prefixes of a are prefixes of w, and prefixes of b are a followed by prefixes of w), so w is balanced by the recursive definition of the set of balanced strings. In the other case, $N(u) \geq 1$ for all nonempty prefixes u of w, other than w itself. Thus w must end with a right parenthesis to make $N(w) = 0$. So $w = (x)$, and $N(x) = 0$. Furthermore $N(u) \geq 0$ for every prefix u of x, since if $N(u)$ dipped to -1, then $N\big((u\big) = 0$ and we would be in the first case. Therefore by the inductive hypothesis x is balanced, and so by the definition of balanced strings w is balanced, as desired.

66. We copy the definition into an algorithm.

> **procedure** $gcd(a, b:$ nonnegative integers, not both zero$)$
> **if** $a > b$ **then return** $gcd(b, a)$
> **else if** $a = 0$ **then return** b
> **else if** a and b are even **then return** $2 \cdot gcd(a/2, b/2)$
> **else if** a is even and b is odd **then return** $gcd(a/2, b)$
> **else return** $gcd(a, b - a)$

68. To prove that a recursive program is correct, we need to check that it works correctly for the base case, and that it works correctly for the inductive step under the inductive assumption that it works correctly on its recursive call. To apply this rule of inference to Algorithm 1 in Section 5.4, we reason as follows. The base case is $n = 1$. In that case the **then** clause is executed, and not the **else** clause, and so the procedure gives the correct value, namely 1. Now assume that the procedure works correctly for $n - 1$, and we want to show that it gives the correct value for the input n, where $n > 1$. In this case, the **else** clause is executed, and not the **then** clause, so the procedure gives us n times whatever the procedure gives for input $n - 1$. By the inductive hypothesis, we know that this latter value is $(n-1)!$. Therefore the procedure gives $n \cdot (n-1)!$, which by definition is equal to $n!$, exactly as we wished.

70. We apply the definition:

$$\begin{aligned}
a(0) &= 0\\
a(1) &= 1 - a(a(0)) = 1 - a(0) = 1 - 0 = 1\\
a(2) &= 2 - a(a(1)) = 2 - a(1) = 2 - 1 = 1\\
a(3) &= 3 - a(a(2)) = 3 - a(1) = 3 - 1 = 2\\
a(4) &= 4 - a(a(3)) = 4 - a(2) = 4 - 1 = 3\\
a(5) &= 5 - a(a(4)) = 5 - a(3) = 5 - 2 = 3\\
a(6) &= 6 - a(a(5)) = 6 - a(3) = 6 - 2 = 4\\
a(7) &= 7 - a(a(6)) = 7 - a(4) = 7 - 3 = 4\\
a(8) &= 8 - a(a(7)) = 8 - a(4) = 8 - 3 = 5\\
a(9) &= 9 - a(a(8)) = 9 - a(5) = 9 - 3 = 6
\end{aligned}$$

72. We follow the hint. First note that by algebra, $\mu^2 = 1 - \mu$, and that $\mu \approx 0.618$. Therefore we have $(\mu n - \lfloor \mu n \rfloor) + (\mu^2 n - \lfloor \mu^2 n \rfloor) = \mu n - \lfloor \mu n \rfloor + (1-\mu)n - \lfloor (1-\mu)n \rfloor = \mu n - \lfloor \mu n \rfloor + n - \mu n - \lfloor n - \mu n \rfloor = \mu n - \lfloor \mu n \rfloor + n - \mu n - n - \lfloor -\mu n \rfloor = -\lfloor \mu n \rfloor - (-\lceil \mu n \rceil) = -\lfloor \mu n \rfloor + \lceil \mu n \rceil = 1$, since μn is irrational and therefore not an integer. (We used here some of the properties of the floor and ceiling function from Table 1 in Section 2.3.) Next, continuing with the hint, suppose that $0 \leq \alpha < 1 - \mu$, and consider $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor$. The second floor term is 0, since $\alpha < 1 - \mu$. The product $(1+\mu)(1-\alpha)$ is greater than $(1+\mu)\mu = \mu + \mu^2 = 1$ and less than $(1 + 1 - \alpha)(1 - \alpha) < 2 \cdot 1 = 2$, so the whole sum equals 1, as desired. For the other case, suppose that $1 - \mu < \alpha < 1$, and again consider $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor$. Here $\alpha + \mu$ is between 1 and 2, and $(1+\mu)(1-\alpha) < 1$, so again the sum is 1.

The rest of the proof is pretty messy algebra. Since we already know from Exercise 71 that the function $a(n)$ is well-defined by the recurrence $a(n) = n - a(a(n-1))$ for all $n \geq 1$ and initial condition $a(0) = 0$, it suffices to prove that $\lfloor (n+1)\mu \rfloor$ satisfies these equations. It clearly satisfies the second, since $0 < \mu < 1$. Thus we must show that $\lfloor (n+1)\mu \rfloor = n - \lfloor (\lfloor n\mu \rfloor + 1)\mu \rfloor$ for all $n \geq 1$. Let $\alpha = n\mu - \lfloor n\mu \rfloor$; then $0 \leq \alpha < 1$, and $\alpha \neq 1 - \mu$, since μ is irrational. First consider $\lfloor (\lfloor n\mu \rfloor + 1)\mu \rfloor$. It equals $\lfloor \mu(1 + \mu n - \alpha) \rfloor = \lfloor \mu + \mu^2 n - \alpha\mu \rfloor = \lfloor \mu + 1 - \alpha + \lfloor \mu^2 n \rfloor - \alpha\mu \rfloor$ by the first fact proved above. Since $\lfloor \mu^2 n \rfloor$ is an integer, this equals $\lfloor \mu^2 n \rfloor + \lfloor \mu + 1 - \alpha - \alpha\mu \rfloor = \lfloor \mu^2 n \rfloor + \lfloor (1+\mu)(1-\alpha) \rfloor = \mu^2 n - 1 + \alpha + \lfloor (1+\mu)(1-\alpha) \rfloor$. Next consider $\lfloor (n+1)\mu \rfloor$. It equals $\lfloor \mu n + \mu \rfloor = \lfloor \lfloor \mu n \rfloor + \alpha + \mu \rfloor = \lfloor \mu n \rfloor + \lfloor \alpha + \mu \rfloor = \mu n - \alpha + \lfloor \alpha + \mu \rfloor$. Putting these together we have $\lfloor (\lfloor n\mu \rfloor + 1)\mu \rfloor + \lfloor (n+1)\mu \rfloor - n = \mu^2 n - 1 + \alpha + \lfloor (1+\mu)(1-\alpha) \rfloor + \mu n - \alpha + \lfloor \alpha + \mu \rfloor - n = (\mu^2 + \mu - 1)n - 1 + \lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor$, which equals $0 - 1 + 1 = 0$ by the definition of μ and the second fact proved above. This is equivalent to what we wanted.

74. a) We apply the definition:

$$
\begin{aligned}
&a(0) = 0 \\
&a(1) = 1 - a(a(a(0))) = 1 - a(a(0)) = 1 - a(0) = 1 - 0 = 1 \\
&a(2) = 2 - a(a(a(1))) = 2 - a(a(1)) = 2 - a(1) = 2 - 1 = 1 \\
&a(3) = 3 - a(a(a(2))) = 3 - a(a(1)) = 3 - a(1) = 3 - 1 = 2 \\
&a(4) = 4 - a(a(a(3))) = 4 - a(a(2)) = 4 - a(1) = 4 - 1 = 3 \\
&a(5) = 5 - a(a(a(4))) = 5 - a(a(3)) = 5 - a(2) = 5 - 1 = 4 \\
&a(6) = 6 - a(a(a(5))) = 6 - a(a(4)) = 6 - a(3) = 6 - 2 = 4 \\
&a(7) = 7 - a(a(a(6))) = 7 - a(a(4)) = 7 - a(3) = 7 - 2 = 5 \\
&a(8) = 8 - a(a(a(7))) = 8 - a(a(5)) = 8 - a(4) = 8 - 3 = 5 \\
&a(9) = 9 - a(a(a(8))) = 9 - a(a(5)) = 9 - a(4) = 9 - 3 = 6
\end{aligned}
$$

b) We apply the definition:

$$
\begin{aligned}
&a(0) = 0 \\
&a(1) = 1 - a(a(a(a(0)))) = 1 - a(a(a(0))) = 1 - a(a(0)) = 1 - a(0) = 1 - 0 = 1 \\
&a(2) = 2 - a(a(a(a(1)))) = 2 - a(a(a(1))) = 2 - a(a(1)) = 2 - a(1) = 2 - 1 = 1 \\
&a(3) = 3 - a(a(a(a(2)))) = 3 - a(a(a(1))) = 3 - a(a(1)) = 3 - a(1) = 3 - 1 = 2 \\
&a(4) = 4 - a(a(a(a(3)))) = 4 - a(a(a(2))) = 4 - a(a(1)) = 4 - a(1) = 4 - 1 = 3 \\
&a(5) = 5 - a(a(a(a(4)))) = 5 - a(a(a(3))) = 5 - a(a(2)) = 5 - a(1) = 5 - 1 = 4 \\
&a(6) = 6 - a(a(a(a(5)))) = 6 - a(a(a(4))) = 6 - a(a(3)) = 6 - a(2) = 6 - 1 = 5 \\
&a(7) = 7 - a(a(a(a(6)))) = 7 - a(a(a(5))) = 7 - a(a(4)) = 7 - a(3) = 7 - 2 = 5 \\
&a(8) = 8 - a(a(a(a(7)))) = 8 - a(a(a(5))) = 8 - a(a(4)) = 8 - a(3) = 8 - 2 = 6 \\
&a(9) = 9 - a(a(a(a(8)))) = 9 - a(a(a(6))) = 9 - a(a(5)) = 9 - a(4) = 9 - 3 = 6
\end{aligned}
$$

c) We apply the definition:

$$\begin{aligned}
a(1) &= 1\\
a(2) &= 1\\
a(3) &= a(3-a(2)) + a(3-a(1)) = a(3-1) + a(3-1) = a(2) + a(2) = 1+1 = 2\\
a(4) &= a(4-a(3)) + a(4-a(2)) = a(4-2) + a(4-1) = a(2) + a(3) = 1+2 = 3\\
a(5) &= a(5-a(4)) + a(5-a(3)) = a(5-3) + a(5-2) = a(2) + a(3) = 1+2 = 3\\
a(6) &= a(6-a(5)) + a(6-a(4)) = a(6-3) + a(6-3) = a(3) + a(3) = 2+2 = 4\\
a(7) &= a(7-a(6)) + a(7-a(5)) = a(7-4) + a(7-3) = a(3) + a(4) = 2+3 = 5\\
a(8) &= a(8-a(7)) + a(8-a(6)) = a(8-5) + a(8-4) = a(3) + a(4) = 2+3 = 5\\
a(9) &= a(9-a(8)) + a(9-a(7)) = a(9-5) + a(9-5) = a(4) + a(4) = 3+3 = 6\\
a(10) &= a(10-a(9)) + a(10-a(8)) = a(10-6) + a(10-5) = a(4) + a(5) = 3+3 = 6
\end{aligned}$$

76. The first term a_1 tells how many 1's there are. If $a_1 \geq 2$, then the sequence would not be nondecreasing, since a 1 would follow this 2. Therefore $a_1 = 1$. This tells us that there is one 1, so the next term must be at least 2. By the same reasoning as before, a_2 can't be 3 or larger, so $a_2 = 2$. This tells us that there are two 2's, and they must all come together since the sequence is nondecreasing. So $a_3 = 2$ as well. But now we know that there are two 3's, and of course they must come next. We continue in this way and obtain the first 20 terms:

1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8

CHAPTER 6
Counting

SECTION 6.1 The Basics of Counting

2. By the product rule there are $27 \cdot 37 = 999$ offices.

4. By the product rule there are $12 \cdot 2 \cdot 3 = 72$ different types of shirt.

6. By the product rule there are $4 \cdot 6 = 24$ routes.

8. There are 26 choices for the first initial, then 25 choices for the second, if no letter is to be repeated, then 24 choices for the third. (We interpret "repeated" broadly, so that a string like RWR, for example, is prohibited, as well as a string like RRW.) Therefore by the product rule the answer is $26 \cdot 25 \cdot 24 = 15{,}600$.

10. We have two choices for each bit, so there are $2^8 = 256$ bit strings.

12. We use the sum rule, adding the number of bit strings of each length up to 6. If we include the empty string, then we get $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 2^7 - 1 = 127$ (using the formula for the sum of a geometric progression—see Theorem 1 in Section 2.4).

14. If $n = 0$, then the empty string—vacuously—satisfies the condition (or does not, depending on how one views it). If $n = 1$, then there is one, namely the string 1. If $n \geq 2$, then such a string is determined by specifying the $n-2$ bits between the first bit and the last, so there are 2^{n-2} such strings.

16. We can subtract from the number of strings of length 4 of lower case letters the number of strings of length 4 of lower case letters other than x. Thus the answer is $26^4 - 25^4 = 66{,}351$.

18. Recall that a DNA sequence is a sequence of letters, each of which is one of A, C, G, or T. Thus by the product rule there are $4^5 = 1024$ DNA sequences of length five if we impose no restrictions.

a) If the sequence must end with A, then there are only four positions at which to make a choice, so the answer is $4^4 = 256$.

b) If the sequence must start with T and end with G, then there are only three positions at which to make a choice, so the answer is $4^3 = 64$.

c) If only two letters can be used rather than four, the number of choices is $2^5 = 32$.

d) As in part **(c)**, there are $3^5 = 243$ sequences that do not contain C.

20. Because neither 5 nor 31 is divisible by either 3 or 4, whether the ranges are meant to be inclusive or exclusive of their endpoints is moot.

a) There are $\lfloor 31/3 \rfloor = 10$ integers less than 31 that are divisible by 3, and $\lfloor 5/3 \rfloor = 1$ of them is less than 5 as well. This leaves $10 - 1 = 9$ numbers between 5 and 31 that are divisible by 3. They are 6, 9, 12, 15, 18, 21, 24, 27, and 30.

b) There are $\lfloor 31/4 \rfloor = 7$ integers less than 31 that are divisible by 4, and $\lfloor 5/4 \rfloor = 1$ of them is less than 5 as well. This leaves $7 - 1 = 6$ numbers between 5 and 31 that are divisible by 4. They are 8, 12, 16, 20, 24, and 28.

c) A number is divisible by both 3 and 4 if and only if it is divisible by their least common multiple, which is 12. Obviously there are two such numbers between 5 and 31, namely 12 and 24. We could also work this out as we did in the previous parts: $\lfloor 31/12 \rfloor - \lfloor 5/12 \rfloor = 2 - 0 = 2$. Note also that the intersection of the sets we found in the previous two parts is precisely what we are looking for here.

22. **a)** Every seventh number is divisible by 7. Therefore there are $\lfloor 999/7 \rfloor = 142$ such numbers. Note that we use the floor function, because the k^{th} multiple of 7 does not occur until the number $7k$ has been reached.

b) For solving this part and the next four parts, we need to use the principle of inclusion–exclusion. Just as in part **(a)**, there are $\lfloor 999/11 \rfloor = 90$ numbers in our range divisible by 11, and there are $\lfloor 999/77 \rfloor = 12$ numbers in our range divisible by both 7 and 11 (the multiples of 77 are the numbers we seek). If we take these 12 numbers away from the 142 numbers divisible by 7, we see that there are 130 numbers in our range divisible by 7 but not 11.

c) As explained in part **(b)**, the answer is 12.

d) By the principle of inclusion–exclusion, the answer, using the data from part **(b)**, is $142 + 90 - 12 = 220$.

e) If we subtract from the answer to part **(d)** the number of numbers divisible by both 7 and 11, we will have the number of numbers divisible by neither of them; so the answer is $220 - 12 = 208$.

f) If we subtract the answer to part **(d)** from the total number of positive integers less than 1000, we will have the number of numbers divisible by exactly one of them; so the answer is $999 - 220 = 779$.

g) If we assume that numbers are written without leading 0's, then we should break the problem down into three cases—one-digit numbers, two-digit numbers and three-digit numbers. Clearly there are 9 one-digit numbers, and each of them has distinct digits. There are 90 two-digit numbers (10 through 99), and all but 9 of them have distinct digits, so there are 81 two-digit numbers with distinct digits. An alternative way to compute this is to note that the first digit must be 1 through 9 (9 choices), and the second digit must be something different from the first digit (9 choices out of the 10 possible digits), so by the product rule, we get $9 \cdot 9 = 81$ choices in all. This approach also tells us that there are $9 \cdot 9 \cdot 8 = 648$ three-digit numbers with distinct digits (again, work from left to right—in the ones place, only 8 digits are left to choose from). So the final answer is $9 + 81 + 648 = 738$.

h) It turns out to be easier to count the odd numbers with distinct digits and subtract from our answer to part **(g)**, so let us proceed that way. There are 5 odd one-digit numbers. For two-digit numbers, first choose the ones digit (5 choices), then choose the tens digit (8 choices), since neither the ones digit value nor 0 is available); therefore there are 40 such two-digit numbers. (Note that this is not exactly half of 81.) For the three-digit numbers, first choose the ones digit (5 choices), then the hundreds digit (8 choices), then the tens digit (8 choices, giving us 320 in all. So there are $5 + 40 + 320 = 365$ odd numbers with distinct digits. Thus the final answer is $738 - 365 = 373$.

24. It will be useful to note first that there are exactly 9000 numbers in this range.

a) Every ninth number is divisible by 9, so the answer is one ninth of 9000 or 1000.

b) Every other number is even, so the answer is one half of 9000 or 4500.

c) We can reason from left to right. There are 9 choices for the first (left-most) digit (since it cannot be a 0), then 9 choices for the second digit (since it cannot equal the first digit), then, in a similar way, 8 choices for the third digit, and 7 choices for the right-most digit. Therefore there are $9 \cdot 9 \cdot 8 \cdot 7 = 4536$ ways to specify such a number. In other words, there are 4536 such numbers. Note that this coincidentally turns out to be almost exactly half of the numbers in the range.

d) Every third number is divisible by 3, so one third of 9000 or 3000 numbers in this range are divisible by 3. The remaining 6000 are not.

e) For this and the next three parts we need to note first that one fifth of the numbers in this range, or 1800 of them, are divisible by 5, and one seventh of them, or 1286 are divisible by 7. [This last calculation is a little more subtle than we let on, since 9000 is not divisible by 7 (the quotient is $1285.71\ldots$). But 1001 is divisible by 7, and $1001+1285\cdot 7=9996$, so there are indeed 1286, and not 1285 such multiples. (By contrast, in the range 1002 to 10001, inclusive, which also includes 9000 numbers, there are only 1285 multiples of 7.)] We also need to know how many of these numbers are divisible by both 5 and 7, which means divisible by 35. The answer, by the similar reasoning, is 257, namely those multiples from $29\cdot 35=1015$ to $285\cdot 35=9975$. (One more note: We could also have come up with these numbers more formally, using the ideas in Section 8.5, especially Example 2. We could find the number of multiples less than $10{,}000$ and subtract the number of multiples less than 1000.) Now to the problem at hand. The number of numbers divisible by 5 or 7 is the number of numbers divisible by 5, plus the number of numbers divisible by 7, minus (because of having overcounted) the number of numbers divisible by both. So our answer is $1800+1286-257=2829$.

f) Since we just found that 2829 of these numbers are divisible by either 5 or 7, it follows that the rest of them, $9000-2829=6171$, are not.

g) We noted in the solution to part **(e)** that 1800 numbers are divisible by 5, and 257 of these are also divisible by 7. Therefore $1800-257=1543$ numbers in our range are divisible by 5 but not by 7.

h) We found this as part of our solution to part **(e)**, namely 257.

26. **a)** There are 10 ways to choose the first digit, 9 ways to choose the second, and so on; therefore the answer is $10\cdot 9\cdot 8\cdot 7=5040$.

b) There are 10 ways to choose each of the first three digits and 5 ways to choose the last; therefore the answer is $10^3\cdot 5=5000$.

c) There are 4 ways to choose the position that is to be different from 9, and 9 ways to choose the digit to go there. Therefore there are $4\cdot 9=36$ such strings.

28. $10^3 26^3+26^3 10^3=35{,}152{,}000$

30. $26^3 10^3+26^4 10^2=63{,}273{,}600$

32. **a)** By the product rule, the answer is $26^8=208{,}827{,}064{,}576$.

b) By the product rule, the answer is $26\cdot 25\cdot 24\cdot 23\cdot 22\cdot 21\cdot 20\cdot 19=62{,}990{,}928{,}000$.

c) This is the same as part **(a)**, except that there are only seven slots to fill, so the answer is $26^7=8{,}031{,}810{,}176$.

d) This is similar to **(b)**, except that there is only one choice in the first slot, rather than 26, so the answer is $1\cdot 25\cdot 24\cdot 23\cdot 22\cdot 21\cdot 20\cdot 19=2{,}422{,}728{,}000$.

e) This is the same as part **(c)**, except that there are only six slots to fill, so the answer is $26^6=308{,}915{,}776$.

f) This is the same as part **(e)**; again there are six slots to fill, so the answer is $26^6=308{,}915{,}776$.

g) This is the same as part **(f)**, except that there are only four slots to fill, so the answer is $26^4=456{,}976$. We are assuming that the question means that the legal strings are BO????BO, where any letters can fill the middle four slots.

h) By part **(f)**, there are 26^6 strings that start with the letters BO in that order. By the same argument, there are 26^6 strings that end that way. By part **(g)**, there are 26^4 strings that both start and end with the letters BO in that order. Therefore by the inclusion–exclusion principle, the answer is $26^6+26^6-26^4=617{,}374{,}576$.

34. In each case the answer is n^{10}, where n is the number of elements in the codomain, since there are n choices for a function value for each of the 10 elements in the domain.

a) $2^{10}=1024$ **b)** $3^{10}=59{,}049$ **c)** $4^{10}=1{,}048{,}576$ **d)** $5^{10}=9{,}765{,}625$

36. There are 2^n such functions, since there is a choice of 2 function values for each element of the domain.

38. By our solution to Exercise 39, the answer is $(n+1)^5$ in each case, where n is the number of elements in the codomain.
a) $2^5 = 32$ **b)** $3^5 = 243$ **c)** $6^5 = 7776$ **d)** $10^5 = 100{,}000$

40. We know that there are 2^{100} subsets in all. Clearly 101 of them do not have more than one element, namely the empty set and the 100 sets consisting of 1 element. Therefore the answer is $2^{100} - 101 \approx 1.3 \times 10^{30}$.

42. Recall that a DNA sequence is a sequence of letters, each of which is one of A, C, G, or T. Thus by the product rule there are $4^4 = 256$ DNA sequences of length four if we impose no restrictions.

a) If the letter T cannot be used, then the number of choices is $3^4 = 81$.

b) The sequence must be either ACGx or xACG, where x is one of the four letters. These two cases do not overlap, so the answer is $4 + 4 = 8$.

c) There are four positions and four letters, each used exactly once. There are 4 choices for the first position, then 3 for the second, 2 for the third, and 1 for the fourth. Therefore the answer is $4 \cdot 3 \cdot 2 \cdot 1 = 24$.

d) There are four ways to choose which letter is to be occur twice and three ways to decide which of the other letters to leave out, so there are $4 \cdot 3 = 12$ choices of the letters for the sequence. There are 4 positions the first (alphabetically) of the single-use letters can occupy, and then 3 positions for the second single-use letter, a total of $4 \cdot 3 = 12$ different sequences once we have determined the letters and their frequencies. Therefore the answer is $12 \cdot 12 = 144$.

44. If we ignore the fact that the table is round and just count ordered arrangements of length 4 from the 10 people, then we get $10 \cdot 9 \cdot 8 \cdot 7 = 5040$ arrangements. However, we can rotate the people around the table in 4 ways and get the same seating arrangement, so this overcounts by a factor of 4. (For example, the sequence Mary–Debra–Cristina–Julie gives the same circular seating as the sequence Julie–Mary–Debra–Cristina.) Therefore the answer is $5040/4 = 1260$.

46. **a)** We first place the bride in any of the 6 positions. Then, from left to right in the remaining positions, we choose the other five people to be in the picture; this can be done in $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 15120$ ways. Therefore the answer is $6 \cdot 15120 = 90{,}720$.

b) We first place the bride in any of the 6 positions, and then place the groom in any of the 5 remaining positions. Then, from left to right in the remaining positions, we choose the other four people to be in the picture; this can be done in $8 \cdot 7 \cdot 6 \cdot 5 = 1680$ ways. Therefore the answer is $6 \cdot 5 \cdot 1680 = 50{,}400$.

c) From part **(a)** there are 90720 ways for the bride to be in the picture. There are (from part **(b)**) 50400 ways for both the bride and groom to be in the picture. Therefore there are $90720 - 50400 = 40320$ ways for just the bride to be in the picture. Symmetrically, there are 40320 ways for just the groom to be in the picture. Therefore the answer is $40320 + 40320 = 80{,}640$.

48. There are 2^5 strings that begin with two 0's (since there are two choices for each of the last five bits). Similarly there are 2^4 strings that end with three 1's. Furthermore, there are 2^2 strings that both begin with two 0's and end with three 1's (since only bits 3 and 4 are free to be chosen). By the inclusion–exclusion principle, there are $2^5 + 2^4 - 2^2 = 44$ such strings in all.

50. First we count the number of bit strings of length 10 that contain five consecutive 0's. We will base the count on where the string of five or more consecutive 0's starts. If it starts in the first bit, then the first five bits are all 0's, but there is free choice for the last five bits; therefore there are $2^5 = 32$ such strings. If it starts in the second bit, then the first bit must be a 1, the next five bits are all 0's, but there is free choice for the last four bits; therefore there are $2^4 = 16$ such strings. If it starts in the third bit, then the second bit must be a 1 but the first bit and the last three bits are arbitrary; therefore there are $2^4 = 16$ such strings. Similarly, there are 16 such strings that have the consecutive 0's starting in each of positions four, five, and six. This gives us a total of $32 + 5 \cdot 16 = 112$ strings that contain five consecutive 0's. Symmetrically, there are 112 strings that contain five consecutive 1's. Clearly there are exactly two strings that contain both (0000011111 and 1111100000). Therefore by the inclusion–exclusion principle, the answer is $112 + 112 - 2 = 222$.

52. This is a straightforward application of the inclusion–exclusion principle: $38+23-7 = 54$ (we need to subtract the 7 double majors counted twice in the sum).

54. Order matters here, since the initials RSZ, for example, are different from the initials SRZ. By the sum rule we can add the number of initials formable with two, three, four, and five letters. By the product rule, these are 26^2, 26^3, 26^4, and 26^5, respectively, so the answer is $676 + 17576 + 456976 + 11881376 = 12{,}356{,}604$.

56. We need to compute the number of variable names of length i for $i = 1, 2, \ldots, 8$, and add. A variable name of length i is specified by choosing a first character, which can be done in 53 ways ($2 \cdot 26$ letters and 1 underscore to choose from), and $i - 1$ other characters, each of which can be done in $53 + 10 = 63$ ways. Therefore the answer is

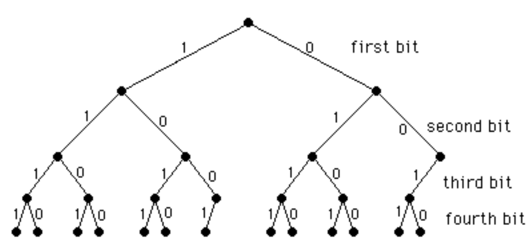
$$\sum_{i=1}^{8} 52 \cdot 63^{i-1} = 52 \cdot \frac{63^8 - 1}{63 - 1} \approx 2.1 \times 10^{14}\,.$$

58. There are $10 - 1 = 9$ country codes of length 1, $10^2 = 100$ of length 2, and $10^3 = 1000$ of length 3, for a total of 1109 country codes. The number of numbers following the country code is $10 + 10^2 + 10^3 + \cdots + 10^{15}$; by the formula for a geometric series (Theorem 1 in Section 2.4), this equals $10(10^{15} - 1)/(10 - 1) = 1{,}111{,}111{,}111{,}111{,}110$. Therefore there are $1109 \cdot 1{,}111{,}111{,}111{,}111{,}110 = 1{,}232{,}222{,}222{,}222{,}220{,}990$ possible numbers.

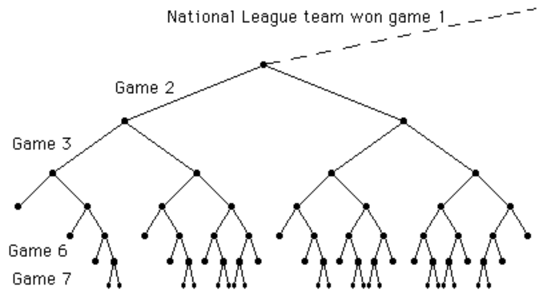
60. By the sum and product rules, the answer is $26^3 + 26^4 + 26^5 + 26^6 = 321{,}271{,}704$.

62. Let P be the set of numbers in $\{1, 2, 3, \ldots, n\}$ that are divisible by p, and similarly define the set Q. We want to count the numbers not divisible by either p or q, so we want $n - |P \cup Q|$. By the principle of inclusion–exclusion, $|P \cup Q| = |P| + |Q| - |P \cap Q|$. Every p^{th} number is divisible by p, so $|P| = \lfloor n/p \rfloor$. Similarly $|Q| = \lfloor n/q \rfloor$. Clearly n is the only positive integer not exceeding n that is divisible by both p and q, so $|P \cap Q| = 1$. Therefore the number of positive integers not exceeding n that are relatively prime to n is $n - (\lfloor n/p \rfloor + \lfloor n/q \rfloor - 1) = n - \lfloor n/p \rfloor - \lfloor n/q \rfloor + 1$.

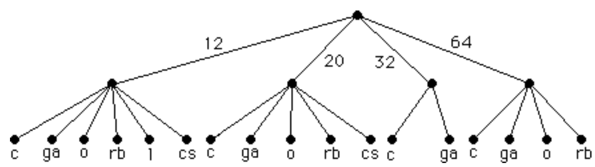
64. We draw the tree, with its root at the top. We show a branch for each of the possibilities 0 and 1, for each bit in order, except that we do not allow three consecutive 0's. Since there are 13 leaves, the answer is 13.



66. The tree is a bit too large to draw in its entirety. We show only half of it, namely the half corresponding to the National League team's having won the first game. By symmetry, the final answer will be twice the number computed with this tree. A branch to the left indicates a win by the National League team; a branch to the right, a win by the American league team. No further branching occurs whenever one team has won four games. Since we see 35 leaves, the answer is 70.



68. **a)** It is more convenient to branch on bottle size first. Note that there are a different number of branches coming off each of the nodes at the second level. The number of leaves in the tree is 17, which is the answer.



b) We can add the number of different varieties for each of the sizes. The 12-ounce bottle has 6, the 20-ounce bottle has 5, the 32-once bottle has 2, and the 64-ounce bottle has 4. Therefore $6+5+2+4=17$ different types of bottles need to be stocked.

70. There are 2^n lines in the truth table, since each of the n propositions can have 2 truth values. Each line can be filled in with T or F, so there are a total of 2^{2^n} possibilities.

72. We want to show that a procedure consisting of m tasks can be done in $n_1n_2\cdots n_m$ ways, if the i^{th} task can be done in n_i ways. The product rule stated in the text is the basis step, $m=2$. Assume the inductive hypothesis. Then to do the procedure we have to do each of the first m tasks, which by the inductive hypothesis can be done in $n_1n_2\cdots n_m$ ways, and then the $(m+1)^{\text{st}}$ task, so there are $(n_1n_2\cdots n_m)n_{m+1}$ possibilities, as desired.

74. **a)** The largest value of TOTAL LENGTH is $2^{16}-1$, since this would be the number represented by a string of 16 1's. So the maximum length of a datagram is 65,535 octets (or bytes).

b) The largest value of HLEN is $2^4-1=15$, since this would be the number represented by a string of four 1's. So the maximum length of a header is 15 32-bit blocks. Since there are four 8-bit octets (or bytes) in a block, the maximum length of the header is $4\cdot 15=60$ octets.

c) We saw in part **(a)** that the maximum total length is 65,535 octets. If at least 20 of these must be devoted to the header, the data area can be at most 65,515 octets long.

d) There are $2^8=256$ different octets, since each bit of an octet can be 0 or 1. In part **(c)** we saw that the data area could be at most 65,515 octets long. So the answer is 256^{65515}, which is a huge number (approximately 7×10^{157775}, according to a computer algebra system).

SECTION 6.2 The Pigeonhole Principle

2. This follows from the pigeonhole principle, with $k = 26$.

4. We assume that the woman does not replace the balls after drawing them.

a) There are two colors: these are the pigeonholes. We want to know the least number of pigeons needed to insure that at least one of the pigeonholes contains three pigeons. By the generalized pigeonhole principle, the answer is 5. If five balls are selected, at least $\lceil 5/2 \rceil = 3$ must have the same color. On the other hand four balls is not enough, because two might be red and two might be blue. Note that the number of balls was irrelevant (assuming that it was at least 5).

b) She needs to select 13 balls in order to insure at least three blue ones. If she does so, then at most 10 of them are red, so at least three are blue. On the other hand, if she selects 12 or fewer balls, then 10 of them could be red, and she might not get her three blue balls. This time the number of balls did matter.

6. There are only d possible remainders when an integer is divided by d, namely 0, 1, $\ldots$, $d-1$. By the pigeonhole principle, if we have $d+1$ remainders, then at least two must be the same.

8. This is just a restatement of the pigeonhole principle, with $k = |T|$.

10. The midpoint of the segment whose endpoints are (a,b) and (c,d) is $((a+c)/2, (b+d)/2)$. We are concerned only with integer values of the original coordinates. Clearly the coordinates of these fractions will be integers as well if and only if a and c have the same parity (both odd or both even) and b and d have the same parity. Thus what matters in this problem is the parities of the coordinates. There are four possible pairs of parities: (odd, odd), $(\text{odd}, \text{even})$, $(\text{even}, \text{odd})$, and $(\text{even}, \text{even})$. Since we are given five points, the pigeonhole principle guarantees that at least two of them will have the same pair of parities. The midpoint of the segment joining these two points will therefore have integer coordinates.

12. This is similar in spirit to Exercise 10. Working modulo 5 there are 25 pairs: $(0,0)$, $(0,1)$, $\ldots$, $(4,4)$. Thus we could have 25 ordered pairs of integers (a,b) such that no two of them were equal when reduced modulo 5. The pigeonhole principle, however, guarantees that if we have 26 such pairs, then at least two of them will have the same coordinates, modulo 5.

14. a) We can group the first ten positive integers into five subsets of two integers each, each subset adding up to 11: $\{1,10\}$, $\{2,9\}$, $\{3,8\}$, $\{4,7\}$, and $\{5,6\}$. If we select seven integers from this set, then by the pigeonhole principle at least two of them come from the same subset. Furthermore, if we forget about these two in the same group, then there are five more integers and four groups; again the pigeonhole principle guarantees two integers in the same group. This gives us two pairs of integers, each pair from the same group. In each case these two integers have a sum of 11, as desired.

b) No. The set $\{1,2,3,4,5,6\}$ has only 5 and 6 from the same group, so the only pair with sum 11 is 5 and 6.

16. We can apply the pigeonhole principle by grouping the numbers cleverly into pairs (subsets) that add up to 16, namely $\{1,15\}$, $\{3,13\}$, $\{5,11\}$, and $\{7,9\}$. If we select five numbers from the set $\{1,3,5,7,9,11,13,15\}$, then at least two of them must fall within the same subset, since there are only four subsets. Two numbers in the same subset are the desired pair that add up to 16. We also need to point out that choosing four numbers is not enough, since we could choose $\{1,3,5,7\}$, and no pair of them add up to more than 12.

18. a) If not, then there would be 4 or fewer male students and 4 or fewer female students, so there would be $4+4=8$ or fewer students in all, contradicting the assumption that there are 9 students in the class.

b) If not, then there would be 2 or fewer male students and 6 or fewer female students, so there would be $2+6=8$ or fewer students in all, contradicting the assumption that there are 9 students in the class.

20. One maximal length increasing sequence is $5, 7, 10, 15, 21$. One maximal length decreasing sequence is $22, 7, 3$. See Exercise 25 for an algorithm.

22. This follows immediately from Theorem 3, with $n = 10$.

24. This problem was on the International Mathematical Olympiad in 2001, a test taken by the six best high school students from each country. Here is a paraphrase of a solution posted on the Web by Steve Olson, author of a book about this competition entitled *Count Down*. Make a table listing the 21 boys at the top of each column and the 21 girls to the left of each row. This table will contain $21 \cdot 21 = 441$ boxes. In each box write the number of a problem solved by both that girl and that boy. From the given information, each box will contain a number. Each contestant solved at most six problems, so only six different numbers can appear in any given row or column of 21 boxes. Because $5 \cdot 2 = 10$, at least $21 - 10 = 11$ of the boxes in any given row or column must contain problem numbers that appear three or more times in that row. (This is an application of the idea of the pigeonhole principle.) In each row color red all the boxes containing problem numbers that appear at least three times in that row. So each row will have at least 11 red boxes, and therefore there will be at least $11 \cdot 21 = 231$ boxes colored red. Repeat the process with the columns, using the color blue. Because at least 231 boxes are red and 231 are blue, and there are only 441 boxes in all, some of the boxes will be both red and blue. (Here is the second place where the pigeonhole principle is used.) The problem number in a doubly-colored box represents a problem solved by at least three girls and at least three boys.

26. Let the people be A, B, C, D, and E. Suppose the following pairs are friends: $A{-}B$, $B{-}C$, $C{-}D$, $D{-}E$, and $E{-}A$. The other five pairs are enemies. In this example, there are no three mutual friends and no three mutual enemies.

28. Let A be one of the people. She must have either 10 friends or 10 enemies, since if there were 9 or fewer of each, then that would account for at most 18 of the 19 other people. Without loss of generality assume that A has 10 friends. By Exercise 27 there are either 4 mutual enemies among these 10 people, or 3 mutual friends. In the former case we have our desired set of 4 mutual enemies; in the latter case, these 3 people together with A form the desired set of 4 mutual friends.

30. This is clear by symmetry, since we can just interchange the notions of friends and enemies.

32. There are 99,999,999 possible positive salaries less than one million dollars, i.e., from \$0.01 to \$999,999.99. By the pigeonhole principle, if there were more than this many people with positive salaries less than one million dollars, then at least two of them must have the same salary.

34. This follows immediately from Theorem 2, with $N = 8{,}008{,}278$ and $k = 1{,}000{,}001$ (the number of hairs can be anywhere from 0 to a million).

36. Let $K(x)$ be the number of other computers that computer x is connected to. The possible values for $K(x)$ are $1, 2, 3, 4, 5$. Since there are 6 computers, the pigeonhole principle guarantees that at least two of the values $K(x)$ are the same, which is what we wanted to prove.

38. This is similar to Example 9. Label the computers C_1 through C_8, and label the printers P_1 through P_4. If we connect C_k to P_k for $k = 1, 2, 3, 4$ and connect each of the computers C_5 through C_8 to *all* the printers, then we have used a total of $4 + 4 \cdot 4 = 20$ cables. Clearly this is sufficient, because if computers C_1 through C_4 need printers, then they can use the printers with the same subscripts, and if any computers with higher subscripts need a printer instead of one or more of these, then they can use the printers that are not being used, since they are connected to all the printers. Now we must show that 19 cables are not enough. Since there are 19 cables and 4 printers, the average number of computers per printer is $19/4$, which is less than 5. Therefore some printer must be connected to fewer than 5 computers (the average of a set of numbers cannot be bigger than each of the numbers in the set). That means it is connected to 4 or fewer computers, so there are at least 4 computers that are not connected to it. If those 4 computers all needed a printer simultaneously, then they would be out of luck, since they are connected to at most the 3 other printers.

40. Let $K(x)$ be the number of other people at the party that person x knows. The possible values for $K(x)$ are $0, 1, \ldots, n-1$, where $n \geq 2$ is the number of people at the party. We cannot apply the pigeonhole principle directly, since there are n pigeons and n pigeonholes. However, it is impossible for both 0 and $n-1$ to be in the range of K, since if one person knows everybody else, then nobody can know no one else (we assume that "knowing" is symmetric). Therefore the range of K has at most $n-1$ elements, whereas the domain has n elements, so K is not one-to-one, precisely what we wanted to prove.

42. **a)** The solution of Exercise 41, with 24 replaced by 2 and 149 replaced by 127, tells us that the statement is true.

b) The solution of Exercise 41, with 24 replaced by 23 and 149 replaced by 148, tells us that the statement is true.

c) We begin in a manner similar to the solution of Exercise 41. Look at a_1, a_2, ..., a_{75}, a_1+25, ..., $a_{75}+25$, where a_i is the total number of matches played up through and including hour i. Then $1 \leq a_1 < a_2 < \cdots < a_{75} \leq 125$, and $26 \leq a_1 + 25 < a_2 + 25 < \cdots < a_{75} + 25 \leq 150$. Now either these 150 numbers are precisely all the number from 1 to 150, or else by the pigeonhole principle we get, as in Exercise 41, $a_i = a_j + 25$ for some i and j and we are done. In the former case, however, since each of the numbers $a_i + 25$ is greater than or equal to 26, the numbers $1, 2, \ldots, 25$ must all appear among the a_i's. But since the a_i's are increasing, the only way this can happen is if $a_1 = 1$, $a_2 = 2$, ..., $a_{25} = 25$. Thus there were exactly 25 matches in the first 25 hours.

d) We need a different approach for this part, an approach, incidentally, that works for many numbers besides 30 in this setting. Let a_1, a_2, ..., a_{75} be as before, and note that $1 \leq a_1 < a_2 < \cdots < a_{75} \leq 125$. By the pigeonhole principle two of the numbers among a_1, a_2, ..., a_{31} are congruent modulo 30. If they differ by 30, then we have our solution. Otherwise they differ by 60 or more, so $a_{31} \geq 61$. Similarly, among a_{31} through a_{61}, either we find a solution, or two numbers must differ by 60 or more; therefore we can assume that $a_{61} \geq 121$. But this means that $a_{66} \geq 126$, a contradiction.

44. Look at the pigeonholes $\{1000, 1001\}$, $\{1002, 1003\}$, $\{1004, 1005\}$, ..., $\{1098, 1099\}$. There are clearly 50 sets in this list. By the pigeonhole principle, if we have 51 numbers in the range from 1000 to 1099 inclusive, then at least two of them must come from the same set. These are the desired two consecutive house numbers.

46. Suppose this statement were not true. Then for each i, the i^{th} box contains at most $n_i - 1$ objects. Adding, we have at most $(n_1 - 1) + (n_2 - 1) + \cdots + (n_t - 1) = n_1 + n_2 + \cdots + n_t - t$ objects in all, contradicting the fact that there were $n_1 + n_2 + \cdots + n_t - t + 1$ objects in all. Therefore the statement must be true.

SECTION 6.3 Permutations and Combinations

2. $P(7,7) = 7! = 5040$

4. There are 10 combinations and 60 permutations. We list them in the following way. Each combination is listed, without punctuation, in increasing order, followed by the five other permutations involving the same numbers, in parentheses, without punctuation.

123 (132 213 231 312 321) 124 (142 214 241 412 421) 125 (152 215 251 512 521)
134 (143 314 341 413 431) 135 (153 315 351 513 531) 145 (154 415 451 514 541)
234 (243 324 342 423 432) 235 (253 325 352 523 532)
245 (254 425 452 524 542) 345 (354 435 453 534 543)

6. **a)** $C(5,1) = 5$ **b)** $C(5,3) = C(5,2) = 5 \cdot 4/2 = 10$ **c)** $C(8,4) = 8 \cdot 7 \cdot 6 \cdot 5/(4 \cdot 3 \cdot 2) = 70$
d) $C(8,8) = 1$ **e)** $C(8,0) = 1$ **f)** $C(12,6) = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7/(6 \cdot 5 \cdot 4 \cdot 3 \cdot 2) = 924$

8. $P(5,5) = 5! = 120$

10. $P(6,6) = 6! = 720$

12. **a)** To specify a bit string of length 12 that contains exactly three 1's, we simply need to choose the three positions that contain the 1's. There are $C(12,3) = 220$ ways to do that.

b) To contain at most three 1's means to contain three 1's, two 1's, one 1, or no 1's. Reasoning as in part **(a)**, we see that there are $C(12,3)+C(12,2)+C(12,1)+C(12,0) = 220+66+12+1 = 299$ such strings.

c) To contain at least three 1's means to contain three 1's, four 1's, five 1's, six 1's, seven 1's, eight 1's, nine 1's, 10 1's, 11 1's, or 12 1's. We could reason as in part **(b)**, but we would have too many numbers to add. A simpler approach would be to figure out the number of ways not to have at least three 1's (i.e., to have two 1's, one 1, or no 1's) and then subtract that from 2^{12}, the total number of bit strings of length 12. This way we get $4096 - (66 + 12 + 1) = 4017$.

d) To have an equal number of 0's and 1's in this case means to have six 1's. Therefore the answer is $C(12,6) = 924$.

14. $C(99,2) = 99 \cdot 98/2 = 4851$

16. We need to compute $C(10,1) + C(10,3) + C(10,5) + C(10,7) + C(10,9) = 10 + 120 + 252 + 120 + 10 = 512$. (In the next section we will see that there are just as many subsets with an odd number of elements as there are subsets with an even number of elements (Exercise 31 in Section 6.4). Since there are $2^{10} = 1024$ subsets in all, the answer is $1024/2 = 512$, in agreement with our computation.)

18. **a)** Each flip can be either heads or tails, so there are $2^8 = 256$ possible outcomes.

b) To specify an outcome that has exactly three heads, we simply need to choose the three flips that came up heads. There are $C(8,3) = 56$ such outcomes.

c) To contain at least three heads means to contain three heads, four heads, five heads, six heads, seven heads, or eight heads. Reasoning as in part **(b)**, we see that there are $C(8,3)+C(8,4)+C(8,5)+C(8,6)+C(8,7)+C(8,8) = 56 + 70 + 56 + 28 + 8 + 1 = 219$ such outcomes. We could also subtract from 256 the number of ways to get two or fewer heads, namely $28 + 8 + 1 = 37$. Since $256 - 37 = 219$, we obtain the same answer using this alternative method.

d) To have an equal number of heads and tails in this case means to have four heads. Therefore the answer is $C(8,4) = 70$.

20. **a)** There are $C(10,3)$ ways to choose the positions for the 0's, and that is the only choice to be made, so the answer is $C(10,3) = 120$.

b) There are more 0's than 1's if there are fewer than five 1's. Using the same reasoning as in part **(a)**, together with the sum rule, we obtain the answer $C(10,0) + C(10,1) + C(10,2) + C(10,3) + C(10,4) = 1 + 10 + 45 + 120 + 210 = 386$. Alternatively, by symmetry, half of all cases in which there are not five 0's have more 0's than 1's; therefore the answer is $(2^{10} - C(10,5)/2 = (1024 - 252)/2 = 386$.

c) We want the number of bit strings with 7, 8, 9, or 10 1's. By the same reasoning as above, there are $C(10,7) + C(10,8) + C(10,9) + C(10,10) = 120 + 45 + 10 + 1 = 176$ such strings.

d) If a string does not have at least three 1's, then it has 0, 1, or 2 1's. There are $C(10,0) + C(10,1) + C(10,2) = 1 + 10 + 45 = 56$ such strings. There are $2^{10} = 1024$ strings in all. Therefore there are $1024 - 56 = 968$ strings with at least three 1's.

22. **a)** If ED is to be a substring, then we can think of that block of letters as one superletter, and the problem is to count permutations of seven items—the letters A, B, C, F, G, and H, and the superletter ED. Therefore the answer is $P(7,7) = 7! = 5040$.

b) Reasoning as in part **(a)**, we see that the answer is $P(6,6) = 6! = 720$.

c) As in part **(a)**, we glue BA into one item and glue FGH into one item. Therefore we need to permute five items, and there are $P(5,5) = 5! = 120$ ways to do it.

d) This is similar to part **(c)**. Glue AB into one item, glue DE into one item, and glue GH into one item, producing five items, so the answer is $P(5,5) = 5! = 120$.

e) If both CAB and BED are substrings, then $CABED$ has to be a substring. So we are really just permuting four items: $CABED$, F, G, and H. Therefore the answer is $P(4,4) = 4! = 24$.

f) There are no permutations with both of these substrings, since B cannot be followed by both C and F at the same time.

24. First position the women relative to each other. Since there are 10 women, there are $P(10,10)$ ways to do this. This creates 11 slots where a man (but not more than one man) may stand: in front of the first woman, between the first and second women, $\ldots$, between the ninth and tenth women, and behind the tenth woman. We need to choose six of these positions, in order, for the first through six man to occupy (order matters, because the men are distinct people). This can be done is $P(11,6)$ ways. Therefore the answer is $P(10,10) \cdot P(11,6) = 10! \cdot 11!/5! = 1{,}207{,}084{,}032{,}000$.

26. **a)** This is just a matter of choosing 10 players from the group of 13, since we are not told to worry about what positions they play; therefore the answer is $C(13,10) = 286$.

b) This is the same as part **(a)**, except that we need to worry about the order in which the choices are made, since there are 10 distinct positions to be filled. Therefore the answer is $P(13,10) = 13!/3! = 1{,}037{,}836{,}800$.

c) There is only one way to choose the 10 players without choosing a woman, since there are exactly 10 men. Therefore (using part **(a)**) there are $286 - 1 = 285$ ways to choose the players if at least one of them must be a woman.

28. We are just being asked for the number of strings of T's and F's of length 40 with exactly 17 T's. The only choice is which 17 of the 40 positions are to have the T's, so the answer is $C(40,17) \approx 8.9 \times 10^{10}$.

30. **a)** There are $C(16,5)$ ways to select a committee if there are no restrictions. There are $C(9,5)$ ways to select a committee from just the 9 men. Therefore there are $C(16,5) - C(9,5) = 4368 - 126 = 4242$ committees with at least one woman.

b) There are $C(16,5)$ ways to select a committee if there are no restrictions. There are $C(9,5)$ ways to select a committee from just the 9 men. There are $C(7,5)$ ways to select a committee from just the 7 men. These two possibilities do not overlap, since there are no ways to select a committee containing neither men nor women. Therefore there are $C(16,5) - C(9,5) - C(7,5) = 4368 - 126 - 21 = 4221$ committees with at least one woman and at least one man.

32. **a)** The only reasonable way to do this is by subtracting from the number of strings with no restrictions the number of strings that do not contain the letter a. The answer is $26^6 - 25^6 = 308915776 - 244140625 =$ 64,775,151.

b) If our string is to contain both of these letters, then we need to subtract from the total number of strings the number that fail to contain one or the other (or both) of these letters. As in part **(a)**, 25^6 strings fail to contain an a; similarly 25^6 fail to contain a b. This is overcounting, however, since 24^6 fail to contain both of these letters. Therefore there are $25^6 + 25^6 - 24^6$ strings that fail to contain at least one of these letters. Therefore the answer is $26^6 - (25^6 + 25^6 - 24^6) = 308915776 - (244140625 + 244140625 - 191102976) = 11{,}737{,}502$.

c) First choose the position for the a; this can be done in 5 ways, since the b must follow it. There are four remaining positions, and these can be filled in $P(24,4)$ ways, since there are 24 letters left (no repetitions being allowed this time). Therefore the answer is $5P(24,4) = 1{,}275{,}120$.

d) First choose the positions for the a and b; this can be done in $C(6,2)$ ways, since once we pick two positions, we put the a in the left-most and the b in the other. There are four remaining positions, and these can be filled in $P(24,4)$ ways, since there are 24 letters left (no repetitions being allowed this time). Therefore the answer is $C(6,2)P(24,4) = 3{,}825{,}360$.

34. Probably the best way to do this is just to break it down into the three cases by sex. There are $C(15,6)$ ways to choose the committee to be composed only of women, $C(15,5)C(10,1)$ ways if there are to be five women and one man, and $C(15,4)C(10,2)$ ways if there are to be four women and two men. Therefore the answer is $C(15,6) + C(15,5)C(10,1) + C(15,4)C(10,2) = 5005 + 30030 + 61425 = 96{,}460$.

36. Glue two 1's to the right of each 0, giving us a collection of nine tokens: five 011's and four 1's. We are asked for the number of strings consisting of these tokens. All that is involved is choosing the positions for the 1's among the nine positions in the string, so the answer is $C(9,4) = 126$.

38. $C(45,3) \cdot C(57,4) \cdot C(69,5) = 14190 \cdot 395010 \cdot 11238513 \approx 6.3 \times 10^{16}$

40. By the reasoning given in the solution to Exercise 41, the answer is $5!/(3 \cdot (5-3))! = 20$.

42. The only difference between this problem and the problem solved in Exercise 41 is a factor of 2. Each seating under the rules here corresponds to two seatings under the original rules, because we can change the order of people around the table from clockwise to counterclockwise. Therefore we need to divide the formula there by 2, giving us $n!/(2r(n-r)!)$. This assumes that $r \geq 3$. If $r = 1$ then the problem is trivial (there are n choices under both sets of rules). If $r = 2$, then we do not introduce the extra factor of 2, because clockwise order and counterclockwise order are the same. In this case, both answers are just $n!/(2(n-2)!)$, which is $C(n,2)$, as one would expect.

44. We can solve this problem by breaking it down into cases depending on the number of ties. There are five cases. (1) If there are no ties, then there are clearly $P(4,4) = 24$ possible ways for the horses to finish. (2) Assume that there are two horses that tie, but the others have distinct finishes. There are $C(4,2) = 6$ ways to choose the horses to be tied; then there are $P(3,3) = 6$ ways to determine the order of finish for the three groups (the pair and the two single horses). Thus there are $6 \cdot 6 = 36$ ways for this to happen. (3) There might be two groups of two horses that are tied. There are $C(4,2) = 6$ ways to choose the winners (and the other two horses are the losers). (4) There might be a group of three horses all tied. There are $C(4,3) = 4$

ways to choose which these horses will be, and then two ways for the race to end (the tied horses win or they lose), so there are $4 \cdot 2 = 8$ possibilities. (5) There is only one way for all the horses to tie. Putting this all together, the answer is $24 + 36 + 6 + 8 + 1 = 75$.

46. a) The complicating factor here is the rule that the penalty kick round (or "group") is over once one team has clinched a victory. For example, if the first team to shoot has missed all of its first four shots and the other team has made two of its first three shots, then the round is over after only seven kicks. There are $2^{10} = 1024$ possible scenarios without this rule (and without worrying yet about whether the score is tied at the end of this round), but it seems rather tedious and dangerous (in the sense of your being likely to make a mistake and leave something out) to try to analyze the more complicated situation by writing out all the possibilities by hand. (This is not impossible, though, and the author has obtained the correct answer in this way.) Rather than do this, one can write a computer program to simulate the situation and do the counting. The result is that there are 672 possible scoring scenarios for a round of penalty kicks, including the possibility that the score is still tied at the end of that round.

Next we need to count the number of ways for the score to end up tied at the end of the round. For this to happen, both teams must score p points, where p is some integer between 0 and 5, inclusive. The scoring scenario is determined by the positions of the kickers who did the scoring. There are $C(5,p)$ ways to choose these positions for each team, or $C(5,p)^2$ ways in all. We need to sum this over the values of p from 0 to 5. The sum is 252. So there are 252 ways for the score to end up tied. We already noted in the paragraph above that there are 672 different scoring scenarios, so there are $672 - 252 = 420$ scenarios in which the score is not tied. This answers the question for this part of the exercise.

b) This is easy after what we've found above. There are 252 ways for the score to be tied at the end of the first group of penalty kicks, and there are 420 ways for the game to be settled in the second group. So there are $252 \cdot 420 = 105{,}840$ ways for the game to end during the second round.

c) We have already seen that there are 420 ways for the game to end in the first round, and $105{,}840$ more ways for it to end in the second round. In order for it to go into a sudden death period, the first two rounds must have ended tied, which can happen in $420 \cdot 420 = 176{,}400$ ways. Thereafter, the game can end after two more kicks in 2 ways (either team can make their kick and have the other team miss theirs), after four more kicks in $2 \cdot 2 = 4$ ways (the first pair of kicks must have the same result, either both made or both missed, and then either team can win), after six more kicks in $2^2 \cdot 2 = 8$ ways (the first two pairs of kicks must have the same results, and then either team can win), after eight more kicks in 16 ways, and after ten more kicks in 32 ways. Thus there are $2+4+8+16+32 = 62$ ways for the sudden death round to end within ten kicks. This needs to be multiplied by the $176{,}400$ ways we can reach sudden death, for a total of $10{,}936{,}800$ scoring scenarios. So the answer to this last question is $420 + 105840 + 10936800 = 11{,}043{,}060$.

SECTION 6.4 Binomial Coefficients

2. a) When $(x+y)^5 = (x+y)(x+y)(x+y)(x+y)(x+y)$ is expanded, all products of a term in the first sum, a term in the second sum, a term in the third sum, a term in the fourth sum, and a term in the fifth sum are added. Terms of the form x^5, x^4y, x^3y^2, x^2y^3, xy^4 and y^5 arise. To obtain a term of the form x^5, an x must be chosen in each of the sums, and this can be done in only one way. Thus, the x^5 term in the product has a coefficient of 1. (We can think of this coefficient as $\binom{5}{5}$.) To obtain a term of the form x^4y, an x must be chosen in four of the five sums (and consequently a y in the other sum). Hence, the number of such terms is the number of 4-combinations of five objects, namely $\binom{5}{4} = 5$. Similarly, the number of terms of the form x^3y^2 is the number of ways to pick three of the five sums to obtain x's (and consequently take a y from each of the other two factors). This can be done in $\binom{5}{3} = 10$ ways. By the same reasoning there are $\binom{5}{2} = 10$ ways to obtain the x^2y^3 terms, $\binom{5}{1} = 5$ ways to obtain the xy^4 terms, and only one way (which we can think of as $\binom{5}{0}$) to obtain a y^5 term. Consequently, the product is $x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$.

b) This is explained in Example 2. The expansion is $\binom{5}{0}x^5 + \binom{5}{1}x^4y + \binom{5}{2}x^3y^2 + \binom{5}{3}x^2y^3 + \binom{5}{4}xy^4 + \binom{5}{5}y^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$. Note that it does not matter whether we think of the bottom of the binomial coefficient expression as corresponding to the exponent on x, as we did in part **(a)**, or the exponent on y, as we do here.

4. $\binom{13}{8} = 1287$

6. $\binom{11}{7}1^4 = 330$

8. $\binom{17}{9}3^8 2^9 = 24310 \cdot 6561 \cdot 512 = 81{,}662{,}929{,}920$

10. By the binomial theorem, the typical term in this expansion is $\binom{100}{j}x^{100-j}(1/x)^j$, which can be rewritten as $\binom{100}{j}x^{100-2j}$. As j runs from 0 to 100, the exponent runs from 100 down to -100 in decrements of 2. If we let k denote the exponent, then solving $k = 100 - 2j$ for j we obtain $j = (100-k)/2$. Thus the values of k for which x^k appears in this expansion are $-100,\ -98,\ \ldots,\ -2,\ 0,\ 2,\ 4,\ \ldots,\ 100$, and for such values of k the coefficient is $\binom{100}{(100-k)/2}$.

12. We just add adjacent numbers in this row to obtain the next row (starting and ending with 1, of course):

$$1 \quad 11 \quad 55 \quad 165 \quad 330 \quad 462 \quad 462 \quad 330 \quad 165 \quad 55 \quad 11 \quad 1$$

14. Using the factorial formulae for computing binomial coefficients, we see that $\binom{n}{k-1} = \frac{k}{n-k+1}\binom{n}{k}$. If $k \le n/2$, then $\frac{k}{n-k+1} < 1$, so the "less than" signs are correct. Similarly, if $k > n/2$, then $\frac{k}{n-k+1} > 1$, so the "greater than" signs are correct. The middle equality is Corollary 2 in Section 6.3, since $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$. The equalities at the ends are clear.

16. a) By Exercise 14, we know that $\binom{n}{\lfloor n/2 \rfloor}$ is the largest of the $n-1$ binomial coefficients $\binom{n}{1}$ through $\binom{n}{n-1}$. Therefore it is at least as large as their average, which is $(2^n - 2)/(n-1)$. But since $2n \le 2^n$ for $n \ge 2$, it follows that $(2^n - 2)/(n-1) \ge 2^n/n$, and the proof is complete.

b) This follows from part **(a)** by replacing n with $2n$ when $n \ge 2$, and it is immediate when $n = 1$.

18. The numeral 11 in base b represents the number $b+1$. Therefore the fourth power of this number is $b^4 + 4b^3 + 6b^2 + 4b + 1$, where the binomial coefficients can be read from Pascal's triangle. As long as $b \ge 7$, these coefficients are single digit numbers in base b, so this is the meaning of the numeral $(14641)_b$. In short, the numeral formed by concatenating the symbols in the fourth row of Pascal's triangle is the answer.

20. It is easy to see that both sides equal

$$\frac{(n-1)!n!(n+1)!}{(k-1)!k!(k+1)!(n-k-1)!(n-k)!(n-k+1)!}.$$

22. a) Suppose that we have a set with n elements, and we wish to choose a subset A with k elements and another, disjoint, subset with $r-k$ elements. The left-hand side gives us the number of ways to do this, namely the product of the number of ways to choose the r elements that are to go into one or the other of the subsets and the number of ways to choose which of *these* elements are to go into the first of the subsets. The right-hand side gives us the number of ways to do this as well, namely the product of the number of ways to choose the first subset and the number of ways to choose the second subset from the elements that remain.

b) On the one hand,

$$\binom{n}{r}\binom{r}{k} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!}{k!(n-r)!(r-k)!},$$

and on the other hand

$$\binom{n}{k}\binom{n-k}{r-k} = \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(r-k)!(n-r)!} = \frac{n!}{k!(n-r)!(r-k)!}.$$

24. We know that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Clearly p divides the numerator. On the other hand, p cannot divide the denominator, since the prime factorizations of these factorials contains only numbers less than p. Therefore the factor p does not cancel when this fraction is reduced to lowest terms (i.e., to a whole number), so p divides $\binom{p}{k}$.

26. First, use Exercise 25 to rewrite the right-hand side of this identity as $\binom{2n}{n+1}$. We give a combinatorial proof, showing that both sides count the number of ways to choose from collection of n men and n women, a subset that has one more man than woman. For the left-hand side, we note that this subset must have k men and $k-1$ women for some k between 1 and n, inclusive. For the (modified) right-hand side, choose any set of $n+1$ people from this collection of n men and n women; the desired subset is the set of men chosen and the women left behind.

28. **a)** To choose 2 people from a set of n men and n women, we can either choose 2 men ($\binom{n}{2}$ ways to do so) or 2 women ($\binom{n}{2}$ ways to do so) or one of each sex ($n \cdot n$ ways to do so). Therefore the right-hand side counts the number of ways to do this (by the sum rule). The left-hand side counts the same thing, since we are simply choosing 2 people from $2n$ people.

b) $2\binom{n}{2} + n^2 = n(n-1) + n^2 = 2n^2 - n = n(2n-1) = 2n(2n-1)/2 = \binom{2n}{2}$

30. We follow the hint. The number of ways to choose this committee is the number of ways to choose the chairman from among the n mathematicians (n ways) times the number of ways to choose the other $n-1$ members of the committee from among the other $2n-1$ professors. This gives us $n\binom{2n-1}{n-1}$, the expression on the right-hand side. On the other hand, for each k from 1 to n, we can have our committee consist of k mathematicians and $n-k$ computer scientists. There are $\binom{n}{k}$ ways to choose the mathematicians, k ways to choose the chairman from among these, and $\binom{n}{n-k}$ ways to choose the computer scientists. Since this last quantity equals $\binom{n}{k}$, we obtain the expression on the left-hand side of the identity.

32. For $n = 0$ we want

$$(x+y)^0 = \sum_{j=0}^{0} \binom{0}{j} x^{0-j} y^j = \binom{0}{0} x^0 y^0,$$

which is true, since $1 = 1$. Assume the inductive hypothesis. Then we have

$$\begin{aligned}(x+y)^{n+1} &= (x+y)\sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j \\ &= \sum_{j=0}^{n}\binom{n}{j}x^{n+1-j}y^j + \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^{j+1}\end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^{n+1} \binom{n}{k-1} x^{n+1-k} y^k \\
&= \binom{n}{0} x^{n+1} + \left(\sum_{k=1}^{n} [\binom{n}{k} + \binom{n}{k-1}] x^{n+1-k} y^k \right) + \binom{n}{n} y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k ,
\end{aligned}$$

as desired. The key point was the use of Pascal's identity to simplify the expression in brackets in the fourth line of this calculation.

34. By Exercise 33 there are $\binom{n-k+k}{k} = \binom{n}{k}$ paths from $(0,0)$ to $(n-k,k)$ and $\binom{k+n-k}{n-k} = \binom{n}{n-k}$ paths from $(0,0)$ to $(k,n-k)$. By symmetry, these two quantities must be the same (flip the picture around the 45° line).

36. A path ending up at $(n+1-k,k)$ must have made its last step either upward or to the right. If the last step was made upward, then it came from $(n+1-k,k-1)$; if it was made to the right, then it came from $(n-k,k)$. The path cannot have passed through both of these points. Therefore the number of paths to $(n+1-k,k)$ is the sum of the number of paths to $(n+1-k,k-1)$ and the number of paths to $(n-k,k)$. By Exercise 33 this tells us that $\binom{n+1-k+k}{k} = \binom{n+1-k+k-1}{k-1} + \binom{n-k+k}{k}$, which simplifies to $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, Pascal's identity.

38. We follow the hint, first noting that we can start the summation with $k=1$, since the term with $k=0$ is 0. The left-hand side counts the number of ways to choose a subset as described in the hint by breaking it down by the number of elements in the subset; note that there are k ways to choose each of the distinguished elements if the subset has size k. For the right-hand side, first note that $n(n+1)2^{n-2} = n(n-1+2)2^{n-2} = n(n-1)2^{n-2} + n2^{n-1}$. The first term counts the number of ways to make this choice if the two distinguished elements are different (choose them, then choose any subset of the remaining elements to be the rest of the subset). The second term counts the number of ways to make this choice if the two distinguished elements are the same (choose it, then choose any subset of the remaining elements to be the rest of the subset). Note that this works even if $n=1$.

SECTION 6.5 Generalized Permutations and Combinations

2. There are 5 choices each of 5 times, so the answer is $5^5 = 3125$.

4. There are 6 choices each of 7 times, so the answer is $6^7 = 279{,}936$.

6. By Theorem 2 the answer is $C(3+5-1,5) = C(7,5) = C(7,2) = 21$.

8. By Theorem 2 the answer is $C(21+12-1,12) = C(32,12) = 225{,}792{,}840$.

10. **a)** $C(6+12-1, 12) = C(17, 12) = 6188$ **b)** $C(6+36-1, 36) = C(41, 36) = 749{,}398$

c) If we first pick the two of each kind, then we have picked $2 \cdot 6 = 12$ croissants. This leaves one dozen left to pick without restriction, so the answer is the same as in part **(a)**, namely $C(6+12-1, 12) = C(17, 12) = 6188$.

d) We first compute the number of ways to violate the restriction, by choosing at least three broccoli croissants. This can be done in $C(6+21-1, 21) = C(26, 21) = 65780$ ways, since once we have picked the three broccoli croissants there are 21 left to pick without restriction. Since there are $C(6+24-1, 24) = C(29, 24) = 118755$ ways to pick 24 croissants without any restriction, there must be $118755 - 65780 = 52{,}975$ ways to choose two dozen croissants with no more than two broccoli.

e) Eight croissants are specified, so this problem is the same as choosing $24 - 8 = 16$ croissants without restriction, which can be done in $C(6+16-1, 16) = C(21, 16) = 20{,}349$ ways.

f) First let us include all the lower bound restrictions. If we choose the required 9 croissants, then there are $24 - 9 = 15$ left to choose, and if there were no restriction on the broccoli croissants then there would be $C(6+15-1, 15) = C(20, 15) = 15504$ ways to make the selections. If in addition we were to violate the broccoli restriction by choosing at least four broccoli croissants, there would be $C(6+11-1, 11) = C(16, 11) = 4368$ choices. Therefore the number of ways to make the selection without violating the restriction is $15504 - 4368 - 11{,}136$.

12. There are 5 things to choose from, repetitions allowed, and we want to choose 20 things, order not important. Therefore by Theorem 2 the answer is $C(5+20-1, 20) = C(24, 20) = C(24, 4) = 10{,}626$.

14. By Theorem 2 the answer is $C(4+17-1, 17) = C(20, 17) = C(20, 3) = 1140$.

16. **a)** We require each $x_i \geq 2$. This uses up 12 of the 29 total required, so the problem is the same as finding the number of solutions to $x_1' + x_2' + x_3' + x_4' + x_5' + x_6' = 17$ with each x_i' a nonnegative integer. The number of solutions is therefore $C(6+17-1, 17) = C(22, 17) = 26{,}334$.

b) The restrictions use up 22 of the total, leaving a free total of 7. Therefore the answer is $C(6+7-1, 7) = C(12, 7) = 792$.

c) The number of solutions without restriction is $C(6+29-1, 29) = C(34, 29) = 278256$. The number of solution violating the restriction by having $x_1 \geq 6$ is $C(6+23-1, 23) = C(28, 23) = 98280$. Therefore the answer is $278256 - 98280 = 179{,}976$.

d) The number of solutions with $x_2 \geq 9$ (as required) but without the restriction on x_1 is $C(6+20-1, 20) = C(25, 20) = 53130$. The number of solution violating the additional restriction by having $x_1 \geq 8$ is $C(6+12-1, 12) = C(17, 12) = 6188$. Therefore the answer is $53130 - 6188 = 46{,}942$.

18. It follows directly from Theorem 3 that the answer is

$$\frac{20!}{2!4!3!1!2!3!2!3!} \approx 5.9 \times 10^{13}.$$

20. We introduce the nonnegative slack variable x_4, and our problem becomes the same as the problem of counting the number of nonnegative integer solutions to $x_1 + x_2 + x_3 + x_4 = 11$. By Theorem 2 the answer is $C(4+11-1, 11) = C(14, 11) = C(14, 3) = 364$.

22. If we think of the balls as doing the choosing, then this is asking for the number of ways to choose 12 bins from the six given bins, with repetition allowed. (The number of times each bin is chosen is the number of balls in that bin.) By Theorem 2 with $n = 6$ and $r = 12$, this choice can be made in $C(6+12-1, 12) = C(17, 12) = 6188$ ways.

24. We assume that this problem leaves us free to pick which boxes get which numbers of balls. There are several ways to count this. Here is one. Line up the 15 objects in a row ($15!$ ways to do that), and line up the five boxes in a row ($5!$ ways to do that). Now put the first object into the first box, the next two into the second box, the next three into the third box, and so on. This overcounts by a factor of $1!\cdot 2!\cdot 3!\cdot 4!\cdot 5!$, since there are that many ways to swap objects in the permutation without affecting the result. Therefore the answer is $15!\cdot 5!/(1!\cdot 2!\cdot 3!\cdot 4!\cdot 5!) = 4{,}540{,}536{,}000$.

26. We can model this problem by letting x_i be the i^{th} digit of the number for $i = 1,2,3,4,5,6$, and asking for the number of solutions to the equation $x_1+x_2+x_3+x_4+x_5+x_6 = 13$, where each x_i is between 0 and 8, inclusive, except that one of them equals 9. First, there are 6 ways to decide which of the digits is 9. Without loss of generality assume that $x_6 = 9$. Then the number of ways to choose the remaining digits is the number of nonnegative integer solutions to $x_1+x_2+x_3+x_4+x_5 = 4$ (note that the restriction that each $x_i \le 8$ was moot, since the sum was only 4). By Theorem 2 there are $C(5+4-1,4) = C(8,4) = 70$ solutions. Therefore the answer is $6\cdot 70 = 420$.

28. (Note that the roles of the letters n and r here are reversed from the usual roles, as, for example, in Theorem 2.) We can choose the required objects first, and there are $q_1+q_2+\cdots+q_r$ of these. Then $n-(q_1+q_2+\cdots+q_r) = n-q_1-q_2-\cdots-q_r$ objects remain to be chosen. There are still r types. Therefore by Theorem 2, the number of ways to make this choice is $C(r+(n-q_1-q_2-\cdots-q_r)-1,(n-q_1-q_2-\cdots-q_r)) = C(n+r-q_1-q_2-\cdots-q_r-1, n-q_1-q_2-\cdots-q_r)$.

30. By Theorem 3 the answer is $11!/(4!4!2!) = 34{,}650$.

32. We can treat the 3 consecutive A's as one letter. Thus we have 6 letters, of which 2 are the same (the two R's), so by Theorem 3 the answer is $6!/2! = 360$.

34. We need to calculate separately, using Theorem 3, the number of strings of length 5, 6, and 7. There are $7!/(3!3!1!) = 140$ strings of length 7. For strings of length 6, we can omit the R and form $6!/(3!3!) = 20$ string; omit an E and form $6!/(3!2!1!) = 60$ strings, or omit an S and also form 60 strings. This gives a total of 140 strings of length 6. For strings of length 5, we can omit two E's or two S's, each giving $5!/(3!1!1!) = 20$ strings; we can omit one E and one S ($5!/(2!2!1!) = 30$ strings); or we can omit the R and either an E or an S ($5!/(3!2!) = 10$ strings each). This gives a total of 90 strings of length 5, for a grand total of 370 strings of length 5 or greater.

36. We simply need to choose the 6 positions, out of the 14 available, to make 1's. There are $C(14,6) = 3003$ ways to do so.

38. We assume that the forty issues are distinguishable.

a) Theorem 4 says that the answer is $40!/10!^4 \approx 4.7\times 10^{21}$.

b) Each distribution into identical boxes gives rise to $4! = 24$ distributions into labeled boxes, since once we have made the distribution into unlabeled boxes we can arbitrarily label the boxes. Therefore the answer is the same as the answer in part **(a)** divided by 24, namely $(40!/10!^4)/4! \approx 2.0\times 10^{20}$.

40. We can describe any such travel in a unique way by a sequence of 4 x's, 3 y's, 5 z's, and 4 w's. By Theorem 3, there are

$$\frac{16!}{4!3!5!4!} = 50{,}450{,}400$$

such sequences.

42. Theorem 4 says that the answer is $52!/13!^4 \approx 5.4 \times 10^{28}$, since each player gets 13 cards.

44. **a)** All that matters is the number of books on each shelf, so the answer is the number of solutions to $x_1 + x_2 + x_3 + x_4 = 12$, where x_i is being viewed as the number of books on shelf i. The answer is therefore $C(4 + 12 - 1, 12) = C(15, 12) = 455$.

b) No generality is lost if we number the books b_1, b_2, $\ldots$, b_{12} and think of placing book b_1, then placing b_2, and so on. There are clearly 4 ways to place b_1, since we can put it as the first book (for now) on any of the shelves. After b_1 is placed, there are 5 ways to place b_2, since it can go to the right of b_1 or it can be the first book on any of the shelves. We continue in this way: there are 6 ways to place b_3 (to the right of b_1, to the right of b_2, or as the first book on any of the shelves), 7 ways to place b_4, $\ldots$, 15 ways to place b_{12}. Therefore the answer is the product of these numbers $4 \cdot 5 \cdots 15 = 217{,}945{,}728{,}000$.

46. We follow the hint. There are 5 bars (chosen books), and therefore there are 6 places where the 7 stars (nonchosen books) can fit (before the first bar, between the first and second bars, $\ldots$, after the fifth bar). Each of the second through fifth of these slots must have at least one star in it, so that adjacent books are not chosen. Once we have placed these 4 stars, there are 3 stars left to be placed in 6 slots. The number of ways to do this is therefore $C(6 + 3 - 1, 3) = C(8, 3) = 56$.

48. We can think of the n distinguishable objects to be distributed into boxes as numbered from 1 to n. Since such a distribution is completely determined by assigning a box number (from 1 to k) to each object, we can think of a distribution simply as a sequence of box numbers a_1, a_2, $\ldots$, a_n, where a_i is the box into which object i goes. Furthermore, since we want n_i objects to go into box i, this sequence must contain n_i copies of the number i (for each i from 1 to k). But this is precisely a permutation of n objects (namely, numbers) with n_i indistinguishable objects of type i (namely, n_i copies of the number i). Thus we have established the desired one-to-one correspondence. Since Theorem 3 tells us that there are $n!/(n_1!n_2!\cdots n_k!)$ permutations, there must also be this many ways to do the distribution into boxes, and the proof of Theorem 4 is complete.

50. This is actually a problem about partitions of sets. Let us call the set of 5 objects $\{a, b, c, d, e\}$. We want to partition this set into three pairwise disjoint subsets (some possibly empty). We count in a fairly ad hoc way. First, we could put all five objects into one subset (i.e., all five objects go into one box, with the other two boxes empty). Second, we could put four of the objects into one subset and one into another, such as $\{a, b, c, d\}$ together with $\{e\}$. There are 5 ways to do this, since each of the five objects can be the singleton. Third, we could put three of the objects into one set (box) and two into another; there are $C(5, 2) = 10$ ways to do this, since there are that many ways to choose which objects are to be the doubleton. Similarly, there are 10 ways to distribute the elements so that three go into one set and one each into the other two sets (for example, $\{a, b, c\}$, $\{d\}$, and $\{e\}$). Finally, we could put two items into one set, two into another, and one into the third (for example, $\{a, b\}$, $\{c, d\}$, and $\{e\}$). Here we need to choose the singleton (5 ways), and then we need to choose one of the 3 ways to separate the remaining four elements into pairs; this gives a total of 15 partitions. In all we have 41 different partitions.

This can also be solved by using the formulae given in the text in a discussion of Stirling numbers of the second kind (this follows Example 10):

$$S(5,1) = \frac{1}{1!}\left(\binom{1}{0}1^5\right) = \frac{1}{1!}(1) = 1$$

$$S(5,2) = \frac{1}{2!}\left(\binom{2}{0}2^5 - \binom{2}{1}1^5\right) = \frac{1}{2!}(32 - 2) = 15$$

$$S(5,3) = \frac{1}{3!}\left(\binom{3}{0}3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5\right) = \frac{1}{3!}(243 - 96 + 3) = 25$$

$$\sum_{j=1}^{3} S(5,j) = 1 + 15 + 25 = 41$$

52. This is similar to Exercise 50, with 3 replaced by 4. We compute this using the formulae:

$$S(5,1) = \frac{1}{1!}\left(\binom{1}{0}1^5\right) = \frac{1}{1!}(1) = 1$$

$$S(5,2) = \frac{1}{2!}\left(\binom{2}{0}2^5 - \binom{2}{1}1^5\right) = \frac{1}{2!}(32-2) = 15$$

$$S(5,3) = \frac{1}{3!}\left(\binom{3}{0}3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5\right) = \frac{1}{3!}(243-96+3) = 25$$

$$S(5,4) = \frac{1}{4!}\left(\binom{4}{0}4^5 - \binom{4}{1}3^5 + \binom{4}{2}2^5 - \binom{4}{3}1^5\right) = \frac{1}{4!}(1024-972+192-4) = 10$$

$$\sum_{j=1}^{4} S(5,j) = 1 + 15 + 25 + 10 = 51$$

54. We are asked for the partitions of 5 into at most 3 parts; notice that we are not required to use all three boxes. We can easily list these partitions explicitly: $5 = 5$, $5 = 4+1$, $5 = 3+2$, $5 = 3+1+1$, and $5 = 2+2+1$. Therefore the answer is 5.

56. This is similar to Exercise 55. Since each box has to contain at least one object, we might as well put one object into each box to begin with. This leaves us with just three more objects, and there are only three choices: we can put them all into the same box (so that the partition we end up with is $8 = 4+1+1+1+1$), or we can put them into three different boxes (so that the partition we end up with is $8 = 2+2+2+1+1$), or we can put two into one box and the last into another (so that the partition we end up with is $8 = 3+2+1+1+1$). So the answer is 3.

58. **a)** This is a straightforward application of the product rule: There are 7 choices for the first ball, 6 choices for the second ball, and so on, for an answer of $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520$.

b) Since each ball must be in a separate box and the boxes are unlabeled, there is only one way to do this.

c) This is just a matter of choosing which five boxes to put balls into, so the answer is $C(7,5) = 21$.

d) As noted in part **(b)**, there is only one way to do this.

60. There are 31 other teams to play, and we can denote these with the symbols x_1, x_2, $\ldots$, x_{31}. We are asked for a list of $4 \cdot 4 + 11 \cdot 3 + 16 \cdot 2 = 81$ of these symbols that contains exactly 4 copies of each of x_1 through x_4, exactly 3 copies of each of x_5 through x_{15}, and exactly 2 copies of each of x_{16} through x_{31}. Theorem 3 tells us that the number of possible lists is

$$\frac{81!}{(4!)^4 \cdot (3!)^{11} \cdot (2!)^{16}} \approx 7.35 \times 10^{101}.$$

(The arithmetic was done with *Maple*.)

62. Each term must be of the form $Cx_1^{n_1}x_2^{n_2}\cdots x_m^{n_m}$, where the n_i's are nonnegative integers whose sum is n. The number of ways to specify a term, then, is the number of nonnegative integer solutions to $n_1+n_2+\cdots+n_m = n$, which by Theorem 2 is $C(m+n-1,n)$. Note that the coefficients C for these terms can be computed using Theorem 3—see Exercise 63.

64. From Exercise 62, we know that there are $C(3+4-1,4) = C(6,4) = 15$ terms, and the coefficients come from Exercise 63. The answer is $x^4 + y^4 + z^4 + 4x^3y + 4xy^3 + 4x^3z + 4xz^3 + 4y^3z + 4yz^3 + 6x^2y^2 + 6x^2z^2 + 6y^2z^2 + 12x^2yz + 12xy^2z + 12xyz^2$.

66. By Exercise 62, the answer is $C(3+100-1,100) = C(102,100) = C(102,2) = 5151$.

SECTION 6.6 Generating Permutations and Combinations

2. 156423, 165432, 231456, 231465, 234561, 314562, 432561, 435612, 541236, 543216, 654312, 654321

4. Our list will have $3^3 \cdot 2^2 = 108$ items in it. Here it is in lexicographic order: 000aa, 000ab, 000ba, 000bb, 001aa, 001ab, 001ba, 001bb, 002aa, 002ab, 002ba, 002bb, 010aa, 010ab, 010ba, 010bb, 011aa, 011ab, 011ba, 011bb, 012aa, 012ab, 012ba, 012bb, 020aa, 020ab, 020ba, 020bb, 021aa, 021ab, 021ba, 021bb, 022aa, 022ab, 022ba, 022bb, 100aa, 100ab, 100ba, 100bb, 101aa, 101ab, 101ba, 101bb, 102aa, 102ab, 102ba, 102bb, 110aa, 110ab, 110ba, 110bb, 111aa, 111ab, 111ba, 111bb, 112aa, 112ab, 112ba, 112bb, 120aa, 120ab, 120ba, 120bb, 121aa, 121ab, 121ba, 121bb, 122aa, 122ab, 122ba, 122bb, 200aa, 200ab, 200ba, 200bb, 201aa, 201ab, 201ba, 201bb, 202aa, 202ab, 202ba, 202bb, 210aa, 210ab, 210ba, 210bb, 211aa, 211ab, 211ba, 211bb, 212aa, 212ab, 212ba, 212bb, 220aa, 220ab, 220ba, 220bb, 221aa, 221ab, 221ba, 221bb, 222aa, 222ab, 222ba, 222bb.

6. These can be done using Algorithm 1 or Example 2. This will be explained in detail for part **(a)**; the others are similar. In the last four parts of this exercise, the next permutation exchanges only the last two elements.
a) The last pair of integers a_j and a_{j+1} where $a_j < a_{j+1}$ is $a_2 = 3$ and $a_3 = 4$. The least integer to the right of 3 that is greater than 3 is 4. Hence 4 is placed in the second position. The integers 2 and 3 are then placed in order in the last two positions, giving the permutation 1423.
b) 51234 **c)** 13254 **d)** 612354 **e)** 1623574 **f)** 23587461

8. The first subset corresponds to the bit string 0000, namely the empty set. The next subset corresponds to the bit string 0001, namely the set $\{4\}$. The next bit string is 0010, corresponding to the set $\{3\}$, and then 0011, which corresponds to the set $\{3,4\}$. We continue in this manner, giving the remaining sets: $\{2\}$, $\{2,4\}$, $\{2,3\}$, $\{2,3,4\}$, $\{1\}$, $\{1,4\}$, $\{1,3\}$, $\{1,3,4\}$, $\{1,2\}$, $\{1,2,4\}$, $\{1,2,3\}$, $\{1,2,3,4\}$.

10. Since the new permutation agrees with the old one in positions 1 to $j-1$, and since the new permutation has a_k in position j, whereas the old one had a_j, with $a_k > a_j$, the new permutation succeeds the old one in lexicographic order. Furthermore the new permutation is the first one (in lexicographic order) with a_1, a_2, $\ldots$, a_{j-1}, a_k in positions 1 to j, and the old permutation was the last one with a_1, a_2, $\ldots$, a_{j-1}, a_j in those positions. Since a_k was picked to be the smallest number greater than a_j among a_{j+1}, a_{j+2}, $\ldots$, a_n, there can be no permutation between these two.

12. One algorithm would combine Algorithm 3 and Algorithm 1. Using Algorithm 3, we generate all the r-combinations of the set with n elements. At each stage, after we have found each r-combination, we use Algorithm 1, with $n = r$ (and a different collection to be permuted than $\{1,2,\ldots,n\}$), to generate all the permutations of the elements in this combination. See the solution to Exercise 13 for an example.

14. **a)** We find that $a_1 = 1$, $a_2 = 1$, $a_3 = 2$, $a_4 = 2$, and $a_5 = 3$. Therefore the number is $1 \cdot 1! + 1 \cdot 2! + 2 \cdot 3! + 2 \cdot 4! + 3 \cdot 5! = 1 + 2 + 12 + 48 + 360 = 423$.
b) Each $a_k = 0$, so the number is 0.
c) We find that $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, and $a_5 = 5$. Therefore the number is $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + 4 \cdot 4! + 5 \cdot 5! = 1 + 4 + 18 + 96 + 600 = 719 = 6! - 1$, as expected, since this is the last permutation.

16. **a)** We find the Cantor expansion of 3 to be $1\cdot 1! + 1\cdot 2!$. Therefore we know that $a_4 = 0$, $a_3 = 0$, $a_2 = 1$, and $a_1 = 1$. Following the algorithm given in the solution to Exercise 15, we put 5 in position $5-0=5$, put 4 in position $4-0=4$, put 3 in position $3-1=2$, and put 2 in the position that is 1 from the rightmost available position, namely position 1. Therefore the answer is 23145.

b) We find that $89 = 1\cdot 1! + 2\cdot 2! + 2\cdot 3! + 3\cdot 4!$. Therefore we insert 5, 4, 3, and 2, in order, skipping 3, 2, 2, and 1 positions from the right among the available positions, obtaining 35421.

c) We find that $111 = 1\cdot 1! + 1\cdot 2! + 2\cdot 3! + 4\cdot 4!$. Therefore we insert 5, 4, 3, and 2, in order, skipping 4, 2, 1, and 1 positions from the right among the available positions, obtaining 52431.

SUPPLEMENTARY EXERCISES FOR CHAPTER 6

2. **a)** There are no ways to do this, since there are not enough items. **b)** $6^{10} = 60{,}466{,}176$

c) There are no ways to do this, since there are not enough items.

d) $C(6+10-1,10) = C(15,10) = C(15,5) = 3003$

4. There are 2^7 bit strings of length 10 that start 000, since each of the last 7 bits can be chosen in either of two ways. Similarly, there are 2^6 bit strings of length 10 that end 1111, and there are 2^3 bit strings of length 10 that both start 000 and end 1111 (since only the 3 middle bits can be freely chosen). Therefore by the inclusion–exclusion principle, the answer is $2^7 + 2^6 - 2^3 = 184$.

6. $9\cdot 10\cdot 10\cdot 10\cdot 10 = 90{,}000$

8. **a)** All the integers from 100 to 999 have three decimal digits, and there are $999-100+1=900$ of these.

b) In addition to the 900 three-digit numbers, there are 9 one-digit positive integers, for a total of 909.

c) There is 1 one-digit number with a 9. Among the two-digit numbers, there are the 10 numbers from 90 to 99, together with the 8 numbers 19, 29, $\ldots$, 89, for a total of 18. Among the three-digit numbers, there are the 100 from 900 to 999; and there are, for each century from the 100's to the 800's, again $1+18=19$ numbers with at least one 9; this gives a total of $100+8\cdot 19 = 252$. Thus our final answer is $1+18+252=271$. Alternately, we can compute this as $10^3 - 9^3 = 271$, since we want to subtract from the number of three-digit nonnegative numbers (with leading 0's allowed) the number of those that use only the nine digits 0 through 8.

d) Since we can use only even digits, there are $5^3 = 125$ ways to specify a three-digit number, allowing leading 0's. Since, however, the number $0 = 000$ is not in our set, we need to subtract 1, obtaining the answer 124.

e) The numbers in question are either of the form $d55$ or $55d$, with $d \neq 5$, or 555. Since d can be any of nine digits, there are $9+9+1=19$ such numbers.

f) All 9 one-digit numbers are palindromes. The 9 two-digit numbers 11, 22, $\ldots$, 99 are palindromes. For three-digit numbers, the first digit (which must equal the third digit) can be any of the 9 nonzero digits, and the second digit can be any of the 10 digits, giving $9\cdot 10 = 90$ possibilities. Therefore the answer is $9+9+90=108$.

10. Using the generalized pigeonhole principle, we see that we need $5\times 12+1=61$ people.

12. There are $7\times 12 = 84$ day-month combinations. Therefore we need 85 people to ensure that two of them were born on the same day of the week and in the same month.

14. We need at least 551 cards to ensure that at least two are identical. Since the cards come in packages of 20, we need $\lceil 551/20\rceil = 28$ packages.

16. Partition the set of numbers from 1 to $2n$ into the n pigeonholes $\{1,2\}$, $\{3,4\}$, $\ldots$, $\{2n-1,2n\}$. If we have $n+1$ numbers from this set (the pigeons), then two of them must be in the same hole. This means that among our collection are two consecutive numbers. Clearly consecutive numbers are relatively prime (since every common divisor must divide their difference, 1).

18. Divide the interior of the square, with lines joining the midpoints of opposite sides, into four 1×1 squares. By the pigeonhole principle, at least two of the five points must be in the same small square. The furthest apart two points in a square could be is the length of the diagonal, which is $\sqrt{2}$ for a square 1 unit on a side.

20. If the worm never gets sent to the same computer twice, then it will infect 100 computers on the first round of forwarding, $100^2 = 10{,}000$ other computers on the second round of forwarding, and so on. Therefore the maximum number of different computers this one computer can infect is $100 + 100^2 + 100^3 + 100^4 + 100^5 = 10{,}101{,}010{,}100$. This figure of ten billion is probably comparable to the total number of computers in the world.

22. **a)** We want to solve $n(n-1) = 110$, or $n^2 - n - 110 = 0$. Simple algebra gives $n = 11$ (we ignore $n = -10$, since we need a positive integer for our answer).

b) We recall that $7! = 5040$, so the answer is 7.

c) We need to solve the equation $n(n-1)(n-2)(n-3) = 12n(n-1)$. Since we have $n \geq 4$ in order for $P(n,4)$ to be defined, this equation reduces to $(n-2)(n-3) = 12$, or $n^2 - 5n - 6 = 0$. Simple algebra gives $n = 6$ (we ignore the solution $n = -1$ since n needs to be a positive integer).

24. An algebraic proof is straightforward. We will give a combinatorial proof of the equivalent identity $P(n+1,r)(n+1-r) = (n+1)P(n,r)$ (and in fact both of these equal $P(n+1,r+1)$). Consider the problem of writing down a permutation of $r+1$ objects from a collection of $n+1$ objects. We can first write down a permutation of r of these objects ($P(n+1,r)$ ways to do so), and then write down one more object (and there are $n+1-r$ objects left to choose from), thereby obtaining the left-hand side; or we can first choose an object to write down first ($n+1$ to choose from), and then write down a permutation of length r using the n remaining objects ($P(n,r)$ ways to do so), thereby obtaining the right-hand side.

26. First note that Corollary 2 of Section 6.4 is equivalent to the assertion that the sum of the numbers $C(n,k)$ for even k is equal to the sum of the numbers $C(n,k)$ for odd k. Since $C(n,k)$ counts the number of subsets of size k of a set with n elements, we need to show that a set has as many even-sized subsets as it has odd-sized subsets. Define a function f from the set of all subsets of A to itself (where A is a set with n elements, one of which is a), by setting $f(B) = B \cup \{a\}$ if $a \notin B$, and $f(B) = B - \{a\}$ if $a \in B$. It is clear that f takes even-sized subsets to odd-sized subsets and vice versa, and that f is one-to-one and onto (indeed, $f^{-1} = f$). Therefore f restricted to the set of subsets of odd size gives a one-to-one correspondence between that set and the set of subsets of even size.

28. The base case is $n = 2$, in which case the identity simply states that $1 = 1$. Assume the inductive hypothesis, that $\sum_{j=2}^{n} C(j,2) = C(n+1,3)$. Then

$$\begin{aligned}\sum_{j=2}^{n+1} C(j,2) &= \left(\sum_{j=2}^{n} C(j,2)\right) + C(n+1,2)\\ &= C(n+1,3) + C(n+1,2) = C((n+1)+1,3)\,,\end{aligned}$$

as desired. The last equality made use of Pascal's identity.

30. Each pair of values of i and j with $1 \leq i < j \leq n$ contributes a 1 to this sum, so the sum is just the number of such pairs. But this is clearly the number of ways to choose two integers from $\{1,2,\ldots,n\}$, which is $C(n,2)$, also known as $\binom{n}{2}$.

32. **a)** For a fixed k, a triple is totally determined by picking i and j; since each can be picked in k ways (each can be any number from 0 to $k-1$, inclusive), there are k^2 ways to choose the triple. Adding over all possible values of k gives the indicated sum.

b) A triple of this sort is totally determined by knowing the *set* of numbers $\{i, j, k\}$, since the order is fixed. Therefore the number of triples of each kind is just the number of sets of 3 elements chosen from the set $\{0, 1, 2, \ldots, n\}$, and that is clearly $C(n+1, 3)$.

c) In order for i to equal j (with both less than k), we need to pick two elements from $\{0, 1, 2, \ldots, n\}$, using the larger one for k and the smaller one for both i and j. Therefore there are as many such choices as there are 2-element subsets of this set, namely $C(n+1, 2)$.

d) This part is its own proof. The last equality follows from elementary algebra.

34. **a)** If we 2-color the $2d-1$ elements of S, then there must be at least d elements of one color (if there were $d-1$ or fewer elements of both colors, then only $2d-2$ elements would be colored); this is just an application of the generalized pigeonhole principle. Thus there is a d-element subset that does not contain both colors, in violation of the condition for being 2-colorable.

b) We must show that every collection of fewer than three sets each containing two elements is 2-colorable, and that there is a collection of three sets each containing two elements that is not 2-colorable. The second statement follows from part **(a)**, with $d = 2$ (the three sets are $\{1, 2\}$, $\{1, 3\}$, and $\{2, 3\}$). On the other hand, if we have two (or fewer) sets each with two elements, then we can color the two elements of the first set with different colors, and we cannot be prevented from properly coloring the second set, since it must contain an element not in the first set.

c) First we show that the given collection is not 2-colorable. Without loss of generality, assume that 1 is red. If 2 is red, then 6 must be blue (second set). Thus either 4 or 5 must be red (seventh set), which means that 3 must be blue (first or fourth set). This would force 7 to be red (sixth set), which would force both 4 and 5 to be blue (third and fifth sets), a contradiction. Thus 2 is blue. If 3 is red, then we can conclude that 5 is blue, 7 is red, 6 is blue, and 4 is blue, making the last set improperly colored. Thus 3 is blue. This implies that 4 is red, hence 7 is blue, hence 5 and 6 are red, another contradiction. So the given collection cannot be 2-colored. Next we must show that all collections of six sets with three elements each are 2-colorable. Since having more elements in S at our disposable only makes it easier to 2-color the collection, we can assume that S has only five elements; let $S = \{a, b, c, d, e\}$. Since there are 18 occurrences of elements in the collection, some element, say a, must occur at least four times (since $3 \cdot 5 < 18$). If a occurs in six of the sets, then we can color a red and the rest of the elements blue. If a occurs in five of the sets, suppose without loss of generality that b and c occur in the sixth set. Then we can color a and b red and the remaining elements blue. Finally, if a occurs in only four of the sets, then that leaves only four elements for the last two sets, and therefore a pair of elements must be shared by them, say b and c. Again coloring a and b red and the remaining elements blue gives the desired coloring.

36. We might as well assume that the first person sits in the northernmost seat. Then there are $P(7, 7)$ ways to seat the remaining people, since they form a permutation reading clockwise from the first person. Therefore the answer is $7! = 5040$.

38. We need to know the number of solutions to $d + m + g = 12$, where d, m, and g are integers greater than or equal to 3. This is equivalent to the number of nonnegative integer solutions to $d' + m' + g' = 3$, where $d' = d-3$, $m' = m-3$, and $g' = g-3$. By Theorem 2 of Section 6.5, the answer is $C(3+3-1, 3) = C(5, 3) = 10$.

40. **a)** By Theorem 3 of Section 6.5, the answer is $10!/(3!2!2!) = 151{,}200$.

b) If we fix the start and the end, then the question concerns only 8 letters, and the answer is $8!/(2!2!) = 10{,}080$.

c) If we think of the three P's as one letter, then the answer is seen to be $8!/(2!2!) = 10{,}080$.

42. There are 26 choices for the third letter. If the digit part of the plate consists of the digits 1, 2, and d, where d is different from 1 or 2, then there are 8 choices for d and $3! = 6$ choices for a permutation of these digits. If $d = 1$ or 2, then there are 2 choices for d and 3 choices for a permutation. Therefore the answer is $26(8 \cdot 6 + 2 \cdot 3) = 1404$.

44. Let us look at the girls first. There are $P(8,8) = 8! = 40320$ ways to order them relative to each other. This much work produces 9 gaps between girls (including the ends), in each of which at most one boy may sit. We need to choose, in order without repetition, 6 of these gaps, and this can be done in $P(9,6) = 60480$ ways. Therefore the answer is, by the product rule, $40320 \cdot 60480 = 2{,}438{,}553{,}600$.

46. We are given no restrictions, so any number of the boxes can be occupied once we have distributed the objects.

a) This is a straightforward application of the product rule; there are $6^5 = 7776$ ways to do this, because there are 6 choices for each of the 5 objects.

b) This is similar to Exercise 50 in Section 6.5. We compute this using the formulae:

$$S(5,1) = \frac{1}{1!}\left(\binom{1}{0}1^5\right) = \frac{1}{1!}(1) = 1$$

$$S(5,2) = \frac{1}{2!}\left(\binom{2}{0}2^5 - \binom{2}{1}1^5\right) = \frac{1}{2!}(32-2) = 15$$

$$S(5,3) = \frac{1}{3!}\left(\binom{3}{0}3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5\right) = \frac{1}{3!}(243-96+3) = 25$$

$$S(5,4) = \frac{1}{4!}\left(\binom{4}{0}4^5 - \binom{4}{1}3^5 + \binom{4}{2}2^5 - \binom{4}{3}1^5\right) = \frac{1}{4!}(1024-972+192-4) = 10$$

$$S(5,5) = \frac{1}{5!}\left(\binom{5}{0}5^5 - \binom{5}{1}4^5 + \binom{5}{2}3^5 - \binom{5}{3}2^5 + \binom{5}{4}1^5\right) = \frac{1}{5!}(3125-5120+2430-320+5) = 1$$

$$\sum_{j=1}^{5} S(5,j) = 1 + 15 + 25 + 10 + 1 = 52$$

c) This is asking for the number of solutions to $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 5$ in nonnegative integers. By Theorem 2 (see also Example 5) in Section 6.5, the answer is $C(6+5-1,5) = C(10,5) = 252$.

d) This is asking for the number of partitions of 5 (into at most six parts, but that is moot). We list them: $5 = 5$, $5 = 4+1$, $5 = 3+2$, $5 = 3+1+1$, $5 = 2+2+1$, $5 = 2+1+1+1$, $5 = 1+1+1+1+1$. Therefore the answer is 7.

48. One way to look at this involves what is called the cycle structure of a permutation. Think of the people as the numbers from 1 to n. Given a permutation π of $\{1,2,\ldots,n\}$, we can write down the cycles the result from applying this permutation. Each cycle can be viewed as a list of the people sitting at a circular table, in clockwise order. The first cycle contains 1, $\pi(1)$, $\pi(\pi(1))$, $\ldots$, until we eventually return to 1 (which must happen because permutation are one-to-one functions). If k is the first number not in the first cycle, then the second cycle consists of k, $\pi(k)$, $\pi(\pi(k))$, $\ldots$, and so on. For example, the permutation that sends x to $x+3$ on a 12-hour clock has cycle structure $(1,4,7,10)$, $(2,5,8,11)$, $(3,6,9,12)$. Thus each of the $n!$ permutations gives rise to a seating of n people around j circular tables for some j between 1 and n inclusive. Conversely, such a seating gives us a permutation—$\pi(x)$ is the number clockwise from x at whatever table x is at (which could be x itself). The identity follows from this discussion.

50. We can give a nice combinatorial proof here. If we wish to have people numbered 1 through $n+1$ sit at k circular tables, there are two choices. We could have $n+1$ sit at a table by himself and then place the remaining n people at $k-1$ circular tables (the first term on the right-hand side of this identity), or we could seat the first n people at the k tables and then have $n+1$ sit immediately to the right of one of those people (there being n choices for this last step, giving us the second term on the right).

52. Except for the last three symbols, for which we have no choice, we need a permutation of 2 A's, 2 C's, 2 U's, and 2 G's. By Theorem 3 in Section 6.5, the answer is $8!/(2!)^4 = 2520$.

54. From the first piece of information, we know that the chain ends AC and preceding that are the chains UG and ACG in some order. So there are only two choices: UGACGAC or ACGUGAC. It is easily seen that breaking the first of these after each U or C produces the fragments stated in the second half of the first sentence, whereas breaking the second choice similarly produces something else (AC, GU, GAC). Therefore the original chain was UGACGAC.

56. Assume without loss of generality that we wish to form r-combinations from the set $\{1, 2, \ldots, n\}$. We modify Algorithm 3 in Section 6.6 for generating the next r-combination in lexicographic order, allowing for repetition. Then we generate all such combinations by starting with $11\ldots1$ and calling this modified algorithm $C(n+r-1, r) - 1$ times (this will give us $nn\ldots n$ as the last one).

> **procedure** *next r-combination*$(a_1, a_2, \ldots, a_r$: integers)
> $\{$We assume that $1 \le a_1 \le a_2 \le \cdots \le a_r \le n$, with $a_1 \ne n\,\}$
> $i := r$
> **while** $a_i = n$
> $i := i - 1$
> $a_i := a_i + 1$
> **for** $j := i + 1$ **to** r
> $a_j := a_i$

58. One needs to play around with this enough to eventually discover a situation satisfying the conditions. Here is a way to do it. Suppose the group consists of three men and three women, and suppose that people of the same sex are always enemies and people of the opposite sex are always friends. Then clearly there can be no set of four mutual enemies, because any set of four people must include at least one man and one woman (since there are only three of each sex in the whole group). Also there can be no set of three mutual friends, because any set of three people must include at least two people of the same sex (since there are only two sexes).

CHAPTER 7
Discrete Probability

SECTION 7.1 An Introduction to Discrete Probability

2. The probability is $1/6 \approx 0.17$, since there are six equally likely outcomes.

4. Since April has 30 days, the answer is $30/366 = 5/61 \approx 0.082$.

6. There are 16 cards that qualify as being an ace or a heart, so the answer is $16/52 = 4/13 \approx 0.31$. We could also compute this from Theorem 2 as $4/52 + 13/52 - 1/52$.

8. We saw in Example 11 of Section 6.3 that there are $C(52,5)$ possible poker hands, and we assume by symmetry that they are all equally likely. In order to solve this problem, we need to compute the number of poker hands that contain the ace of hearts. There is no choice about choosing the ace of hearts. To form the rest of the hand, we need to choose 4 cards from the 51 remaining cards, so there are $C(51,4)$ hands containing the ace of hearts. Therefore the answer to the question is the ratio

$$\frac{C(51,4)}{C(52,5)} = \frac{5}{52} \approx 9.6\%.$$

The problem can also be done by subtracting from 1 the answer to Exercise 9, since a hand contains the ace of hearts if and only if it is not the case that it does not contain the ace of hearts.

10. This is similar to Exercise 8. We need to compute the number of poker hands that contain the two of diamonds and the three of spades. There is no choice about choosing these two cards. To form the rest of the hand, we need to choose 3 cards from the 50 remaining cards, so there are $C(50,3)$ hands containing these two specific cards. Therefore the answer to the question is the ratio

$$\frac{C(50,3)}{C(52,5)} = \frac{5}{663} \approx 0.0075.$$

12. There are 4 ways to specify the ace. Once the ace is chosen for the hand, there are $C(48,4)$ ways to choose nonaces for the remaining four cards. Therefore there are $4C(48,4)$ hands with exactly one ace. Since there are $C(52,5)$ equally likely hands, the answer is the ratio

$$\frac{4C(48,4)}{C(52,5)} \approx 0.30.$$

14. We saw in Example 11 of Section 6.3 that there are $C(52,5) = 2{,}598{,}960$ different hands, and we assume by symmetry that they are all equally likely. We need to count the number of hands that have 5 different kinds (ranks). There are $C(13,5)$ ways to choose the kinds. For each card, there are then 4 ways to choose the suit. Therefore there are $C(13,5) \cdot 4^5 = 1{,}317{,}888$ ways to choose the hand. Thus the probability is $1317888/2598960 = 2112/4165 \approx 0.51$.

16. Of the $C(52,5) = 2{,}598{,}960$ hands, $4 \cdot C(13,5) = 5148$ are flushes, since we can specify a flush by choosing a suit and then choosing 5 cards from that suit. Therefore the answer is $5148/2598960 = 33/16660 \approx 0.0020$.

18. There are clearly only $10 \cdot 4 = 40$ straight flushes, since all we get to specify for a straight flush is the starting (lowest) kind in the straight (anything from ace up to ten) and the suit. Therefore the answer is $40/C(52,5) = 40/2598960 = 1/64974$.

20. There are 4 royal flushes, one in each suit. Therefore the answer is $4/C(52,5) = 4/2598960 = 1/649740$.

22. There are $\lfloor 100/3 \rfloor = 33$ multiples of 3 among the integers from 1 to 100 (inclusive), so the answer is $33/100 = 0.33$.

24. In each case, if the numbers are chosen from the integers from 1 to n, then there are $C(n,6)$ possible entries, only one of which is the winning one, so the answer is $1/C(n,6)$.
a) $1/C(30,6) = 1/593775 \approx 1.7 \times 10^{-6}$ **b)** $1/C(36,6) = 1/1947792 \approx 5.1 \times 10^{-7}$
c) $1/C(42,6) = 1/5245786 \approx 1.9 \times 10^{-7}$ **d)** $1/C(48,6) = 1/12271512 \approx 8.1 \times 10^{-8}$

26. In each case, if the numbers are chosen from the integers from 1 to n, then there are $C(n,6)$ possible entries. If we wish to avoid all the winning numbers, then we must make our choice from the $n-6$ nonwinning numbers, and this can be done in $C(n-6,6)$ ways. Therefore, since the winning numbers are picked at random, the probability is $C(n-6,6)/C(n,6)$.
a) $C(34,6)/C(40,6) = 1344904/3838380 \approx 0.35$ **b)** $C(42,6)/C(48,6) = 5245786/12271512 \approx 0.43$
c) $C(50,6)/C(56,6) = 15890700/32468436 \approx 0.49$ **d)** $C(58,6)/C(64,6) = 40475358/74974368 \approx 0.54$

28. We need to find the number of ways for the computer to select its 11 numbers, and we need to find the number of ways for it to select its 11 numbers so as to contain the 7 numbers that we chose. For the former, the number is clearly $C(80,11)$. For the latter, the computer must select four more numbers besides the ones we chose, from the $80 - 7 = 73$ other numbers, so there are $C(73,4)$ ways to do this. Therefore the probability that we win is the ratio $C(73,4)/C(80,11)$, which works out to $3/28879240$, or about one chance in ten million (1.04×10^{-7}). The same answer can be obtained by counting things in the other direction: the number of ways for us to choose 7 of the computer's predestined 11 numbers divided by the number of ways for us to pick 7 numbers. This gives $C(11,7)/C(80,7)$, which has the same value as before.

30. In order to specify a winning ticket, we must choose five of the six numbers to match ($C(6,5) = 6$ ways to do so) and one number from among the remaining 34 numbers not to match ($C(34,1) = 34$ ways to do so). Therefore there are $6 \cdot 34 = 204$ winning tickets. Since there are $C(40,6) = 3{,}838{,}380$ tickets in all, the answer is $204/3838380 = 17/319865 \approx 5.3 \times 10^{-5}$, or about 1 chance in 19,000.

32. The number of ways for the drawing to turn out is $100 \cdot 99 \cdot 98$. The number of ways of ways for the drawing to cause Kumar, Janice, and Pedro each to win a prize is $3 \cdot 2 \cdot 1$ (three ways for one of these to be picked to win first prize, two ways for one of the others to win second prize, one way for the third to win third prize). Therefore the probability we seek is $(3 \cdot 2 \cdot 1)/(100 \cdot 99 \cdot 98) = 1/161700$.

34. **a)** There are $50 \cdot 49 \cdot 48 \cdot 47$ equally likely outcomes of the drawings. In only one of these do Bo, Colleen, Jeff, and Rohini win the first, second, third, and fourth prizes, respectively. Therefore the probability is $1/(50 \cdot 49 \cdot 48 \cdot 47) = 1/5527200$.
b) There are $50 \cdot 50 \cdot 50 \cdot 50$ equally likely outcomes of the drawings. In only one of these do Bo, Colleen, Jeff, and Rohini win the first, second, third, and fourth prizes, respectively. Therefore the probability is $1/50^4 = 1/6250000$.

36. Reasoning as in Example 2, we see that there are 5 ways to get a total of 8 when two dice are rolled: $(6,2)$, $(5,3)$, $(4,4)$, $(3,5)$, and $(2,6)$. There are $6^2 = 36$ equally likely possible outcomes of the roll of two dice, so the probability of getting a total of 8 when two dice are rolled is $5/36 \approx 0.139$. For three dice, there are $6^3 = 216$ equally likely possible outcomes, which we can represent as ordered triples (a,b,c). We need to enumerate the possibilities that give a total of 8. This is done in a more systematic way in Section 6.5, but we will do it here by brute force. The first die could turn out to be a 6, giving rise to the 1 triple $(6,1,1)$. The first die could be a 5, giving rise to the 2 triples $(5,2,1)$, and $(5,1,2)$. Continuing in this way, we see that there are 3 triples giving a total of 8 when the first die shows a 4, 4 triples when it shows a 3, 5 triples when it shows a 2, and 6 triples when it shows a 1 (namely $(1,6,1)$, $(1,5,2)$, $(1,4,3)$, $(1,3,4)$, $(1,2,5)$, and $(1,1,6)$). Therefore there are $1+2+3+4+5+6 = 21$ possible outcomes giving a total of 8. This tells us that the probability of rolling a 8 when three dice are thrown is $21/216 \approx 0.097$, smaller than the corresponding value for two dice. Thus rolling a total of 8 is more likely when using two dice than when using three.

38. **a)** Intuitively, these should be independent, since the first event seems to have no influence on the second. In fact we can compute as follows. First $p(E_1) = 1/2$ and $p(E_2) = 1/2$ by the symmetry of coin tossing. Furthermore, $E_1 \cap E_2$ is the event that the first two coins come up tails and heads, respectively. Since there are four equally likely outcomes for the first two coins (HH, HT, TH, and TT), $p(E_1 \cap E_2) = 1/4$. Therefore $p(E_1 \cap E_2) = 1/4 = (1/2) \cdot (1/2) = p(E_1)p(E_2)$, so the events are indeed independent.

b) Again $p(E_1) = 1/2$. For E_2, note that there are 8 equally likely outcomes for the three coins, and in 2 of these cases E_2 occurs (namely HHT and THH); therefore $p(E_2) = 2/8 = 1/4$. Thus $p(E_1)p(E_2) = (1/2) \cdot (1/4) = 1/8$. Now $E_1 \cap E_2$ is the event that the first coin comes up tails, and two but not three heads come up in a row. This occurs precisely when the outcome is THH, so the probability is $1/8$. This is the same as $p(E_1)p(E_2)$, so the events are independent.

c) As in part **(b)**, $p(E_1) = 1/2$ and $p(E_2) = 1/4$. This time $p(E_1 \cap E_2) = 0$, since there is no way to get two heads in a row if the second coin comes up tails. Since $p(E_1)p(E_2) \neq p(E_1 \cap E_2)$, the events are not independent.

40. You had a $1/4$ chance of winning with your original selection. Just as in the original problem, the host's action did not change this, since he would act the same way regardless of whether your selection was a winner or a loser. Therefore you have a $1/4$ chance of winning if you do not change. This implies that there is a $3/4$ chance of the prize's being behind one of the other doors. Since there are two such doors and by symmetry the probabilities for each of them must be the same, your chance of winning after switching is half of $3/4$, or $3/8$.

SECTION 7.2 Probability Theory

2. We are told that $p(3) = 2p(x)$ for each $x \neq 3$, but it is implied that $p(1) = p(2) = p(4) = p(5) = p(6)$. We also know that the sum of these six numbers must be 1. It follows easily by algebra that $p(3) = 2/7$ and $p(x) = 1/7$ for $x = 1,2,4,5,6$.

4. If outcomes are equally likely, then the probability of each outcome is $1/n$, where n is the number of outcomes. Clearly this quantity is between 0 and 1 (inclusive), so (i) is satisfied. Furthermore, there are n outcomes, and the probability of each is $1/n$, so the sum shown in (ii) must equal $n \cdot (1/n) = 1$.

6. We can exploit symmetry in answering these.

a) Since 1 has either to precede 3 or to follow it, and there is no reason that one of these should be any more likely than the other, we immediately see that the answer is $1/2$. We could also simply list all 6 permutations and count that 3 of them have 1 preceding 3, namely 123, 132, and 213.

b) By the same reasoning as in part **(a)**, the answer is again $1/2$.

c) The stated conditions force 3 to come first, so only 312 and 321 are allowed. Therefore the answer is $2/6 = 1/3$.

8. We exploit symmetry in answering many of these.

a) Since 1 has either to precede 2 or to follow it, and there is no reason that one of these should be any more likely than the other, we immediately see that the answer is $1/2$.

b) By the same reasoning as in part **(a)**, the answer is again $1/2$.

c) For 1 immediately to precede 2, we can think of these two numbers as glued together in forming the permutation. Then we are really permuting $n-1$ numbers—the single numbers from 3 through n and the one glued object, 12. There are $(n-1)!$ ways to do this. Since there are $n!$ permutations in all, the probability of randomly selecting one of these is $(n-1)!/n! = 1/n$.

d) Half of the permutations have n preceding 1. Of these permutations, half of them have $n-1$ preceding 2. Therefore one fourth of the permutations satisfy these conditions, so the probability is $1/4$.

e) Looking at the relative placements of 1, 2, and n, we see that one third of the time, n will come first. Therefore the answer is $1/3$.

10. Note that there are $26!$ permutations of the letters, so the denominator in all of our answers is $26!$. To find the numerator, we have to count the number of ways that the given event can happen. Alternatively, in some cases we may be able to exploit symmetry.

a) There are $13!$ possible arrangements of the first 13 letters of the permutation, and in only one of these are they in alphabetical order. Therefore the answer is $1/13!$.

b) Once these two conditions are met, there are $24!$ ways to choose the remaining letters for positions 2 through 25. Therefore the answer is $24!/26! = 1/650$.

c) In effect we are forming a permutation of 25 items—the letters b through y and the double letter combination az or za. There are $25!$ ways to permute these items, and for each of these permutations there are two choices as to whether a or z comes first. Thus there are $2 \cdot 25!$ ways for form such a permutation, and therefore the answer is $2 \cdot 25!/26! = 1/13$.

d) By part **(c)**, the probability that a and b *are* next to each other is $1/13$. Therefore the probability that a and b are *not* next to each other is $12/13$.

e) There are six ways this can happen: $ax^{24}z$, $zx^{24}a$, $xax^{23}z$, $xzx^{23}a$, $ax^{23}zx$, and $zx^{23}ax$, where x stands for any letter other than a and z (but of course all the x's are different in each permutation). In each of these there are $24!$ ways to permute the letters other than a and z, so there are $24!$ permutations of each type. This gives a total of $6 \cdot 24!$ permutations meeting the conditions, so the answer is $(6 \cdot 24!)/26! = 3/325$.

f) Looking at the relative placements of z, a, and b, we see that one third of the time, z will come first. Therefore the answer is $1/3$.

12. Clearly $p(E \cup F) \geq p(E) = 0.8$. Also, $p(E \cup F) \leq 1$. If we apply Theorem 2 from Section 7.1, we can rewrite this as $p(E) + p(F) - p(E \cap F) \leq 1$, or $0.8 + 0.6 - p(E \cap F) \leq 1$. Solving for $p(E \cap F)$ gives $p(E \cap F) \geq 0.4$.

14. The basis step $n = 1$ is the trivial statement that $p(E_1) \geq p(E_1)$, and the case $n = 2$ was done in Exercise 13. Assume the inductive hypothesis:

$$p(E_1 \cap E_2 \cap \cdots \cap E_n) \geq p(E_1) + p(E_2) + \cdots + p(E_n) - (n-1)$$

Now let $E = E_1 \cap E_2 \cap \cdots \cap E_n$ and let $F = E_{n+1}$, and apply Exercise 13. We obtain

$$p(E_1 \cap E_2 \cap \cdots \cap E_n \cap E_{n+1}) \geq p(E_1 \cap E_2 \cap \cdots \cap E_n) + p(E_{n+1}) - 1\,.$$

Substituting from the inductive hypothesis we have

$$\begin{aligned} p(E_1 \cap E_2 \cap \cdots \cap E_n \cap E_{n+1}) &\geq p(E_1) + p(E_2) + \cdots + p(E_n) - (n-1) + p(E_{n+1}) - 1 \\ &= p(E_1) + p(E_2) + \cdots + p(E_n) + p(E_{n+1}) - ((n+1) - 1)\,, \end{aligned}$$

as desired.

16. By definition, to say that $\overline{E}$ and $\overline{F}$ are independent is to say that $p(\overline{E} \cap \overline{F}) = p(\overline{E}) \cdot p(\overline{F})$. By De Morgan's Law, $\overline{E} \cap \overline{F} = \overline{E \cup F}$. Therefore

$$\begin{aligned} p(\overline{E} \cap \overline{F}) &= p(\overline{E \cup F}) = 1 - p(E \cup F) \\ &= 1 - (p(E) + p(F) - p(E \cap F)) \\ &= 1 - p(E) - p(F) + p(E \cap F) \\ &= 1 - p(E) - p(F) + p(E) \cdot p(F) \\ &= (1 - p(E)) \cdot (1 - p(F)) = p(\overline{E}) \cdot p(\overline{F})\,. \end{aligned}$$

(We used the two facts presented in the subsection on combinations of events.)

18. As instructed, we assume that births are independent and the probability of a birth in each day is $1/7$. (This is not exactly true; for example, doctors tend to schedule C-sections on weekdays.)

a) The probability that the second person has the same birth day-of-the-week as the first person (whatever that was) is $1/7$.

b) We proceed as in Example 13. The probability that all the birth days-of-the-week are different is

$$p_n = \frac{6}{7} \cdot \frac{5}{7} \cdot \cdots \cdot \frac{8-n}{7}$$

since each person after the first must have a different birth day-of-the-week from all the previous people in the group. Note that if $n \geq 8$, then $p_n = 0$ since the seventh fraction is 0 (this also follows from the pigeonhole principle). The probability that at least two are born on the same day of the week is therefore $1 - p_n$.

c) We compute $1 - p_n$ for $n = 2, 3, \ldots$ and find that the first time this exceeds $1/2$ is when $n = 4$, so that is our answer. With four people, the probability that at least two will share a birth day-of-the-week is $223/343$, or about 65%.

20. If n people are chosen at random (and we assume 366 equally likely and independent birthdays, as instructed), then the probability that none of them has a birthday today is $(365/366)^n$. The question asks for the smallest n such that this quantity is less than $1/2$. We can determine this by trial and error, or we can solve the equation $(365/366)^n = 1/2$ using logarithms. In either case, we find that for $n \leq 253$, $(365/366)^n > 1/2$, but $(365/366)^{254} \approx .4991$. Therefore the answer is 254.

22. a) Given that we are no longer close to the year 1900, which was not a leap year, let us assume that February 29 occurs one time every four years, and that every other date occurs four times every four years. A cycle of four years contains $4 \cdot 365 + 1 = 1461$ days. Therefore the probability that a randomly chosen day is February 29 is $1/1461$, and the probability that a randomly chosen day is any of the other 365 dates is each $4/1461$.

b) We need to compute the probability that in a group of n people, all of them have different birthdays. Rather than compute probabilities at each stage, let us count the number of ways to choose birthdays from the four-year cycle so that all n people have distinct birthdays. There are two cases to consider, depending on whether the group contains a person born on February 29. Let us suppose that there is such a leap-day person; there are n ways to specify which person he is to be. Then there are 1460 days on which the second person can be born so as not to have the same birthday; then there are 1456 days on which the third person can be born so as not to have the same birthday as either of the first two, as so on, until there are $1468-4n$ days on which the n^{th} person can be born so as not to have the same birthday as any of the others. This gives a total of

$$n \cdot 1460 \cdot 1456 \cdots (1468-4n)$$

ways in all. The other case is that in which there is no leap-day birthday. Then there are 1460 possible birthdays for the first person, 1456 for the second, and so on, down to $1464-4n$ for the n^{th}. Thus the total number of ways to choose birthdays without including February 29 is

$$1460 \cdot 1456 \cdots (1464-4n)\,.$$

The sum of these two numbers is the numerator of the fraction giving the probability that all the birthdays are distinct. The denominator is 1461^n, since each person can have any birthday within the four-year cycle. Putting this all together, we see that the probability that there are at least two people with the same birthday is

$$1 - \frac{n \cdot 1460 \cdot 1456 \cdots (1468-4n) + 1460 \cdot 1456 \cdots (1464-4n)}{1461^n}\,.$$

24. There are 16 equally likely outcomes of flipping a fair coin five times in which the first flip comes up tails (each of the other flips can be either heads or tails). Of these only one will result in four heads appearing, namely $THHHH$. Therefore the answer is $1/16$.

26. Intuitively the answer should be yes, because the parity of the number of 1's is a fifty-fifty proposition totally determined by any one of the flips (for example, the last flip). What happened on the other flips is really rather irrelevant. Let us be more rigorous, though. There are 8 bit strings of length 3, and 4 of them contain an odd number of 1's (namely 001, 010, 100, and 111). Therefore $p(E)=4/8=1/2$. Since 4 bit strings of length 3 start with a 1 (namely 100, 101, 110, and 111), we see that $p(F)=4/8=1/2$ as well. Furthermore, since there are 2 strings that start with a 1 and contain an odd number of 1's (namely 100 and 111), we see that $p(E\cap F)=2/8=1/4$. Then since $p(E)\cdot p(F)=(1/2)\cdot(1/2)=1/4=p(E\cap F)$, we conclude from the definition that E and F are independent.

28. These questions are applications of the binomial distribution. Following the lead of King Henry VIII, we call having a boy success. Then $p=0.51$ and $n=5$ for this problem.

a) We are asked for the probability that $k=3$. By Theorem 2 the answer is $C(5,3)0.51^3 0.49^2 \approx 0.32$.

b) There will be at least one boy if there are not all girls. The probability of all girls is 0.49^5, so the answer is $1-0.49^5 \approx 0.972$.

c) This is just like part **(b)**: The probability of all boys is 0.51^5, so the answer is $1-0.51^5 \approx 0.965$.

d) There are two ways this can happen. The answer is clearly $0.51^5+0.49^5 \approx 0.063$.

30. **a)** The probability that all bits are a 1 is $(1/2)^{10}=1/1024$. This is what is being asked for.

b) This is the same as part **(a)**, except that the probability of a 1 bit is 0.6 rather than $1/2$. Thus the answer is $0.6^{10} \approx 0.0060$.

c) We need to multiply the probabilities of each bit being a 1, so the answer is

$$\frac{1}{2}\cdot\frac{1}{2^2}\cdots\frac{1}{2^{10}} = \frac{1}{2^{1+2+\cdots+10}} = \frac{1}{2^{55}} \approx 2.8\times 10^{-17}\,.$$

Note that this is essentially 0.

32. Let E be the event that the bit string begins with a 1, and let F be the event that it ends with 00. In each case we need to calculate the probability $p(E \cup F)$, which is the same as $p(E) + p(F) - p(E) \cdot p(F)$. (The fact that $p(E \cap F) = p(E) \cdot p(F)$ follows from the obvious independence of E and F.) So for each part we will compute $p(E)$ and $p(F)$ and then plug into this formula.

a) We have $p(E) = 1/2$ and $p(F) = (1/2) \cdot (1/2) = 1/4$. Therefore the answer is

$$\frac{1}{2} + \frac{1}{4} - \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}.$$

b) We have $p(E) = 0.6$ and $p(F) = (0.4) \cdot (0.4) = 0.16$. Therefore the answer is

$$0.6 + 0.16 - 0.6 \cdot 0.16 = 0.664.$$

c) We have $p(E) = 1/2$ and

$$p(F) = (1 - \frac{1}{2^9}) \cdot (1 - \frac{1}{2^{10}}) = 1 - \frac{1}{2^9} - \frac{1}{2^{10}} + \frac{1}{2^{19}}.$$

Therefore the answer is

$$\frac{1}{2} + 1 - \frac{1}{2^9} - \frac{1}{2^{10}} + \frac{1}{2^{19}} - \frac{1}{2} \cdot (1 - \frac{1}{2^9} - \frac{1}{2^{10}} + \frac{1}{2^{19}}) = 1 - \frac{1}{2^9} + \frac{1}{2^{11}} + \frac{1}{2^{19}} - \frac{1}{2^{20}}.$$

34. We need to use the binomial distribution, which tells us that the probability of k successes is

$$b(k; n, p) = C(n, k)p^k(1-p)^{n-k}.$$

a) Here $k = 0$, since we want all the trials to result in failure. Plugging in and computing, we have $b(0; n, p) = 1 \cdot p^0 \cdot (1-p)^n = (1-p)^n$.

b) There is at least one success if and only if it is not the case that there are no successes. Thus we obtain the answer by subtracting the probability in part **(a)** from 1, namely $1 - (1-p)^n$.

c) There are two ways in which there can be at most one success: no successes or one success. We already computed that the probability of no successes is $(1-p)^n$. Plugging in $k = 1$, we compute that the probability of exactly one success is $b(1; n, p) = n \cdot p^1 \cdot (1-p)^{n-1}$. Therefore the answer is $(1-p)^n + np(1-p)^{n-1}$. This formula only makes sense if $n > 0$, of course; if $n = 0$, then the answer is clearly 1.

d) Since this event is just that the event in part **(c)** does not happen, the answer is $1 - [(1-p)^n + np(1-p)^{n-1}]$. Again, this is for $n > 0$; the probability is clearly 0 if $n = 0$.

36. The basis case here can be taken to be $n = 2$, in which case we have $p(E_1 \cup E_2) = p(E_1) + p(E_2)$. The left-hand side is the sum of $p(x)$ for all $x \in E_1 \cup E_2$. Since E_1 and E_2 are disjoint, this is the sum of $p(x)$ for all $x \in E_1$ added to the sum of $p(x)$ for all $x \in E_2$, which is the right-hand side. Assume the strong inductive hypothesis that the statement is true for $n \le k$, and consider the statement for $n = k+1$, namely $p\left(\bigcup_{i=1}^{k+1} E_i\right) = \sum_{i=1}^{k+1} p(E_i)$. Let $F = \left(\bigcup_{i=1}^{k} E_i\right)$. Then we can rewrite the left-hand side as $p(F \cup E_{k+1})$. By the inductive hypothesis for $n = 2$ (since $F \cap E_{k+1} = \emptyset$) this equals $p(F) + p(E_{k+1})$. Then by the inductive hypothesis for $n = k$ (since the E_i's are pairwise disjoint), this equals $\sum_{i=1}^{k} p(E_i) + p(E_{k+1}) = \sum_{i=1}^{k+1} p(E_i)$, as desired.

38. **a)** We assume that the observer was instructed ahead of time to tell us whether or not at least one die came up 6 and to provide no more information than that. If we do not make such an assumption, then the following analysis would not be valid. We use the notation (i, j) to represent that the first die came up i and the second die came up j. Note that there are 36 equally likely outcomes.

a) Let S be the event that at least one die came up 6, and let T be the event that sum of the dice is 7. We want $p(T \mid S)$. By Definition 3, this equals $p(S \cap T)/p(S)$. The outcomes in $S \cap T$ are $(1, 6)$ and $(6, 1)$, so $p(S \cap T) = 2/36$. There are $5^2 = 25$ outcomes in $\overline{S}$ (five ways to choose what happened on each die), so $p(S) = (36 - 25)/36 = 11/36$. Therefore the answer is $(2/36)/(11/36) = 2/11$.

b) The analysis is exactly the same as in part **(a)**, so the answer is again $2/11$.

40. We assume that n is much greater than k, since otherwise, we could simply compare each element with its successor in the list and know for sure whether or not the list is sorted. We choose two distinct random integers i and j from 1 to n, and we compare the i^{th} and j^{th} elements of the given list; if they are in correct order relative to each other, then we answer "unknown" at this step and proceed. If not, then we answer "true" (i.e., the list is not sorted) and halt. We repeat this for k steps (or until we have found elements out of order), choosing new random indices each time. If we have not found any elements out of order after k steps, we halt and answer "false" (i.e., the original list is probably sorted). Since in a random list the probability that two randomly chosen elements are in correct order relative to each other is $1/2$, the probability that we wrongly answer "false" will be about $1/2^k$ if the list is a random permutation. If k is large, this will be very small; for example, if $k = 100$, then this will be less than one chance in 10^{30}.

SECTION 7.3 Bayes' Theorem

2. We know that $p(E \mid F) = p(E \cap F)/p(F)$, so we need to find those two quantities. We are given $p(F) = 3/4$. To compute $p(E \cap F)$, we can use the fact that $p(E \cap F) = p(E)p(F \mid E)$. We are given that $p(E) = 2/3$ and that $p(F \mid E) = 5/8$; therefore $p(F \cap E) = (2/3)(5/8) = 5/12$. Putting this together, we have $p(E \mid F) = (5/12)/(3/4) = 5/9$.

4. Let F be the event that Ann picks the second box. Thus we know that $p(F) = p(\overline{F}) = 1/2$. Let B be the event that Frida picks an orange ball. Because of the contents of the boxes, we know that $p(B \mid F) = 5/11$ (five of the eleven balls in the second box are orange) and $p(B \mid \overline{F}) = 3/7$. We are asked for $p(F \mid B)$. We use Bayes' theorem:

$$p(F \mid B) = \frac{p(B \mid F)p(F)}{p(B \mid F)p(F) + p(B \mid \overline{F})p(\overline{F})} = \frac{(5/11)(1/2)}{(5/11)(1/2) + (3/7)(1/2)} = \frac{35}{68}$$

6. Let S be the event that a randomly chosen soccer player uses steroids. We know that $p(S) = 0.05$ and therefore $p(\overline{S}) = 0.95$. Let P be the event that a randomly chosen person tests positive for steroid use. We are told that $p(P \mid S) = 0.98$ and $p(P \mid \overline{S}) = 0.12$ (this is a "false positive" test result). We are asked for $p(S \mid P)$. We use Bayes' theorem:

$$p(S \mid P) = \frac{p(P \mid S)p(S)}{p(P \mid S)p(S) + p(P \mid \overline{S})p(\overline{S})} = \frac{(0.98)(0.05)}{(0.98)(0.05) + (0.12)(0.95)} \approx 0.301$$

8. Let D be the event that a randomly chosen person has the rare genetic disease. We are told that $p(D) = 1/10000 = 0.0001$ and therefore $p(\overline{D}) = 0.9999$. Let P be the event that a randomly chosen person tests positive for the disease. We are told that $p(P \mid D) = 0.999$ ("true positive") and that $p(P \mid \overline{D}) = 0.0002$ ("false positive"). From these we can conclude that $p(\overline{P} \mid D) = 0.001$ ("false negative") and $p(\overline{P} \mid \overline{D}) = 0.9998$ ("true negative").

a) We are asked for $p(D \mid P)$. We use Bayes' theorem:

$$p(D \mid P) = \frac{p(P \mid D)p(D)}{p(P \mid D)p(D) + p(P \mid \overline{D})p(\overline{D})} = \frac{(0.999)(0.0001)}{(0.999)(0.0001) + (0.0002)(0.9999)} \approx 0.333$$

b) We are asked for $p(\overline{D} \mid \overline{P})$. We use Bayes' theorem:

$$p(\overline{D} \mid \overline{P}) = \frac{p(\overline{P} \mid \overline{D})p(\overline{D})}{p(\overline{P} \mid \overline{D})p(\overline{D}) + p(\overline{P} \mid D)p(D)} = \frac{(0.9998)(0.9999)}{(0.9998)(0.9999) + (0.001)(0.0001)} \approx 1.000$$

(This last answer is exactly $49985001/49985006 \approx 0.99999989997$.)

10. Let A be the event that a randomly chosen person in the clinic is infected with avian influenza. We are told that $p(A) = 0.04$ and therefore $p(\overline{A}) = 0.96$. Let P be the event that a randomly chosen person tests positive for avian influenza on the blood test. We are told that $p(P \mid A) = 0.97$ and $p(P \mid \overline{A}) = 0.02$ ("false positive"). From these we can conclude that $p(\overline{P} \mid A) = 0.03$ ("false negative") and $p(\overline{P} \mid \overline{A}) = 0.98$.

a) We are asked for $p(A \mid P)$. We use Bayes' theorem:

$$p(A \mid P) = \frac{p(P \mid A)p(A)}{p(P \mid A)p(A) + p(P \mid \overline{A})p(\overline{A})} = \frac{(0.97)(0.04)}{(0.97)(0.04) + (0.02)(0.96)} \approx 0.669$$

b) In part **(a)** we found $p(A \mid P)$. Here we are asked for the probability of the complementary event (given a positive test result). Therefore we have simply $p(\overline{A} \mid P) = 1 - p(A \mid P) \approx 1 - 0.669 = 0.331$.

c) We are asked for $p(A \mid \overline{P})$. We use Bayes' theorem:

$$p(A \mid \overline{P}) = \frac{p(\overline{P} \mid A)p(A)}{p(\overline{P} \mid A)p(A) + p(\overline{P} \mid \overline{A})p(\overline{A})} = \frac{(0.03)(0.04)}{(0.03)(0.04) + (0.98)(0.96)} \approx 0.001$$

d) In part **(c)** we found $p(A \mid \overline{P})$. Here we are asked for the probability of the complementary event (given a negative test result). Therefore we have simply $p(\overline{A} \mid \overline{P}) = 1 - p(A \mid \overline{P}) \approx 1 - 0.001 = 0.999$.

12. Let E be the event that a 0 was received; let F_1 be the event that a 0 was sent; and let F_2 be the event that a 1 was sent. Note that $F_2 = \overline{F}_1$. Then we are told that $p(F_2) = 1/3$, $p(F_1) = 2/3$, $p(E \mid F_1) = 0.9$, and $p(E \mid F_2) = 0.2$.

a) $p(E) = p(E \mid F_1)p(F_1) + p(E \mid F_2)p(F_2) = 0.9 \cdot (2/3) + 0.2 \cdot (1/3) = 2/3$.

b) We use Bayes' theorem:

$$p(F_1 \mid E) = \frac{p(E \mid F_1)p(F_1)}{p(E \mid F_1)p(F_1) + p(E \mid F_2)p(F_2)} = \frac{0.9 \cdot (2/3)}{0.9 \cdot (2/3) + 0.2 \cdot (1/3)} = \frac{0.6}{2/3} = 0.9$$

14. By the generalized version of Bayes' theorem,

$$\begin{aligned} p(F_2 \mid E) &= \frac{p(E \mid F_2)p(F_2)}{p(E \mid F_1)p(F_1) + p(E \mid F_2)p(F_2) + p(E \mid F_3)p(F_3)} \\ &= \frac{(3/8)(1/2)}{(2/7)(1/6) + (3/8)(1/2) + (1/2)(1/3)} = \frac{7}{15}. \end{aligned}$$

16. Let L be the event that Ramesh is late, and let B, C, and O (standing for "omnibus") be the events that he went by bicycle, car, and bus, respectively. We are told that $p(L \mid B) = 0.05$, $p(L \mid C) = 0.50$, and $p(L \mid O) = 0.20$. We are asked to find $p(C \mid L)$.

a) We are to assume here that $p(B) = p(C) = p(O) = 1/3$. Then by the generalized version of Bayes' theorem,

$$\begin{aligned} p(C \mid L) &= \frac{p(L \mid C)p(C)}{p(L \mid B)p(B) + p(L \mid C)p(C) + p(L \mid O)p(O)} \\ &= \frac{(0.50)(1/3)}{(0.05)(1/3) + (0.50)(1/3) + (0.20)(1/3)} = \frac{2}{3}. \end{aligned}$$

b) Now we are to assume here that $p(B) = 0.60$, $p(C) = 0.30$, $p(O) = 0.10$. Then by the generalized version of Bayes' theorem,

$$\begin{aligned} p(C \mid L) &= \frac{p(L \mid C)p(C)}{p(L \mid B)p(B) + p(L \mid C)p(C) + p(L \mid O)p(O)} \\ &= \frac{(0.50)(0.30)}{(0.05)(0.60) + (0.50)(0.30) + (0.20)(0.10)} = \frac{3}{4}. \end{aligned}$$

18. We follow the procedure in Example 3. We first compute that $p(\text{exciting}) = 40/500 = 0.08$ and $q(\text{exciting}) = 25/200 = 0.125$. Then we compute that
$$r(\text{exciting}) = \frac{p(\text{exciting})}{p(\text{exciting}) + q(\text{exciting})} = \frac{0.08}{0.08 + 0.125} \approx 0.390\,.$$
Because $r(\text{exciting})$ is less than the threshold 0.9, an incoming message containing "exciting" would not be rejected.

20. **a)** We follow the procedure in Example 3. In Example 4 we found $p(\text{undervalued}) = 0.1$ and $q(\text{undervalued}) = 0.025$. So we compute that
$$r(\text{undervalued}) = \frac{p(\text{undervalued})}{p(\text{undervalued}) + q(\text{undervalued})} = \frac{0.01}{0.01 + 0.025} \approx 0.286\,.$$
Because $r(\text{undervalued})$ is less than the threshold 0.9, an incoming message containing "undervalued" would not be rejected.
b) This is similar to part **(a)**, where $p(\text{stock}) = 0.2$ and $q(\text{stock}) = 0.06$. Then we compute that
$$r(\text{stock}) = \frac{p(\text{stock})}{p(\text{stock}) + q(\text{stock})} = \frac{0.2}{0.2 + 0.06} \approx 0.769\,.$$
Because $r(\text{stock})$ is less than the threshold 0.9, an incoming message containing "stock" would not be rejected. Notice that each event alone was not enough to cause rejection, but both events together were enough (see Example 4).

22. **a)** Out of a total of $s + h$ messages, s are spam, so $p(S) = s/(s + h)$. Similarly, $p(\overline{S}) = h/(s + h)$.
b) Let W be the event that an incoming message contains the word w. We are told that $p(W \mid S) = p(w)$ and $p(W \mid \overline{S}) = q(w)$. We want to find $p(S \mid W)$. We use Bayes' theorem:
$$p(S \mid W) = \frac{p(W \mid S)p(S)}{p(W \mid S)p(S) + p(W \mid \overline{S})p(\overline{S})} = \frac{p(w)\frac{s}{(s+h)}}{p(w)\frac{s}{(s+h)} + q(w)\frac{h}{(s+h)}} = \frac{p(w)s}{p(w)s + q(w)h}$$
The assumption made in this section was that $s = h$, so those factors cancel out of this answer to give the formula for $r(w)$ obtained in the text.

SECTION 7.4 Expected Value and Variance

2. By Theorem 2 the expected number of successes for n Bernoulli trials is np. In the present problem we have $n = 10$ and $p = 1/2$. Therefore the expected number of successes (i.e., appearances of a head) is $10 \cdot (1/2) = 5$.

4. This is identical to Exercise 2, except that $p = 0.6$. Thus the expected number of heads is $10 \cdot 0.6 = 6$.

6. There are $C(50, 6)$ equally likely possible outcomes when the state picks its winning numbers. The probability of winning \$10 million is therefore $1/C(50, 6)$, and the probability of winning \$0 is $1 - (1/C(50, 6))$. By definition, the expectation is therefore $\$10{,}000{,}000 \cdot 1/C(50, 6) + 0 = \$10{,}000{,}000/15{,}890{,}700 \approx \$0.63$.

8. By Theorem 3 we know that the expectation of a sum is the sum of the expectations. In the current exercise we can let X be the random variable giving the value on the first die, let Y be the random variable giving the value on the second die, and let Z be the random variable giving the value on the third die. In order to compute the expectation of X, of Y, and of Z, we can ignore what happens on the dice not under consideration. Looking just at the first die, then, we compute that the expectation of X is
$$1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3.5\,.$$
Similarly, $E(Y) = 3.5$ and $E(Z) = 3.5$. Therefore $E(X + Y + Z) = 3 \cdot 3.5 = 10.5$.

10. There are 6 different outcomes of our experiment. Let the random variable X be the number of times we flip the coin. For $i = 1, 2, \ldots, 6$, we need to compute the probability that $X = i$. In order for this to happen when $i < 6$, the first $i - 1$ flips must contain exactly one tail, and there are $i - 1$ ways this can happen. Therefore $p(X = i) = (i-1)/2^i$, since there are 2^i equally likely outcomes of i flips. So we have $p(X = 1) = 0$, $p(X = 2) = 1/4$, $p(X = 3) = 2/8 = 1/4$, $p(X = 4) = 3/16$, $p(X = 5) = 4/32 = 1/8$. To compute $p(X = 6)$, we note that this will happen when there is exactly one tail or no tails among the first five flips (probability $5/32 + 1/32 = 6/32 = 3/16$). As a check see that $0 + 1/4 + 1/4 + 3/16 + 1/8 + 3/16 = 1$. We compute the expected number by summing i times $p(X = i)$, so we get $1 \cdot 0 + 2 \cdot 1/4 + 3 \cdot 1/4 + 4 \cdot 3/16 + 5 \cdot 1/8 + 6 \cdot 3/16 = 3.75$.

12. If X is the number of times we roll the die, then X has a geometric distribution with $p = 1/6$.
a) $p(X = n) = (1-p)^{n-1}p = (5/6)^{n-1}(1/6) = 5^{n-1}/6^n$
b) $1/(1/6) = 6$ by Theorem 4

14. We are asked to show that $\sum_{k=1}^{\infty}(1-p)^{k-1}p = \sum_{i=0}^{\infty}(1-p)^i p = 1$. This is a geometric series with initial term p and common ratio $1 - p$, which is less than 1 in absolute value. Therefore the sum converges and equals $p/(1-(1-p)) = 1$.

16. We need to show that $p(X = i \text{ and } Y = j)$ is not always equal to $p(X = i)p(Y = j)$. If we try $i = j = 2$, then we see that the former is 0 (since the sum of the number of heads and the number of tails has to be 2, the number of flips), whereas the latter is $(1/4)(1/4) = 1/16$.

18. Note that by the definition of maximum and the fact that X and Y take on only nonnegative values, $Z(s) \le X(s) + Y(s)$ for every outcome s. Then

$$E(Z) = \sum_{s \in S} p(s)Z(s) \le \sum_{s \in S} p(s)(X(s) + Y(s)) = \sum_{s \in S} p(s)X(s) + \sum_{s \in S} p(s)Y(s) = E(X) + E(Y).$$

20. We proceed by induction on n. If $n = 1$ there is nothing to prove, and the case $n = 2$ is Theorem 5. Assume that the equality holds for n, and consider $E\left(\prod_{i=1}^{n+1} X_i\right)$. Let $Y = \prod_{i=1}^{n} X_i$. By the inductive hypothesis, $E(Y) = \prod_{i=1}^{n} E(X_i)$. The fact that all the X_i's are mutually independent guarantees that Y and X_{n+1} are independent. Therefore by Theorem 5, $E(YX_{n+1}) = E(Y)E(X_{n+1})$. The result follows.

22. This is basically a matter of applying the definitions:

$$\begin{aligned} E(X) &= \sum_r r \cdot P(X = r) \\ &= \sum_r r \cdot \left(\sum_{j=1}^{n} P(X = r \cap S_j) \right) \\ &= \sum_r r \cdot \left(\sum_{j=1}^{n} P(X = r \mid S_j) \cdot P(S_j) \right) \\ &= \sum_{j=1}^{n} \left(\sum_r r \cdot P(X = r \mid S_j) \right) \cdot P(S_j) \\ &= \sum_{j=1}^{n} E(X \mid S_j) \cdot P(S_j) \end{aligned}$$

24. By definition of expectation we have $E(I_A) = \sum_{s \in S} p(s)I_A(s) = \sum_{s \in A} p(s)$, since $I_A(s)$ is 1 when $s \in A$ and 0 when $s \notin A$. But $\sum_{s \in A} p(s) = p(A)$ by definition.

26. By definition, $E(X) = \sum_{k=1}^{\infty} k \cdot p(X = k)$. Let us write this out and regroup (such regrouping is valid even if the sum is infinite since all the terms are positive):

$$\begin{aligned} E(X) &= p(X=1) + (p(X=2) + p(X=2)) + (p(X=3) + p(X=3) + p(X=3)) + \cdots \\ &= (p(X=1) + p(X=2) + p(X=3) + \cdots) + (p(X=2) + p(X=3) + \cdots) + (p(X=3) + \cdots) + \cdots . \end{aligned}$$

But this is precisely $p(A_1) + p(A_2) + p(A_3) + \cdots$, as desired.

28. In Example 18 we saw that the variance of the number of successes in n Bernoulli trials is npq. Here $n = 10$ and $p = 1/6$ and $q = 5/6$. Therefore the variance is $25/18$.

30. This is an exercise in algebra, using the definitions and theorems of this section. By Theorem 6 the left-hand side is $E(X^2Y^2) - E(XY)^2$, which equals $E(X^2)E(Y^2) - E(X)^2E(Y)^2$ because X and Y are independent. The right-hand side is

$$\begin{aligned} E(X)^2V(Y) + V(X)V(Y) + E(Y)^2V(X) &= V(Y)(E(X)^2 + V(X)) + E(Y)^2V(X) \\ &= (E(Y^2) - E(Y)^2)(E(X)^2 + V(X)) + E(Y)^2V(X) \\ &= E(Y^2)E(X)^2 + E(Y^2)V(X) - E(Y)^2E(X)^2 \\ &= E(Y^2)E(X)^2 + E(Y^2)(E(X^2) - E(X)^2) - E(Y)^2E(X)^2 \\ &= E(Y^2)E(X^2) - E(Y)^2E(X)^2 , \end{aligned}$$

which is the same thing.

32. A dramatic example is to take $Y = -X$. Then the sum of the two random variables is identically 0, so the variance is certainly 0; but the sum of the variances is $2V(X)$, since Y has the same variance as X. For another (more concrete) example, we can take X to be the number of heads when a coin is flipped and Y to be the number of tails. Then by Example 14, $V(X) = V(Y) = 1/4$; but clearly $X+Y = 1$, so $V(X+Y) = 0$.

34. All we really need to do is copy the proof of Theorem 7, replacing sums of two events with sums of n events. The algebra gets only slightly messier. We will use summation notation. Note that by the distributive law we have

$$\left(\sum_{i=1}^{n} a_i\right)^2 = \sum_{i=1}^{n} a_i^2 + 2 \sum_{1 \le i < j \le n} a_i a_j .$$

From Theorem 6 we have

$$V\left(\sum_{i=1}^{n} X_i\right) = E\left(\left(\sum_{i=1}^{n} X_i\right)^2\right) - \left(E\left(\sum_{i=1}^{n} X_i\right)\right)^2 .$$

It follows from algebra and linearity of expectation that

$$\begin{aligned} V\left(\sum_{i=1}^{n} X_i\right) &= E\left(\sum_{i=1}^{n} X_i^2 + 2 \sum_{1 \le i < j \le n} X_i X_j\right) - \left(\sum_{i=1}^{n} E(X_i)\right)^2 \\ &= \sum_{i=1}^{n} E(X_i^2) + 2 \sum_{1 \le i < j \le n} E(X_i X_j) - \sum_{i=1}^{n} E(X_i)^2 - 2 \sum_{1 \le i < j \le n} E(X_i)E(X_j) . \end{aligned}$$

Because the events are pairwise disjoint, by Theorem 5 we have $E(X_iX_j) = E(X_i)E(X_j)$. It follows that

$$V\left(\sum_{i=1}^{n} X_i\right) = \sum_{i=1}^{n} (E(X_i^2) - E(X_i)^2) = \sum_{i=1}^{n} V(X_i) .$$

36. We proceed as in Example 19, applying Chebyshev's inequality with $V(X) = (0.6)(0.4)n = 0.24n$ by Example 18 and $r = \sqrt{n}$. We have $p(|X(s) - E(X)| \geq \sqrt{n}) \leq V(X)/r^2 = (0.24n)/(\sqrt{n})^2 = 0.24$.

38. It is interesting to note that Markov was Chebyshev's student in Russia. One caution—the variance is not 1000 cans; it is 1000 square cans (the units for the variance of X are the square of the units for X). So a measure of how much the number of cans filled per day varies is about the square root of this, or about 31 cans.

a) We have $E(X) = 10{,}000$ and we take $a = 11{,}000$. Then $p(X \geq 11{,}000) \leq 10{,}000/11{,}000 = 10/11$. This is not a terribly good estimate.

b) We apply Theorem 8, with $r = 1000$. The probability that the number of cans filled will differ from the expectation of 10,000 by at least 1000 is at most $1000/1000^2 = 0.001$. Therefore the probability is at least 0.999 that the plant will fill between 9,000 and 11,000 cans. This is also not a very good estimate, since if the number of cans filled per day usually differs by only about 31 from the mean of 10,000, it is virtually impossible that the difference would ever be over 30 times this amount—the probability is much, much less than 1 in 1000.

40. Since

$$\sum_{i=1}^{n} \frac{i}{n(n+1)} = \frac{1}{n(n+1)} \sum_{i=1}^{n} i = \frac{1}{n(n+1)} \frac{n(n+1)}{2} = \frac{1}{2},$$

the probability that the item is not in the list is $1/2$. We know (see Example 8) that if the item is not in the list, then $2n+2$ comparisons are needed; and if the item is the i^{th} item in the list then $2i+1$ comparisons are needed. Therefore the expected number of comparisons is given by

$$\frac{1}{2}(2n+2) + \sum_{i=1}^{n} \frac{i}{n(n+1)}(2i+1).$$

To evaluate the sum, we use not only the fact that $\sum_{i=1}^{n} i = n(n+1)/2$, but also the fact that $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$:

$$\begin{aligned}\frac{1}{2}(2n+2) + \sum_{i=1}^{n} \frac{i}{n(n+1)}(2i+1) &= n+1 + \frac{2}{n(n+1)} \sum_{i=1}^{n} i^2 + \frac{1}{n(n+1)} \sum_{i=1}^{n} i \\ &= n+1 + \frac{2}{n(n+1)} \frac{n(n+1)(2n+1)}{6} + \frac{1}{n(n+1)} \frac{n(n+1)}{2} \\ &= n+1 + \frac{(2n+1)}{3} + \frac{1}{2} = \frac{10n+11}{6}\end{aligned}$$

42. a) Each of the $n!$ permutations occurs with probability $1/n!$, so clearly $E(X)$ is the average number of comparisons, averaged over all these permutations.

b) The summation considers each unordered pair jk once and contributes a 1 if the j^{th} smallest element and the k^{th} smallest element are compared (and contributes 0 otherwise). Therefore the summation counts the number of comparisons, which is what X was defined to be. Note that by the way the algorithm works, the element being compared with at each round is put between the two sublists, so it is never compared with any other elements after that round is finished.

c) Take the expectation of both sides of the equation in part **(b)**. By linearity of expectation we have $E(X) = \sum_{k=2}^{n} \sum_{j=1}^{n-1} E(I_{j,k})$, and $E(I_{j,k})$ is the stated probability by Theorem 2 (with $n = 1$).

d) We prove this by strong induction on n. It is true when $n = 2$, since in this case the two elements are indeed compared once, and $2/(k-j+1) = 2/(2-1+1) = 1$. Assume the inductive hypothesis, and consider the first round of quick sort. Suppose that the element in the first position (the element to be compared this round) is the i^{th} smallest element. If $j < i < k$, then the j^{th} smallest element gets put into the first sublist and the k^{th} smallest element gets put into the second sublist, and so these two elements will never be compared. This happens with probability $(k-j-1)/n$ in a random permutation. If $i = j$ or $i = k$, then the j^{th} smallest element and the k^{th} smallest element will be compared this round. This happens with probability $2/n$. If $i < j$, then both the j^{th} smallest element and the k^{th} smallest element get put into the second sublist and so by induction the probability that they will be compared later on will be $2/(k-j+1)$. Similarly if $i > k$. The probability that $i < j$ is $(j-1)/n$, and the probability that $i > k$ is $(n-k)/n$. Putting this all together, the probability of the desired comparison is

$$0 \cdot \frac{k-j-1}{n} + 1 \cdot \frac{2}{n} + \frac{2}{k-j+1} \cdot \left(\frac{j-1}{n} + \frac{n-k}{n}\right),$$

which after a little algebra simplifies to $2/(k-j+1)$, as desired.

e) From the previous two parts, we need to prove that

$$\sum_{k=2}^{n} \sum_{j-1}^{k-1} \frac{2}{k-j+1} = 2(n+1)\sum_{i=2}^{n} \frac{1}{i} - 2(n-1).$$

This can be done, painfully, by induction.

f) This follows immediately from the previous two parts.

44. We can prove this by doing some algebra on the definition, using the facts (Theorem 3) that the expectation of a sum (or difference) is the sum (or difference) of the expectations and that the expectation of a constant times a random variable equals that constant times the expectation of the random variable:

$$\begin{aligned}\operatorname{Cov}(X,Y) &= E((X-E(X))\cdot(Y-E(Y))) = E(XY - Y\cdot E(X) - X\cdot E(Y) + E(X)\cdot E(Y))\\ &= E(XY) - E(Y)\cdot E(X) - E(X)\cdot E(Y) + E(X)\cdot E(Y) = E(XY) - E(X)\cdot E(Y)\end{aligned}$$

If X and Y are independent, then by Theorem 5 these last two terms are the same, so their difference is 0.

46. We can use the result of Exercise 44. It is easy to see that $E(X) = 7$ and $E(Y) = 7$ (see Example 4). To find the expectation of XY, we construct the following table to show the value of $2i(i+j)$ for the 36 equally-likely outcomes (i is the row label, j the column label):

	1	2	3	4	5	6
1	4	6	8	10	12	14
2	12	16	20	24	28	32
3	24	30	36	42	48	54
4	40	48	56	64	72	80
5	60	70	80	90	100	110
6	84	96	108	120	132	144

The expected value of XY is therefore the sum of these entries divided by 36, namely $1974/36 = 329/6$. Therefore the covariance is $329/6 - 7\cdot 7 = 35/6 \approx 5.8$.

48. Let $X = X_1 + X_2 + \cdots + X_m$, where $X_i = 1$ if the i^{th} ball falls into the first bin and $X_i = 0$ otherwise. Then X is the number of balls that fall into the first bin, so we are being asked to compute $E(X)$. Clearly $E(X_i) = p(X_i = 1) = 1/n$. By linearity of expectation (Theorem 3), the expected number of balls that fall into the first bin is therefore m/n.

SUPPLEMENTARY EXERCISES FOR CHAPTER 7

2. There are $C(56,5)\cdot C(46,1) = 175{,}711{,}536$ possible outcomes of the draw, so that is the denominator for all the fractions giving the desired probabilities. You can check your answers to these exercises with Mega Millions's website: `www.megamillions.com/howto`.

a) There is only one way to win, so the probability of winning is $1/175{,}711{,}536$.

b) There are 45 ways to win in this case (you must not match the sixth ball), so the answer is $45/175{,}711{,}536 \approx 1/3{,}904{,}701$.

c) To match three of the first five balls, there are $C(5,3)$ ways to choose the matching numbers and $C(51,2)$ ways to choose the non-matching numbers; therefore the numerator for this case is $C(5,3)\cdot C(51,2)$. Similarly, matching four of the first five balls but not the sixth ball can be done in $C(5,4)\cdot C(51,1)\cdot 45$ ways. Therefore the answer is

$$\frac{C(5,3)\cdot C(51,2) + C(5,4)\cdot C(51,1)\cdot 45}{C(56,5)\cdot C(46,1)} = \frac{24{,}225}{175{,}711{,}536} \approx \frac{1}{7253}\,.$$

d) To not win a prize requires matching zero, one, or two of the first five numbers, and not matching the sixth number. Therefore the answer is

$$1 - \frac{(C(5,0)\cdot C(51,5) + C(5,1)\cdot C(51,4) + C(5,2)\cdot C(51,3))\cdot 45}{C(59,5)\cdot C(46,1)} = \frac{34{,}961}{1{,}394{,}536} \approx \frac{1}{40}\,.$$

4. There are $C(52,13)$ possible hands. A hand with no pairs must contain exactly one card of each kind. The only choice involved, therefore, is the suit for each of the 13 cards. There are 4 ways to specify the suit, and there are 13 tasks to be performed. Therefore there are 4^{13} hands with no pairs. The probability of drawing such a hand is thus $4^{13}/C(52,13) = 67108864/635013559600 = 4194304/39688347475 \approx 0.000106$.

6. The denominator of each probability is the number of 7-card poker hands, namely $C(52,7) = 133784560$.

a) The number of such hands is $13\cdot 12\cdot 4$, since there are 13 ways to choose the kind for the four, then 12 ways to choose another kind for the three, then $C(4,3) = 4$ ways to choose which three cards of that second kind to use. Therefore the probability is $624/133784560 \approx 4.7\times 10^{-6}$.

b) The number of such hands is $13\cdot 4\cdot 66\cdot 6^2$, since there are 13 ways to choose the kind for the three, $C(4,3) = 4$ ways to choose which three cards of that kind to use, then $C(12,2) = 66$ ways to choose two more kinds for the pairs, then $C(4,2) = 6$ ways to choose which two cards of each of those kinds to use. Therefore the probability is $123552/133784560 \approx 9.2\times 10^{-4}$.

c) The number of such hands is $286\cdot 6^3\cdot 10\cdot 4$, since there are $C(13,3) = 286$ ways to choose the kinds for the pairs, $C(4,2) = 6$ ways to choose which two cards of each of those kinds to use, 10 ways to choose the kind for the singleton, and 4 ways to choose which card of that kind to use. Therefore the probability is $2471040/133784560 \approx 0.018$.

d) The number of such hands is $78\cdot 6^2\cdot 165\cdot 4^3$, since there are $C(13,2) = 78$ ways to choose the kinds for the pairs, $C(4,2) = 6$ ways to choose which two cards of each of those kinds to use, $C(11,3) = 165$ ways to choose the kinds for the singletons, and 4 ways to choose which card of each of those kinds to use. Therefore the probability is $29652480/133784560 \approx 0.22$.

e) The number of such hands is $1716\cdot 4^7$, since there are $C(13,7) = 1716$ ways to choose the kinds and 4 ways to choose which card of each of kind to use. Therefore the probability is $28114944/133784560 \approx 0.21$.

f) The number of such hands is $4\cdot 1716$, since there are 4 ways to choose the suit for the flush and $C(13,7) = 1716$ ways to choose the kinds in that suit. Therefore the probability is $6864/133784560 \approx 5.1\times 10^{-5}$.

g) The number of such hands is $8\cdot 4^7$, since there are 8 ways to choose the kind for the straight to start at (A, 2, 3, 4, 5, 6, 7, or 8) and 4 ways to choose the suit for each kind. Therefore the probability is $131072/133784560 \approx 9.8\times 10^{-4}$.

h) There are only $4 \cdot 8$ straight flushes, since the only choice is the suit and the starting kind (see part **(g)**). Therefore the probability is $32/133784560 \approx 2.4 \times 10^{-7}$.

8. **a)** Each of the outcomes 1 through 12 occurs with probability $1/12$, so the expectation is $(1/12)(1+2+3+\cdots+12) = 13/2$.

b) We compute $V(X) = E(X^2) - E(X)^2 = (1/12)(1^2+2^2+3^2+\cdots+12^2) - (13/2)^2 = (325/6) - (169/4) = 143/12$.

10. **a)** Since expected value is linear, the expected value of the sum is the sum of the expected values, each of which is $13/2$ by Exercise 8a. Therefore the answer is 13.

b) Since variance is linear for independent random variables, and clearly these variables are independent, the variance of the sum is the sum of the variances, each of which is $143/12$ by Exercise 8b. Therefore the answer is $143/6$.

12. **a)** Since expected value is linear, the expected value of the sum is the sum of the expected values, which are $9/2$ by Exercise 7a and $13/2$ by Exercise 8a. Therefore the answer is $(9/2)+(13/2) = 11$.

b) Since variance is linear for independent random variables, and clearly these variables are independent, the variance of the sum is the sum of the variances, which are $21/4$ by Exercise 7b and $143/12$ by Exercise 8b. Therefore the answer is $(21/4)+(143/12) = 103/6$.

14. We need to determine how many positive integers less than $n = pq$ are divisible by either p or q. Certainly the numbers p, $2p$, $3p$, ..., $(q-1)p$ are all divisible by p. This gives $q-1$ numbers. Similarly, $p-1$ numbers are divisible by q. None of these numbers is divisible by both p and q since $lcm(p,q) = pq/\gcd(p,q) = pq/1 = pq = n$. Therefore $p+q-2$ numbers in this range are divisible by p or q, so the remaining $pq-1-(p+q-2) = pq-p-q+1 = (p-1)(q-1)$ are not. Therefore the probability that a randomly chosen integer in this range is not divisible by either p or q is $(p-1)(q-1)/(pq-1)$.

16. Technically a proof by mathematical induction is required, but we will give a somewhat less formal version. We just apply the definition of conditional probability to the right-hand side and observe that practically everything cancels (each denominator with the numerator of the previous term):

$$\begin{aligned}
&p(E_1)p(E_2|E_1)p(E_3|E_1\cap E_2)\cdots p(E_n|E_1\cap E_2\cap\cdots\cap E_{n-1})\\
&\qquad = p(E_1)\cdot\frac{p(E_1\cap E_2)}{p(E_1)}\cdot\frac{p(E_1\cap E_2\cap E_3)}{p(E_1\cap E_2)}\cdots\frac{p(E_1\cap E_2\cap\cdots\cap E_n)}{p(E_1\cap E_2\cap\cdots\cap E_{n-1})}\\
&\qquad = p(E_1\cap E_2\cap\cdots\cap E_n)
\end{aligned}$$

18. If n is odd, then it is impossible, so the probability is 0. If n is even, then there are $C(n,n/2)$ ways that an equal number of heads and tails can appear (choose the flips that will be heads), and 2^n outcomes in all, so the probability is $C(n,n/2)/2^n$.

20. There are 2^{11} bit strings. There are 2^6 palindromic bit strings, since once the first six bits are specified arbitrarily, the remaining five bits are forced. If a bit string is picked at random, then, the probability that it is a palindrome is $2^6/2^{11} = 1/32$.

22. **a)** Since there are b bins, each equally likely to receive the ball, the answer is $1/b$.

b) By linearity of expectation, the fact that n balls are tossed, and the answer to part **(a)**, the answer is n/b.

c) In order for this part to make sense, we ignore n, and assume that the ball supply is unlimited and we keep tossing until the bin contains a ball. The number of tosses then has a geometric distribution with $p = 1/b$ from part **(a)**. The expectation is therefore b.

d) Again we have to assume that the ball supply is unlimited and we keep tossing until every bin contains at least one ball. The analysis is identical to that of Exercise 33 in this set, with b here playing the role of n there. By the solution given there, the answer is $b\sum_{j=1}^{b} 1/j$.

24. a) The intersection of two sets is a subset of each of them, so the largest $p(A \cap B)$ could be would occur when the smaller is a subset of the larger. In this case, that would mean that we want $B \subseteq A$, in which case $A \cap B = B$, so $p(A \cap B) = p(B) = 1/2$. To construct an example, we find a common denominator of the fractions involved, namely 6, and let the sample space consist of 6 equally likely outcomes, say numbered 1 through 6. We let $B = \{1, 2, 3\}$ and $A = \{1, 2, 3, 4\}$. The smallest intersection would occur when $A \cup B$ is as large as possible, since $p(A \cup B) = p(A) + p(B) - p(A \cap B)$. The largest $A \cup B$ could ever be is the entire sample space, whose probability is 1, and that certainly can occur here. So we have $1 = (2/3) + (1/2) - p(A \cap B)$, which gives $p(A \cap B) = 1/6$. To construct an example, again we find a common denominator of these fractions, namely 6, and let the sample space consist of 6 equally likely outcomes, say numbered 1 through 6. We let $A = \{1, 2, 3, 4\}$ and $B = \{4, 5, 6\}$. Then $A \cap B = \{4\}$, and $p(A \cap B) = 1/6$.

b) The largest $p(A \cup B)$ could ever be is 1, which occurs when $A \cup B$ is the entire sample space. As we saw in part **(a)**, that is possible here, using the second example above. The union of two sets is a subset of each of them, so the smallest $p(A \cup B)$ could be would occur when the smaller is a subset of the larger. In this case, that would mean that we want $B \subseteq A$, in which case $A \cup B = A$, so $p(A \cup B) = p(A) = 2/3$. This occurs in the first example given above.

26. From $p(B \mid A) < p(B)$ it follows that $p(A \cap B)/p(A) < p(B)$, which is equivalent to $p(A \cap B) < p(A)p(B)$. Dividing both sides by $p(B)$ and using the fact that then $p(A \mid B) = p(A \cap B)/p(B)$ yields the desired result.

28. For the first interpretation, there are 27 possible situations (out of the $14 \cdot 14 = 196$ possible pairings of gender and birthday of the two children) in which Mr. Smith will have a son born on a Tuesday—14 cases in which the older child is a son born on a Tuesday, and 13 cases in which the older child is not a son born on a Tuesday but the younger child is. In 7 of the first cases and 6 of the second cases, Mr. Smith has two sons. Therefore the answer is $13/27$. For the second interpretation, assume Mr. Smith randomly chose a child and reported its gender and birthday. Then we know nothing about the other child, so the probability that it is a boy is $1/2$ (under the usual assumptions of equal likelihood and independence, which are close to biological truth). Therefore the answer is $1/2$.

30. By Example 6 in Section 7.4, the expected value of X, the number of people who get their own hat back, is 1. By Exercise 43 in that section, the variance of X is also 1. If we apply Chebyshev's inequality (Theorem 8 in Section 7.4) with $r = 10$, we find that the probability that X is greater than or equal to 11 is at most $1/10^2 = 1/100$.

32. In order for the stated outcome to occur, the first $m + n$ trials must result in exactly m successes and n failures, and the $(m+n)^{\text{th}}$ trial must be a success. There are many ways in which this can occur; specifically, there are $C(n + m - 1, n)$ ways to choose which n of the first $n + m - 1$ trials are to be the failures. Each particular sequence has probability $q^n p^m$ of occurring, since the successes occur with probability p and the failures occur with probability q. The answer follows.

34. a) Clearly each assignment has a probability $1/2^n$.

b) The probability that the random assignment of truth values made the first of the two literals in the clause false is $1/2$, and similarly for the second. Since the coin tosses were independent, the probability that both are false is therefore $(1/2)(1/2) = 1/4$, so the probability that the disjunction is true is $1 - (1/4) = 3/4$.

c) By linearity of expectation, the answer is $(3/4)D$.

d) By part **(c)**, averaged over all possible outcomes of the coin flips, 3/4 of the clauses are true. Since the average cannot be greater than all the numbers being averaged, at least 3/4 of the clauses must be true for at least one outcome of the coin tosses.

36. Rather than following the hint, we will give a direct argument. The protocol given here has $n!$ possible outcomes, each equally likely, because there are n possible choices for $r(n)$, $n-1$ possible choices for $r(n-1)$, and so on. Therefore if we can argue that each outcome gives rise to exactly one permutation, then each permutation will be equally likely. But this is clear. Suppose $(a_1, a_2, a_3, \ldots, a_n)$ is a permutation of $(1, 2, 3, \ldots, n)$. In order for this permutation to be generated by the protocol, it must be the case that $r(n) = a_n$, because it is only on round one of the protocol that anything gets moved into the n^{th} position. Next, $r(n-1)$ must the unique value that picks out a_{n-1} to put in the $(n-1)^{\text{st}}$ position (this is not necessarily a_{n-1}, because it might happen that $a_{n-1} = n$, and n could have been put into one of the other positions as a result of round one). And so on. Thus each permutation corresponds to exactly one sequence of choices of the random numbers.

CHAPTER 8
Advanced Counting Techniques

SECTION 8.1 Applications of Recurrence Relations

2. **a)** A permutation of a set with n elements consists of a choice of a first element (which can be done in n ways), followed by a permutation of a set with $n-1$ elements. Therefore $P_n = nP_{n-1}$. Note that $P_0 = 1$, since there is just one permutation of a set with no objects, namely the empty sequence.

b) $P_n = nP_{n-1} = n(n-1)P_{n-2} = \cdots = n(n-1)\cdots 2 \cdot 1 \cdot P_0 = n!$

4. This is similar to Exercise 3 and solved in exactly the same way. The recurrence relation is $a_n = a_{n-1} + a_{n-2} + 2a_{n-5} + 2a_{n-10} + a_{n-20} + a_{n-50} + a_{n-100}$. It would be quite tedious to write down the 100 initial conditions.

6. **a)** Let s_n be the number of such sequences. A string ending in n must consist of a string ending in something less than n, followed by an n as the last term. Therefore the recurrence relation is $s_n = s_{n-1} + s_{n-2} + \cdots + s_2 + s_1$. Here is another approach, with a more compact form of the answer. A sequence ending in n is either a sequence ending in $n-1$, followed by n (and there are clearly s_{n-1} of these), or else it does not contain $n-1$ as a term at all, in which case it is *identical* to a sequence ending in $n-1$ in which the $n-1$ has been replaced by an n (and there are clearly s_{n-1} of these as well). Therefore $s_n = 2s_{n-1}$. Finally we notice that we can derive the second form from the first (or vice versa) algebraically (for example, $s_4 = 2s_3 = s_3 + s_3 = s_3 + s_2 + s_2 = s_3 + s_2 + s_1$).

b) We need two initial conditions if we use the second formulation above, $s_1 = 1$ and $s_2 = 1$ (otherwise, our argument is invalid, because the first and last terms are the same). There is one sequence ending in 1, namely the sequence with just this 1 in it, and there is only the sequence $1, 2$ ending in 2. If we use the first formulation above, then we can get by with just the initial condition $s_1 = 1$.

c) Clearly the solution to this recurrence relation and initial condition is $s_n = 2^{n-2}$ for all $n \geq 2$.

8. This is very similar to Exercise 7, except that we need to go one level deeper.

a) Let a_n be the number of bit strings of length n containing three consecutive 0's. In order to construct a bit string of length n containing three consecutive 0's we could start with 1 and follow with a string of length $n-1$ containing three consecutive 0's, or we could start with a 01 and follow with a string of length $n-2$ containing three consecutive 0's, or we could start with a 001 and follow with a string of length $n-3$ containing three consecutive 0's, or we could start with a 000 and follow with any string of length $n-3$. These four cases are mutually exclusive and exhaust the possibilities for how the string might start. From this analysis we can immediately write down the recurrence relation, valid for all $n \geq 3$: $a_n = a_{n-1} + a_{n-2} + a_{n-3} + 2^{n-3}$.

b) There are no bit strings of length 0, 1, or 2 containing three consecutive 0's, so the initial conditions are $a_0 = a_1 = a_2 = 0$.

c) We will compute a_3 through a_7 using the recurrence relation:

$$a_3 = a_2 + a_1 + a_0 + 2^0 = 0 + 0 + +0 + 1 = 1$$
$$a_4 = a_3 + a_2 + a_1 + 2^1 = 1 + 0 + 0 + 2 = 3$$
$$a_5 = a_4 + a_3 + a_2 + 2^2 = 3 + 1 + 0 + 4 = 8$$
$$a_6 = a_5 + a_4 + a_3 + 2^3 = 8 + 3 + 1 + 8 = 20$$
$$a_7 = a_6 + a_5 + a_4 + 2^4 = 20 + 8 + 3 + 16 = 47$$

Thus there are 47 bit strings of length 7 containing three consecutive 0's.

10. First let us solve this problem without using recurrence relations at all. It is clear that the only strings that do not contain the string 01 are those that consist of a string of 1's follows by a string of 0's. The string can consist of anywhere from 0 to n 1's, so the number of such strings is $n+1$. All the rest have at least one occurrence of 01. Therefore the number of bit strings that contain 01 is $2^n - (n+1)$. However, this approach does not meet the instructions of this exercise.

a) Let a_n be the number of bit strings of length n that contain 01. If we want to construct such a string, we could start with a 1 and follow it with a bit string of length $n-1$ that contains 01, and there are a_{n-1} of these. Alternatively, for any k from 1 to $n-1$, we could start with k 0's, follow this by a 1, and then follow this by any $n-k-1$ bits. For each such k there are 2^{n-k-1} such strings, since the final bits are free. Therefore the number of such strings is $2^0 + 2^1 + 2^2 + \cdots + 2^{n-2}$, which equals $2^{n-1} - 1$. Thus our recurrence relation is $a_n = a_{n-1} + 2^{n-1} - 1$. It is valid for all $n \geq 2$.

b) The initial conditions are $a_0 = a_1 = 0$, since no string of length less than 2 can have 01 in it.

c) We will compute a_2 through a_7 using the recurrence relation:

$$a_2 = a_1 + 2^1 - 1 = 0 + 2 - 1 = 1$$
$$a_3 = a_2 + 2^2 - 1 = 1 + 4 - 1 = 4$$
$$a_4 = a_3 + 2^3 - 1 = 4 + 8 - 1 = 11$$
$$a_5 = a_4 + 2^4 - 1 = 11 + 16 - 1 = 26$$
$$a_6 = a_5 + 2^5 - 1 = 26 + 32 - 1 = 57$$
$$a_7 = a_6 + 2^6 - 1 = 57 + 64 - 1 = 120$$

Thus there are 120 bit strings of length 7 containing 01. Note that this agrees with our nonrecursive analysis, since $2^7 - (7+1) = 120$.

12. This is identical to Exercise 11, one level deeper.

a) Let a_n be the number of ways to climb n stairs. In order to climb n stairs, a person must either start with a step of one stair and then climb $n-1$ stairs (and this can be done in a_{n-1} ways) or else start with a step of two stairs and then climb $n-2$ stairs (and this can be done in a_{n-2} ways) or else start with a step of three stairs and then climb $n-3$ stairs (and this can be done in a_{n-3} ways). From this analysis we can immediately write down the recurrence relation, valid for all $n \geq 3$: $a_n = a_{n-1} + a_{n-2} + a_{n-3}$.

b) The initial conditions are $a_0 = 1$, $a_1 = 1$, and $a_2 = 2$, since there is one way to climb no stairs (do nothing), clearly only one way to climb one stair, and two ways to climb two stairs (one step twice or two steps at once). Note that the recurrence relation is the same as that for Exercise 9.

c) Each term in our sequence $\{a_n\}$ is the sum of the previous three terms, so the sequence begins $a_0 = 1$, $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 7$, $a_5 = 13$, $a_6 = 24$, $a_7 = 44$, $a_8 = 81$. Thus a person can climb a flight of 8 stairs in 81 ways under the restrictions in this problem.

14. a) Let a_n be the number of ternary strings that contain two consecutive 0's. To construct such a string we could start with either a 1 or a 2 and follow with a string containing two consecutive 0's (and this can be done in $2a_{n-1}$ ways), or we could start with 01 or 02 and follow with a string containing two consecutive 0's (and this can be done in $2a_{n-2}$ ways), we could start with 00 and follow with any ternary string of length $n-2$ (of which there are clearly 3^{n-2}). Therefore the recurrence relation, valid for all $n \geq 2$, is $a_n = 2a_{n-1} + 2a_{n-2} + 3^{n-2}$.

b) Clearly $a_0 = a_1 = 0$.

c) We will compute a_2 through a_6 using the recurrence relation:

$$\begin{aligned} a_2 &= 2a_1 + 2a_0 + 3^0 = 2\cdot 0 + 2\cdot 0 + 1 = 1 \\ a_3 &= 2a_2 + 2a_1 + 3^1 = 2\cdot 1 + 2\cdot 0 + 3 = 5 \\ a_4 &= 2a_3 + 2a_2 + 3^2 = 2\cdot 5 + 2\cdot 1 + 9 = 21 \\ a_5 &= 2a_4 + 2a_3 + 3^3 = 2\cdot 21 + 2\cdot 5 + 27 = 79 \\ a_6 &= 2a_5 + 2a_4 + 3^4 = 2\cdot 79 + 2\cdot 21 + 81 = 281 \end{aligned}$$

Thus there are 281 bit strings of length 6 containing two consecutive 0's.

16. a) Let a_n be the number of ternary strings that contain either two consecutive 0's or two consecutive 1's. To construct such a string we could start with a 2 and follow with a string containing either two consecutive 0's or two consecutive 1's, and this can be done in a_{n-1} ways. There are other possibilities, however. For each k from 0 to $n-2$, the string could start with $n-1-k$ alternating 0's and 1's, followed by a 2, and then be followed by a string of length k containing either two consecutive 0's or two consecutive 1's. The number of such strings is $2a_k$, since there are two ways for the initial part to alternate. The other possibility is that the string has no 2's at all. Then it must consist $n-k-2$ alternating 0's and 1's, followed by a pair of 0's or 1's, followed by any string of length k. There are $2\cdot 3^k$ such strings. Now the sum of these quantities as k runs from 0 to $n-2$ is (since this is a geometric progression) $3^{n-1}-1$. Putting this all together, we have the following recurrence relation, valid for all $n \geq 2$: $a_n = a_{n-1} + 2a_{n-2} + 2a_{n-3} + \cdots + 2a_0 + 3^{n-1} - 1$. (By subtracting this recurrence relation from the same relation with $n-1$ substituted for n, we can obtain the following closed form recurrence relation for this problem: $a_n = 2a_{n-1} + a_{n-2} + 2\cdot 3^{n-2}$.)

b) Clearly $a_0 = a_1 = 0$.

c) We will compute a_2 through a_6 using the recurrence relation:

$$\begin{aligned} a_2 &= a_1 + 2a_0 + 3^1 - 1 = 0 + 2\cdot 0 + 3 - 1 = 2 \\ a_3 &= a_2 + 2a_1 + 2a_0 + 3^2 - 1 = 2 + 2\cdot 0 + 2\cdot 0 + 9 - 1 = 10 \\ a_4 &= a_3 + 2a_2 + 2a_1 + 2a_0 + 3^3 - 1 = 10 + 2\cdot 2 + 2\cdot 0 + 2\cdot 0 + 27 - 1 = 40 \\ a_5 &= a_4 + 2a_3 + 2a_2 + 2a_1 + 2a_0 + 3^4 - 1 = 40 + 2\cdot 10 + 2\cdot 2 + 2\cdot 0 + 2\cdot 0 + 81 - 1 = 144 \\ a_6 &= a_5 + 2a_4 + 2a_3 + 2a_2 + 2a_1 + 2a_0 + 3^5 - 1 \\ &= 144 + 2\cdot 40 + 2\cdot 10 + 2\cdot 2 + 2\cdot 0 + 2\cdot 0 + 243 - 1 = 490 \end{aligned}$$

Thus there are 490 ternary strings of length 6 containing two consecutive 0's or two consecutive 1's.

18. a) Let a_n be the number of ternary strings that contain two consecutive symbols that are the same. We will develop a recurrence relation for a_n by exploiting the symmetry among the three symbols. In particular, it must be the case that $a_n/3$ such strings start with each of the three symbols. Now let us see how we might specify a string of length n satisfying the condition. We can choose the first symbol in any of three ways. We can follow this by a string that starts with a different symbol but has in it a pair of consecutive symbols; by what we have just said, there are $2a_{n-1}/3$ such strings. Alternatively, we can follow the initial symbol by another copy of itself and then any string of length $n-2$; there are clearly 3^{n-2} such strings. Thus the recurrence relation is $a_n = 3\cdot((2a_{n-1}/3) + 3^{n-2}) = 2a_{n-1} + 3^{n-1}$. It is valid for all $n \geq 2$.

b) Clearly $a_0 = a_1 = 0$.

c) We will compute a_2 through a_6 using the recurrence relation:

$$\begin{aligned}
a_2 &= 2a_1 + 3^1 = 2 \cdot 0 + 3 = 3 \\
a_3 &= 2a_2 + 3^2 = 2 \cdot 3 + 9 = 15 \\
a_4 &= 2a_3 + 3^3 = 2 \cdot 15 + 27 = 57 \\
a_5 &= 2a_4 + 3^4 = 2 \cdot 57 + 81 = 195 \\
a_6 &= 2a_5 + 3^5 = 2 \cdot 195 + 243 = 633
\end{aligned}$$

Thus there are 633 bit strings of length 6 containing two consecutive 0's, 1's, or 2's.

20. We let a_n be the number of ways to pay a toll of $5n$ cents. (Obviously there is no way to pay a toll that is not a multiple of 5 cents.)

a) This problem is isomorphic to Exercise 11, so the answer is the same: $a_n = a_{n-1} + a_{n-2}$, with $a_0 = a_1 = 1$.

b) Iterating, we find that $a_9 = 55$.

22. **a)** We start by computing the first few terms to get an idea of what's happening. Clearly $R_1 = 2$, since the equator, say, splits the sphere into two hemispheres. Also, $R_2 = 4$ and $R_3 = 8$. Let's try to analyze what happens when the n^{th} great circle is added. It must intersect each of the other circles twice (at diametrically opposite points), and each such intersection results in one prior region being split into two regions, as in Exercise 21. There are $n-1$ previous great circles, and therefore $2(n-1)$ new regions. Therefore $R_n = R_{n-1} + 2(n-1)$. If we impose the initial condition $R_1 = 2$, then our values of R_2 and R_3 found above are consistent with this recurrence. Note that $R_4 = 14$, $R_5 = 22$, and so on.

b) We follow the usual technique, as in Exercise 17 in Section 2.4. In the last line we use the familiar formula for the sum of the first $n-1$ positive integers. Note that the formula agrees with the values computed above.

$$\begin{aligned}
R_n &= 2(n-1) + R_{n-1} \\
&= 2(n-1) + 2(n-2) + R_{n-2} \\
&= 2(n-1) + 2(n-2) + 2(n-3) + R_{n-3} \\
&\ \ \vdots \\
&= 2(n-1) + 2(n-2) + 2(n-3) + 2 \cdot 1 + R_1 \\
&= n(n-1) + 2 = n^2 - n + 2
\end{aligned}$$

24. Let e_n be the number of bit sequences of length n with an even number of 0's. Note that therefore there are $2^n - e_n$ bit sequences with an odd number of 0's. There are two ways to get a bit string of length n with an even number of 0's. It can begin with a 1 and be followed by a bit string of length $n-1$ with an even number of 0's, and there are e_{n-1} of these; or it can begin with a 0 and be followed by a bit string of length $n-1$ with an odd number of 0's, and there are $2^{n-1} - e_{n-1}$ of these. Therefore $e_n = e_{n-1} + 2^{n-1} - e_{n-1}$, or simply $e_n = 2^{n-1}$. See also Exercise 31 in Section 6.4.

26. Let a_n be the number of coverings.

a) We follow the hint. If the right-most domino is positioned vertically, then we have a covering of the left-most $n-1$ columns, and this can be done in a_{n-1} ways. If the right-most domino is positioned horizontally, then there must be another domino directly beneath it, and these together cover the last two columns. The first $n-2$ columns therefore will need to contain a covering by dominoes, and this can be done in a_{n-2} ways. Thus we obtain the Fibonacci recurrence $a_n = a_{n-1} + a_{n-2}$.

b) Clearly $a_1 = 1$ and $a_2 = 2$.

c) The sequence we obtain is just the Fibonacci sequence, shifted by one. The sequence is thus 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, ..., so the answer to this part is 2584.

28. The initial conditions are of course true. We prove the recurrence relation by induction on n, starting with base cases $n = 5$ and $n = 6$, in which cases we find $5f_1 + 3f_0 = 5 = f_5$ and $5f_2 + 3f_1 = 8 = f_6$. Assume the inductive hypothesis. Then we have $5f_{n-4} + 3f_{n-5} = 5(f_{n-5} + f_{n-6}) + 3(f_{n-6} + f_{n-7}) = (5f_{n-5}+3f_{n-6})+(5f_{n-6}+3f_{n-7}) = f_{n-1}+f_{n-2} = f_n$ (we used both the inductive hypothesis and the recursive definition of the Fibonacci numbers). Finally, we prove that f_{5n} is divisible by 5 by induction on n. It is true for $n = 1$, since $f_5 = 5$ is divisible by 5. Assume that it is true for f_{5n}. Then $f_{5(n+1)} = f_{5n+5} = 5f_{5n+1}+3f_{5n}$ is divisible by 5, since both summands in this expression are divisible by 5.

30. **a)** We do this systematically, based on the position of the outermost dot, working from left to right:

$$\begin{gathered}
x_0 \cdot (x_1 \cdot (x_2 \cdot (x_3 \cdot x_4)))\\
x_0 \cdot (x_1 \cdot ((x_2 \cdot x_3) \cdot x_4))\\
x_0 \cdot ((x_1 \cdot x_2) \cdot (x_3 \cdot x_4))\\
x_0 \cdot ((x_1 \cdot (x_2 \cdot x_3)) \cdot x_4)\\
x_0 \cdot (((x_1 \cdot x_2) \cdot x_3) \cdot x_4)\\
(x_0 \cdot x_1) \cdot (x_2 \cdot (x_3 \cdot x_4))\\
(x_0 \cdot x_1) \cdot ((x_2 \cdot x_3) \cdot x_4)\\
(x_0 \cdot (x_1 \cdot x_2)) \cdot (x_3 \cdot x_4)\\
((x_0 \cdot x_1) \cdot x_2) \cdot (x_3 \cdot x_4)\\
(x_0 \cdot (x_1 \cdot (x_2 \cdot x_3))) \cdot x_4\\
(x_0 \cdot ((x_1 \cdot x_2) \cdot x_3)) \cdot x_4\\
((x_0 \cdot x_1) \cdot (x_2 \cdot x_3)) \cdot x_4\\
((x_0 \cdot (x_1 \cdot x_2)) \cdot x_3) \cdot x_4\\
(((x_0 \cdot x_1) \cdot x_2) \cdot x_3) \cdot x_4
\end{gathered}$$

b) We know from Example 5 that $C_0 = 1$, $C_1 = 1$, and $C_3 = 5$. It is also easy to see that $C_2 = 2$, since there are only two ways to parenthesize the product of three numbers. Therefore the recurrence relation tells us that $C_4 = C_0C_3 + C_1C_2 + C_2C_1 + C_3C_0 = 1\cdot 5 + 1\cdot 2 + 2\cdot 1 + 5\cdot 1 = 14$. We have the correct number of solutions listed above.

c) Here $n = 4$, so the formula gives $\frac{1}{5}C(8,4) = \frac{1}{5}\cdot 8\cdot 7\cdot 6\cdot 5/4! = 14$.

32. We let a_n be the number of moves required for this puzzle.

a) In order to move the bottom disk off peg 1, we must have transferred the other $n-1$ disks to peg 3 (since we must move the bottom disk to peg 2); this will require a_{n-1} steps. Then we can move the bottom disk to peg 2 (one more step). Our goal, though, was to move it to peg 3, so now we must move the other $n-1$ disks from peg 3 back to peg 1, leaving the bottom disk quietly resting on peg 2. By symmetry, this again takes a_{n-1} steps. One more step lets us move the bottom disk from peg 2 to peg 3. Now it takes a_{n-1} steps to move the remaining disks from peg 1 to peg 3. So our recurrence relation is $a_n = 3a_{n-1} + 2$. The initial condition is of course that $a_0 = 0$.

b) Computing the first few values, we find that $a_1 = 2$, $a_2 = 8$, $a_3 = 26$, and $a_4 = 80$. It appears that $a_n = 3^n - 1$. This is easily verified by induction: The base case is $a_0 = 3^0 - 1 = 1 - 1 = 0$, and $3a_{n-1} + 2 = 3\cdot(3^{n-1} - 1) + 2 = 3^n - 3 + 2 = 3^n - 1 = a_n$.

c) The only choice in distributing the disks is which peg each disk goes on, since the order of the disks on a given peg is fixed. Since there are three choices for each disk, the answer is 3^n.

d) The puzzle involves $1 + a_n = 3^n$ arrangements of disks during its solution—the initial arrangement and the arrangement after each move. None of these arrangements can repeat a previous arrangement, since if it did so, there would have been no point in making the moves between the two occurrences of the same arrangement. Therefore these 3^n arrangements are all distinct. We saw in part **(c)** that there are exactly 3^n arrangements, so every arrangement was used.

34. If we follow the hint, then it certainly looks as if $J(n) = 2k+1$, where k is the amount left over after the largest possible power of 2 has been subtracted from n (i.e., $n = 2^m + k$ and $k < 2^m$).

36. The basis step is trivial, since when $n = 1 = 2^0 + 0$, the conjecture in Exercise 34 states that $J(n) = 2 \cdot 0 + 1 = 1$, which is correct. For the inductive step, we look at two cases, depending on whether there are an even or an odd number of players. If there are $2n$ players, suppose that $2n = 2^m + k$, as in the hint for Exercise 34. Then k must be even and we can write $n = 2^{m-1} + (k/2)$, and $k/2 < 2^{m-1}$. By the inductive hypothesis, $J(n) = 2(k/2) + 1 = k + 1$. Then by the recurrence relation from Exercise 35, $J(2n) = 2J(n) - 1 = 2(k+1) - 1 = 2k + 1$, as desired. For the other case, assume that there are $2n+1$ players, and again write $2n+1 = 2^m + k$, as in the hint for Exercise 34. Then k must be odd and we can write $n = 2^{m-1} + (k-1)/2$, where $(k-1)/2 < 2^{m-1}$. By the inductive hypothesis, $J(n) = 2((k-1)/2) + 1 = k$. Then by the recurrence relation from Exercise 35, $J(2n+1) = 2J(n) + 1 = 2k + 1$, as desired.

38. Since we can only move one disk at a time, we need one move to lift the smallest disk off the middle disk, and another to lift the middle disk off the largest. Similarly, we need two moves to rejoin these disks. And of course we need at least one move to get the largest disk off peg 1. Therefore we can do no better than five moves. To see that this is possible, we just make the obvious moves (disk 1 is the smallest, and $a \xrightarrow{b} c$ means to move disk b from peg a to peg c: $1 \xrightarrow{1} 2$, $1 \xrightarrow{2} 3$, $1 \xrightarrow{3} 4$, $3 \xrightarrow{2} 4$, $2 \xrightarrow{1} 4$.

40. In our notation (see Exercise 38), disk 1 is the smallest, disk n is the largest, and $a \xrightarrow{b} c$ means to move disk b from peg a to peg c.

a) According to the algorithm, we take $k = 3$, since 5 is between the triangular numbers $t_2 = 3$ and $t_3 = 6$. The moves are to first move $5 - 3 = 2$ disks from peg 1 to peg 2 ($1 \xrightarrow{1} 3$, $1 \xrightarrow{2} 2$, $3 \xrightarrow{1} 2$), then working with pegs 1, 3, and 4 move disks 3, 4, and 5 to peg 4 ($1 \xrightarrow{3} 4$, $1 \xrightarrow{4} 3$, $4 \xrightarrow{3} 3$, $1 \xrightarrow{5} 4$, $3 \xrightarrow{3} 1$, $3 \xrightarrow{4} 4$, $1 \xrightarrow{3} 4$), and then move disks 1 and 2 from peg 2 to peg 4 ($2 \xrightarrow{1} 3$, $2 \xrightarrow{2} 4$, $3 \xrightarrow{1} 4$). Note that this took 13 moves in all.

b) According to the algorithm, we take $k = 3$, since 6 is between the triangular numbers $t_2 = 3$ and $t_3 = 6$. The moves are to first move $6 - 3 = 3$ disks from peg 1 to peg 2 ($1 \xrightarrow{1} 3$, $1 \xrightarrow{2} 4$, $1 \xrightarrow{3} 2$, $4 \xrightarrow{2} 2$, $3 \xrightarrow{1} 2$), then working with pegs 1, 3, and 4 move disks 4, 5, and 6 to peg 4 ($1 \xrightarrow{4} 4$, $1 \xrightarrow{5} 3$, $4 \xrightarrow{4} 3$, $1 \xrightarrow{6} 4$, $3 \xrightarrow{4} 1$, $3 \xrightarrow{5} 4$, $1 \xrightarrow{4} 4$), and then move disks 1, 2, and 3 from peg 2 to peg 4 ($2 \xrightarrow{1} 3$, $2 \xrightarrow{2} 1$, $2 \xrightarrow{3} 4$, $1 \xrightarrow{2} 4$, $3 \xrightarrow{1} 4$). Note that this took 17 moves in all.

c) According to the algorithm, we take $k = 4$, since 7 is between the triangular numbers $t_3 = 6$ and $t_4 = 10$. The moves are to first move $7 - 4 = 3$ disks from peg 1 to peg 2 (five moves, as in part **(b)**), then working with pegs 1, 3, and 4 move disks 4, 5, 6, and 7 to peg 4 (15 moves, using the usual Tower of Hanoi algorithm), and then move disks 1, 2, and 3 from peg 2 to peg 4 (again five moves, as in part **(b)**). Note that this took 25 moves in all.

d) According to the algorithm, we take $k = 4$, since 8 is between the triangular numbers $t_3 = 6$ and $t_4 = 10$. The moves are to first move $8 - 4 = 4$ disks from peg 1 to peg 2 (nine moves, as in Exercise 39, with peg 2 playing the role of peg 4), then working with pegs 1, 3, and 4 move disks 5, 6, 7, and 8 to peg 4 (15 moves, using the usual Tower of Hanoi algorithm), and then move disks 1, 2, 3, and 4 from peg 2 to peg 4 (again nine moves, as above). Note that this took 33 moves in all.

42. To clarify the problem, we note that k is chosen to be the smallest nonnegative integer such that $n \leq k(k+1)/2$. If $n - 1 \neq k(k-1)/2$, then this same value of k applies to $n - 1$ as well; otherwise the value for $n - 1$ is $k - 1$. If $n - 1 \neq k(k-1)/2$, it also follows by subtracting k from both sides of the inequality that the smallest nonnegative integer m such that $n-k \le m(m+1)/2$ is $m=k-1$, so $k-1$ is the value selected by the Frame–Stewart algorithm for $n-k$. Now we proceed by induction, the basis steps being trivial. There are two cases for the inductive step. If $n-1 \ne k(k-1)/2$, then we have from the recurrence relation in Exercise 41 that $R(n) = 2R(n-k) + 2^k - 1$ and $R(n-1) = 2R(n-k-1) + 2^k - 1$. Subtracting yields $R(n) - R(n-1) = 2(R(n-k) - R(n-k-1))$. Since $k-1$ is the value selected for $n-k$, the inductive hypothesis tells us that this difference is $2 \cdot 2^{k-2} = 2^{k-1}$, as desired. On the other hand, if $n-1 = k(k-1)/2$, then $R(n) - R(n-1) = 2R(n-k) + 2^k - 1 - (2R(n-1-(k-1)) + 2^{k-1} - 1 = 2^{k-1}$.

44. Since the Frame–Stewart algorithm solves the puzzle, the number of moves it uses, $R(n)$, is an upper bound to the number of moves needed to solve the puzzle. By Exercise 43 we have a recurrence or formula for these numbers. The table below shows n, the corresponding k and t_k, and $R(n)$.

n	k	t_k	$R(n)$
1	1	1	1
2	2	3	3
3	2	3	5
4	3	6	9
5	3	6	13
6	3	6	17
7	4	10	25
8	4	10	33
9	4	10	41
10	4	10	49
11	5	15	65
12	5	15	81
13	5	15	97
14	5	15	113
15	5	15	129
16	6	21	161
17	6	21	193
18	6	21	225
19	6	21	257
20	6	21	289
21	6	21	321
22	7	28	353
23	7	28	417
24	7	28	481
25	7	28	545

46. **a)** $\nabla a_n = 4 - 4 = 0$ **b)** $\nabla a_n = 2n - 2(n-1) = 2$
c) $\nabla a_n = n^2 - (n-1)^2 = 2n - 1$ **d)** $\nabla a_n = 2^n - 2^{n-1} = 2^{n-1}$

48. This follows immediately (by algebra) from the definition.

50. We prove this by induction on k. The case $k=1$ was Exercise 48. Assume the inductive hypothesis, that a_{n-k} can be expressed in terms of a_n, ∇a_n, $\ldots$, $\nabla^k a_n$, for all n. We will show that $a_{n-(k+1)}$ can be expressed in terms of a_n, ∇a_n, $\ldots$, $\nabla^k a_n$, $\nabla^{k+1} a_n$. Note from the definitions that $a_{n-1} = a_n - \nabla a_n$ and that $\nabla^i a_{n-1} = \nabla^i a_n - \nabla^{i+1} a_n$ for all i. By the inductive hypothesis, we know that $a_{(n-1)-k}$ (which is just $a_{n-(k+1)}$ rewritten) can be expressed as $f(a_{n-1}, \nabla a_{n-1}, \ldots, \nabla^k a_{n-1}) = f(a_n - \nabla a_n, \nabla a_n - \nabla^2 a_n, \ldots, \nabla^k a_n - \nabla^{k+1} a_n)$—exactly what we wished to show. Note that in fact all the equations involved are linear.

52. By Exercise 50, each a_{n-i} can be so expressed (as a linear function), so the entire recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$ can be written as $a_n = c_1f_1 + c_2f_2 + \cdots + c_kf_k$, where each f_i is a linear expression involving a_n, ∇a_n, ..., $\nabla^k a_n$. This gives us the desired difference equation.

54. This problem was solved in Exercise 55.

56. **a)** If all the terms are nonnegative, then the more terms we have, the larger the sum. A sequence such as $5, -2$ shows that the maximum might not be achieved by taking all the terms if some are negative; in this example the maximum is achieved by taking just the first term, and taking all the terms gives a smaller sum.

b) If the string of consecutive terms must end at a_k, then either it consists just of a_k or it consists of a string of consecutive terms ending at a_{k-1} followed by a_k. If we want the largest such sum in the second case, then we must take the largest sum of consecutive terms ending at a_{k-1}. Therefore the given recurrence relation must hold.

c) We compute and store the values $M(k)$ using the recurrence relation in part **(b)**. We could also store, for each k, the starting point of the string of numbers ending at position k that achieves the maximum sum. This would not only give us the sum but also tell us which terms to add to achieve it. Note also that the max function will choose the first argument if and only if $M(k-1)$ is positive (or nonnegative).

```
procedure max sum(a_1, a_2, ..., a_n : real numbers)
M(1) := a_1
for k := 2 to n
        M(k) := max(M(k − 1) + a_k, a_k)
return M(n)
```

d) The successive values for $M(k)$ are 2, -1 (because $-3+2 > -3$), 4 (because $4 > -1+4$), 5 (because $4+1 > 1$), 3 (because $5+(-2) > -2$), and 6 (because $3+3 > 3$).

e) The algorithm has just the one loop containing a few arithmetic steps, iterated $O(n)$ times.

SECTION 8.2 Solving Linear Recurrence Relations

2. **a)** linear, homogeneous, with constant coefficients; degree 2

b) linear with constant coefficients but not homogeneous

c) not linear

d) linear, homogeneous, with constant coefficients; degree 3

e) linear and homogeneous, but not with constant coefficients

f) linear with constant coefficients, but not homogeneous

g) linear, homogeneous, with constant coefficients; degree 7

4. For each problem, we first write down the characteristic equation and find its roots. Using this we write down the general solution. We then plug in the initial conditions to obtain a system of linear equations. We solve these equations to determine the arbitrary constants in the general solution, and finally we write down the unique answer.

a) $r^2 - r - 6 = 0 \qquad r = -2, 3$

$$a_n = \alpha_1(-2)^n + \alpha_2 3^n$$

$$3 = \alpha_1 + \alpha_2$$

$$6 = -2\alpha_1 + 3\alpha_2$$

$$\alpha_1 = 3/5 \qquad \alpha_2 = 12/5$$

$$a_n = (3/5)(-2)^n + (12/5)3^n$$

b) $r^2 - 7r + 10 = 0 \qquad r = 2, 5$

$$a_n = \alpha_1 2^n + \alpha_2 5^n$$
$$2 = \alpha_1 + \alpha_2$$
$$1 = 2\alpha_1 + 5\alpha_2$$
$$\alpha_1 = 3 \qquad \alpha_2 = -1$$
$$a_n = 3 \cdot 2^n - 5^n$$

c) $r^2 - 6r + 8 = 0 \qquad r = 2, 4$
$$a_n = \alpha_1 2^n + \alpha_2 4^n$$
$$4 = \alpha_1 + \alpha_2$$
$$10 = 2\alpha_1 + 4\alpha_2$$
$$\alpha_1 = 3 \qquad \alpha_2 = 1$$
$$a_n = 3 \cdot 2^n + 4^n$$

d) $r^2 - 2r + 1 = 0 \qquad r = 1, 1$
$$a_n = \alpha_1 1^n + \alpha_2 n 1^n = \alpha_1 + \alpha_2 n$$
$$4 = \alpha_1$$
$$1 = \alpha_1 + \alpha_2$$
$$\alpha_1 = 4 \qquad \alpha_2 = -3$$
$$a_n = 4 - 3n$$

e) $r^2 - 1 = 0 \qquad r = -1, 1$
$$a_n = \alpha_1(-1)^n + \alpha_2 1^n = \alpha_1(-1)^n + \alpha_2$$
$$5 = \alpha_1 + \alpha_2$$
$$-1 = -\alpha_1 + \alpha_2$$
$$\alpha_1 = 3 \qquad \alpha_2 = 2$$
$$a_n = 3 \cdot (-1)^n + 2$$

f) $r^2 + 6r + 9 = 0 \qquad r = -3, -3$
$$a_n = \alpha_1(-3)^n + \alpha_2 n(-3)^n$$
$$3 = \alpha_1$$
$$-3 = -3\alpha_1 - 3\alpha_2$$
$$\alpha_1 = 3 \qquad \alpha_2 = -2$$
$$a_n = 3(-3)^n - 2n(-3)^n = (3 - 2n)(-3)^n$$

g) $r^2 + 4r - 5 = 0 \qquad r = -5, 1$
$$a_n = \alpha_1(-5)^n + \alpha_2 1^n = \alpha_1(-5)^n + \alpha_2$$
$$2 = \alpha_1 + \alpha_2$$
$$8 = -5\alpha_1 + \alpha_2$$
$$\alpha_1 = -1 \qquad \alpha_2 = 3$$
$$a_n = -(-5)^n + 3$$

6. The model is the recurrence relation $a_n = a_{n-1} + a_{n-2} + a_{n-2} = a_{n-1} + 2a_{n-2}$, with $a_0 = a_1 = 1$ (see the technique of Exercise 19 in Section 8.1). To solve this, we use the characteristic equation $r^2 - r - 2 = 0$, which has roots -1 and 2. Therefore the general solution is $a_n = \alpha_1(-1)^n + \alpha_2 2^n$. Plugging in the initial conditions gives the equations $1 = \alpha_1 + \alpha_2$ and $1 = -\alpha_1 + 2\alpha_2$, which solve to $\alpha_1 = 1/3$ and $\alpha_2 = 2/3$. Therefore in n microseconds $(1/3)(-1)^n + (2/3)2^n$ messages can be transmitted.

8. a) The recurrence relation is, by the definition of average, $L_n = (1/2)L_{n-1} + (1/2)L_{n-2}$.

b) The characteristic equation is $r^2 - (1/2)r - (1/2) = 0$, which gives us $r = -1/2$ and $r = 1$. Therefore the general solution is $L_n = \alpha_1(-1/2)^n + \alpha_2$. Plugging in the initial conditions $L_1 = 100000$ and $L_2 = 300000$ gives $100000 = (-1/2)\alpha_1 + \alpha_2$ and $300000 = (1/4)\alpha_1 + \alpha_2$. Solving these yields $\alpha_1 = 800000/3$ and $\alpha_2 = 700000/3$. Therefore the answer is $L_n = (800000/3)(-1/2)^n + (700000/3)$.

10. The proof may be found in textbooks such as *Introduction to Combinatorial Mathematics* by C. L. Liu (McGraw-Hill, 1968), Chapter 3. It is similar to the proof of Theorem 1.

12. The characteristic equation is $r^3 - 2r^2 - r + 2 = 0$. This factors as $(r-1)(r+1)(r-2) = 0$, so the roots are 1, -1, and 2. Therefore the general solution is $a_n = \alpha_1 + \alpha_2(-1)^n + \alpha_3 2^n$. Plugging in initial conditions gives $3 = \alpha_1 + \alpha_2 + \alpha_3$, $6 = \alpha_1 - \alpha_2 + 2\alpha_3$, and $0 = \alpha_1 + \alpha_2 + 4\alpha_3$. The solution to this system of equations is $\alpha_1 = 6$, $\alpha_2 = -2$, and $\alpha_3 = -1$. Therefore the answer is $a_n = 6 - 2(-1)^n - 2^n$.

14. The characteristic equation is $r^4 - 5r^2 + 4 = 0$. This factors as $(r^2-1)(r^2-4) = (r-1)(r+1)(r-2)(r+2) = 0$, so the roots are 1, -1, 2, and -2. Therefore the general solution is $a_n = \alpha_1 + \alpha_2(-1)^n + \alpha_3 2^n + \alpha_4(-2)^n$. Plugging in initial conditions gives $3 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$, $2 = \alpha_1 - \alpha_2 + 2\alpha_3 - 2\alpha_4$, $6 = \alpha_1 + \alpha_2 + 4\alpha_3 + 4\alpha_4$, and $8 = \alpha_1 - \alpha_2 + 8\alpha_3 - 8\alpha_4$. The solution to this system of equations is $\alpha_1 = \alpha_2 = \alpha_3 = 1$ and $\alpha_4 = 0$. Therefore the answer is $a_n = 1 + (-1)^n + 2^n$.

16. This requires some linear algebra, but follows the same basic idea as the proof of Theorem 1. See textbooks such as *Introduction to Combinatorial Mathematics* by C. L. Liu (McGraw-Hill, 1968), Chapter 3.

18. This is a third degree recurrence relation. The characteristic equation is $r^3 - 6r^2 + 12r - 8 = 0$. By the rational root test, the possible rational roots are $\pm 1, \pm 2, \pm 4$. We find that $r = 2$ is a root. Dividing $r-2$ into $r^3 - 6r^2 + 12r - 8$, we find that $r^3 - 6r^2 + 12r - 8 = (r-2)(r^2 - 4r + 4)$. By inspection we factor the rest, obtaining $r^3 - 6r^2 + 12r - 8 = (r-2)^3$. Hence the only root is 2, with multiplicity 3, so the general solution is (by Theorem 4) $a_n = \alpha_1 2^n + \alpha_2 n 2^n + \alpha_3 n^2 2^n$. To find these coefficients, we plug in the initial conditions:

$$\begin{aligned} -5 &= a_0 = \alpha_1 \\ 4 &= a_1 = 2\alpha_1 + 2\alpha_2 + 2\alpha_3 \\ 88 &= a_2 = 4\alpha_1 + 8\alpha_2 + 16\alpha_3 . \end{aligned}$$

Solving this system of equations, we get $\alpha_1 = -5$, $\alpha_2 = 1/2$, and $\alpha_3 = 13/2$. Therefore the answer is $a_n = -5 \cdot 2^n + (n/2) \cdot 2^n + (13n^2/2) \cdot 2^n = -5 \cdot 2^n + n \cdot 2^{n-1} + 13n^2 \cdot 2^{n-1}$.

20. This is a fourth degree recurrence relation. The characteristic polynomial is $r^4 - 8r^2 + 16$, which factors as $(r^2-4)^2$, which then further factors into $(r-2)^2(r+2)^2$. The roots are 2 and -2, each with multiplicity 2. Thus we can write down the general solution as usual: $a_n = \alpha_1 2^n + \alpha_2 n \cdot 2^n + \alpha_3(-2)^n + \alpha_4 n \cdot (-2)^n$.

22. This is similar to Example 6. We can immediately write down the general solution using Theorem 4. In this case there are four distinct roots, so $t = 4$. The multiplicities are 3, 2, 2, and 1. So the general solution is $a_n = (\alpha_{1,0} + \alpha_{1,1}n + \alpha_{1,2}n^2)(-1)^n + (\alpha_{2,0} + \alpha_{2,1}n)2^n + (\alpha_{3,0} + \alpha_{3,1}n)5^n + \alpha_{4,0}7^n$.

24. **a)** We compute the right-hand side of the recurrence relation: $2(n-1)2^{n-1} + 2^n = (n-1)2^n + 2^n = n2^n$, which is the left-hand side.

b) The solution of the associated homogeneous equation $a_n = 2a_{n-1}$ is easily found to be $a_n = \alpha 2^n$. Therefore the general solution of the inhomogeneous equation is $a_n = \alpha 2^n + n2^n$.

c) Plugging in $a_0 = 2$, we obtain $\alpha = 2$. Therefore the solution is $a_n = 2 \cdot 2^n + n2^n = (n+2)2^n$.

26. We need to use Theorem 6, and so we need to find the roots of the characteristic polynomial of the associated homogeneous recurrence relation. The characteristic equation is $r^3 - 6r^2 + 12r - 8 = 0$, and as we saw in Exercise 18, $r = 2$ is the only root, and it has multiplicity 3.

a) Since 1 is not a root of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $p_2 n^2 + p_1 n + p_0$. In the notation of Theorem 6, $s = 1$ here.

b) Since 2 is a root with multiplicity 3 of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $n^3p_0 2^n$.

c) Since 2 is a root with multiplicity 3 of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $n^3(p_1 n + p_0)2^n$.

d) Since -2 is not a root of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $p_0(-2)^n$.

e) Since 2 is a root with multiplicity 3 of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $n^3(p_2n^2 + p_1 n + p_0)2^n$.

f) Since -2 is not a root of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form $(p_3n^3 + p_2n^2 + p_1 n + p_0)(-2)^n$.

g) Since 1 is not a root of the characteristic polynomial of the associated homogeneous recurrence relation, Theorem 6 tells us that the particular solution will be of the form p_0. In the notation of Theorem 6, $s = 1$ here.

28. a) The associated homogeneous recurrence relation is $a_n = 2a_{n-1}$. We easily solve it to obtain $a_n^{(h)} = \alpha 2^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = p_2n^2 + p_1n + p_0$. (Note that $s = 1$ here, and 1 is not a root of the characteristic polynomial.) We plug this into our recurrence relation and obtain $p_2n^2 + p_1n + p_0 = 2(p_2(n-1)^2 + p_1(n-1) + p_0) + 2n^2$. We rewrite this by grouping terms with equal powers of n, obtaining $(-p_2 - 2)n^2 + (4p_2 - p_1)n + (-2p_2 + 2p_1 - p_0) = 0$. In order for this equation to be true for all n, we must have $p_2 = -2$, $4p_2 = p_1$, and $-2p_2 + 2p_1 - p_0 = 0$. This tells us that $p_1 = -8$ and $p_0 = -12$. Therefore the particular solution we seek is $a_n^{(p)} = -2n^2 - 8n - 12$. So the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha 2^n - 2n^2 - 8n - 12$.

b) We plug the initial condition into our solution from part **(a)** to obtain $4 = a_1 = 2\alpha - 2 - 8 - 12$. This tells us that $\alpha = 13$. So the solution is $a_n = 13 \cdot 2^n - 2n^2 - 8n - 12$.

30. a) The associated homogeneous recurrence relation is $a_n = -5a_{n-1} - 6a_{n-2}$. To solve it we find the characteristic equation $r^2 + 5r + 6 = 0$, find that $r = -2$ and $r = -3$ are its solutions, and therefore obtain the homogeneous solution $a_n^{(h)} = \alpha(-2)^n + \beta(-3)^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = c \cdot 4^n$. We plug this into our recurrence relation and obtain $c \cdot 4^n = -5c \cdot 4^{n-1} - 6c \cdot 4^{n-2} + 42 \cdot 4^n$. We divide through by 4^{n-2}, obtaining $16c = -20c - 6c + 42 \cdot 16$, whence with a little simple algebra $c = 16$. Therefore the particular solution we seek is $a_n^{(p)} = 16 \cdot 4^n = 4^{n+2}$. So the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha(-2)^n + \beta(-3)^n + 4^{n+2}$.

b) We plug the initial conditions into our solution from part **(a)** to obtain $56 = a_1 = -2\alpha - 3\beta + 64$ and $278 = a_2 = 4\alpha + 9\beta + 256$. A little algebra yields $\alpha = 1$ and $\beta = 2$. So the solution is $a_n = (-2)^n + 2(-3)^n + 4^{n+2}$.

32. The associated homogeneous recurrence relation is $a_n = 2a_{n-1}$. We easily solve it to obtain $a_n^{(h)} = \alpha 2^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = cn \cdot 2^n$. We plug this into our recurrence relation and obtain $cn \cdot 2^n = 2c(n-1)2^{n-1} + 3 \cdot 2^n$. We divide through by 2^{n-1}, obtaining $2cn = 2c(n-1) + 6$, whence with a little simple algebra $c = 3$. Therefore the particular solution we seek is $a_n^{(p)} = 3n \cdot 2^n$. So the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha 2^n + 3n \cdot 2^n = (3n + \alpha)2^n$.

34. The associated homogeneous recurrence relation is $a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3}$. To solve it we find the characteristic equation $r^3 - 7r^2 + 16r - 12 = 0$. By the rational root test we soon discover that $r = 2$ is a root and factor our equation into $(r-2)^2(r-3) = 0$. Therefore the general solution of the homogeneous relation is $a_n^{(h)} = \alpha 2^n + \beta n \cdot 2^n + \gamma 3^n$. Next we need a particular solution to the given recurrence relation. By Theorem 6 we want to look for a function of the form $a_n = (cn+d)4^n$, since the coefficient of 4^n in our given relation is a linear function of n, and 4 is not a root of the characteristic equation. We plug this into our recurrence relation and obtain $(cn+d)4^n = 7(cn-c+d)4^{n-1} - 16(cn-2c+d)4^{n-2} + 12(cn-3c+d)4^{n-3} + n \cdot 4^n$. We divide through by 4^{n-2}, expand and collect terms (a tedious process, to be sure), obtaining $(c-16)n + (5c+d) = 0$. Therefore $c = 16$ and $d = -80$, so the particular solution we seek is $a_n^{(p)} = (16n-80)4^n$. Thus the general solution is the sum of the homogeneous solution and this particular solution, namely $a_n = \alpha 2^n + \beta n \cdot 2^n + \gamma 3^n + (16n-80)4^n$. Next we plug in the initial conditions to obtain $-2 = a_0 = \alpha + \gamma - 80$, $0 = a_1 = 2\alpha + 2\beta + 3\gamma - 256$, and $5 = a_2 = 4\alpha + 8\beta + 9\gamma - 768$. We solve this system of three linear equations in three unknowns by standard methods to obtain $\alpha = 17$, $\beta = 39/2$, and $\gamma = 61$. So the solution is $a_n = 17 \cdot 2^n + 39n \cdot 2^{n-1} + 61 \cdot 3^n + (16n-80)4^n$. As a check of our work (it would be too much to hope that we could always get this far without making an algebraic error), we can compute a_3 both from the recurrence and from the solution, and we find that $a_3 = 203$ both ways.

36. Obviously the n^{th} term of the sequence comes from the $(n-1)^{\text{st}}$ term by adding n^2; in symbols, $a_{n-1} + n^2 = \left(\sum_{k=1}^{n-1} k^2\right) + n^2 = \sum_{k=1}^{n} k^2 = a_n$. Also, the sum of the first square is clearly 1. To solve this recurrence relation, we easily see that the homogeneous solution is $a_n = \alpha$, so since the nonhomogeneous term is a second degree polynomial, we need a particular solution of the form $a_n = cn^3 + dn^2 + en$. Plugging this into the recurrence relation gives $cn^3 + dn^2 + en = c(n-1)^3 + d(n-1)^2 + e(n-1) + n^2$. Expanding and collecting terms, we have $(3c-1)n^2 + (-3c+2d)n + (c-d+e) = 0$, whence $c = 1/3$, $d = 1/2$, and $e = 1/6$. Thus $a_n^{(h)} = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$. So the general solution is $a_n = \alpha + \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$. It is now a simple matter to plug in the initial condition to see that $\alpha = 0$. Note that we can find a common denominator and write our solution in the familiar form $a_n = n(n+1)(2n+1)/6$, as was noted in Table 2 of Section 2.4 and proved by mathematical induction in Exercise 3 of Section 5.1.

38. **a)** The characteristic equation is $r^2 - 2r + 2 = 0$, whose roots are, by the quadratic formula, $1 \pm \sqrt{-1}$, in other words, $1+i$ and $1-i$.

b) The general solution is, by part **(a)**, $a_n = \alpha_1(1+i)^n + \alpha_2(1-i)^n$. Plugging in the initial conditions gives us $1 = \alpha_1 + \alpha_2$ and $2 = (1+i)\alpha_1 + (1-i)\alpha_2$. Solving these linear equations tells us that $\alpha_1 = \frac{1}{2} - \frac{1}{2}i$ and $\alpha_2 = \frac{1}{2} + \frac{1}{2}i$. Therefore the solution is $a_n = (\frac{1}{2} - \frac{1}{2}i)(1+i)^n + (\frac{1}{2} + \frac{1}{2}i)(1-i)^n$.

40. First we reduce this system to a recurrence relation and initial conditions involving only a_n. If we subtract the two equations, we obtain $a_n - b_n = 2a_{n-1}$, which gives us $b_n = a_n - 2a_{n-1}$. We plug this back into the first equation to get $a_n = 3a_{n-1} + 2(a_{n-1} - 2a_{n-2}) = 5a_{n-1} - 4a_{n-2}$, our desired recurrence relation in one variable. Note also that the first of the original equations gives us the necessary second initial condition, namely $a_1 = 3a_0 + 2b_0 = 7$. We now solve this problem for $\{a_n\}$ in the usual way. The roots of the characteristic equation $r^2 - 5r + 4 = 0$ are 1 and 4, and the solution, after solving for the arbitrary constants, is $a_n = -1 + 2 \cdot 4^n$. Finally, we plug this back into the equation $b_n = a_n - 2a_{n-1}$ to find that $b_n = 1 + 4^n$.

42. We can prove this by induction on n. If $n = 1$, then the assertion is $a_1 = s \cdot f_0 + t \cdot f_1 = s \cdot 0 + t \cdot 1 = t$, which is given; and if $n = 2$, then the assertion is $a_2 = s \cdot f_1 + t \cdot f_2 = s \cdot 1 + t \cdot 1 = s + t$, which is true, since $a_2 = a_1 + a_0 = t + s$. Having taken care of the base cases, we assume the inductive hypothesis, that the statement is true for values less than n. Then $a_n = a_{n-1} + a_{n-2} = (sf_{n-2} + tf_{n-1}) + (sf_{n-3} + tf_{n-2}) = s(f_{n-2} + f_{n-3}) + t(f_{n-1} + f_{n-2}) = sf_{n-1} + tf_n$, as desired.

44. We can compute the first few terms by hand. For $n = 1$, the matrix is just the number 2, so $d_1 = 2$. For

$n = 2$, the matrix is $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, and its determinant is clearly $d_2 = 4 - 1 = 3$. For $n = 3$ the matrix is

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix},$$

and we get $d_3 = 4$ after a little arithmetic. For the general case, our matrix is

$$\mathbf{A}_n = \begin{bmatrix} 2 & 1 & 0 & 0 & \dots & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 \\ 0 & 1 & 2 & 1 & \dots & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 \end{bmatrix}.$$

To compute the determinant, we expand along the top row. This gives us a value of 2 times the determinant of the matrix obtained by deleting the first row and first column minus the determinant of the matrix obtained by deleting the first row and second column. The first of these smaller matrices is just $\mathbf{A}_{n-1}$, with determinant d_{n-1}. The second of these smaller matrices has just one nonzero entry in its first column, so we expand its determinant along the first column and see that it equals d_{n-2}. Therefore our recurrence relation is $d_n = 2d_{n-1} - d_{n-2}$, with initial conditions as computed at the start of this solution. If we compute a few more terms we are led to the conjecture that $d_n = n + 1$. If we show that this satisfies the recurrence, then we have proved that it is indeed the solution. And sure enough, $n + 1 = 2n - (n - 1)$. (Of course, we could have also dragged out the machinery of this section to solve the recurrence relation and initial conditions.)

46. Let a_n represent the number of goats on the island at the start of the n^{th} year.

a) The initial condition is $a_1 = 2$; we are told that at the beginning of the first year there are two goats. During each subsequent year (year n, with $n \geq 2$), the goats who were on the island the year before (year $n - 1$) double in number, and an extra 100 goats are added in. So $a_n = 2a_{n-1} + 100$.

b) The associated homogeneous recurrence relation is $a_n = 2a_{n-1}$, whose solution is $a_n^{(h)} = \alpha 2^n$. The particular solution is a polynomial of degree 0, namely a constant, $a_n = c$. Plugging this into the recurrence relation gives $c = 2c + 100$, whence $c = -100$. So the particular solution is $a_n^{(p)} = -100$ and the general solution is $a_n = \alpha 2^n - 100$. Plugging in the initial condition and solving for α gives us $2 = 2\alpha - 100$, or $\alpha = 51$. Hence the desired formula is $a_n = 51 \cdot 2^n - 100$. There are $51 \cdot 2^n - 100$ goats on the island at the start of the n^{th} year.

c) We are told that $a_1 = 2$, but that is not the relevant initial condition. Instead, since the first two years are special (no goats are removed), the relevant initial condition is $a_2 = 4$. During each subsequent year (year n, with $n \geq 3$), the goats who were on the island the year before (year $n - 1$) double in number, and n goats are removed. So $a_n = 2a_{n-1} - n$. (We assume that the removal occurs after the doubling has occurred; if we assume that the removal takes place first, then we'd have to write $a_n = 2(a_{n-1} - n) = 2a_{n-1} - 2n$.)

d) The associated homogeneous recurrence relation is $a_n = 2a_{n-1}$, whose solution is $a_n^{(h)} = \alpha 2^n$. The particular solution is a polynomial of degree 1, say $a_n = cn + d$. Plugging this into the recurrence relation and grouping like terms gives $(-c + 1)n + (2c - d) = 0$, whence $c = 1$ and $d = 2$. So the particular solution is $a_n^{(p)} = n + 2$ and the general solution is $a_n = \alpha 2^n + n + 2$. Plugging in the initial condition $a_2 = 4$ and solving for α gives us $4 = 4\alpha + 4$, or $\alpha = 0$. Hence the desired formula is simply $a_n = n + 2$ for all $n \geq 2$ (and $a_1 = 2$). There are $n + 2$ goats on the island at the start of the n^{th} year, for all $n \geq 2$.

48. a) This is just a matter of keeping track of what all the symbols mean. First note that $Q(n + 1) = Q(n)f(n)/g(n+1)$. Now the left-hand side of the desired equation is $b_n = g(n+1)Q(n+1)a_n = Q(n)f(n)a_n$. The right-hand side is $b_{n-1} + Q(n)h(n) = g(n)Q(n)a_{n-1} + Q(n)h(n) = Q(n)(g(n)a_{n-1} + h(n))$. That the two sides are the same now follows from the original recurrence relation, $f(n)a_n = g(n)a_{n-1} + h(n)$. Note that the initial condition for $\{b_n\}$ is $b_0 = g(1)Q(1)a_0 = g(1)(1/g(1))a_0 = a_0 = C$, since it is conventional to view an empty product as the number 1.

b) Since $\{b_n\}$ satisfies the trivial recurrence relation shown in part **(a)**, we see immediately that

$$\begin{aligned} b_n &= Q(n)h(n) + b_{n-1} = Q(n)h(n) + Q(n-1)h(n-1) + b_{n-2} = \cdots \\ &= \sum_{i=1}^{n} Q(i)h(i) + b_0 = \sum_{i=1}^{n} Q(i)h(i) + C\,. \end{aligned}$$

The value of a_n follows from the definition of b_n given in part **(a)**.

50. **a)** We can show this by proving that $nC_n - (n+1)C_{n-1} = 2n$, so let us calculate, using the given recurrence:

$$\begin{aligned} nC_n - (n+1)C_{n-1} &= nC_n - (n-1)C_{n-1} - 2C_{n-1} \\ &= n^2 + n + 2\sum_{k=0}^{n-1} C_k - (n-1)\left(n + \frac{2}{n-1}\sum_{k=0}^{n-2} C_k\right) - 2C_{n-1} \\ &= n^2 + n + 2\sum_{k=0}^{n-2} C_k + 2C_{n-1} - n^2 + n - 2\sum_{k=0}^{n-2} C_k \ - 2C_{n-1} = 2n. \end{aligned}$$

b) We use the formula given in Exercise 48. Note first that $f(n) = n$, $g(n) = n+1$, and $h(n) = 2n$. Thus $Q(n) = \dfrac{(n-1)!}{(n+1)!} = \dfrac{1}{n(n+1)}$. Plugging this into the formula gives

$$\frac{0 + \sum_{i=1}^{n} \dfrac{2i}{i(i+1)}}{(n+2)\cdot \dfrac{1}{(n+1)(n+2)}} = 2(n+1)\sum_{i=1}^{n} \frac{1}{i+1}.$$

There is no nice closed form way to write this sum (the harmonic series), but we can check that both this formula and the recurrence yield the same values of C_n for small n (namely, $C_1 = 2$, $C_2 = 5$, $C_3 = 26/3$, and so on).

52. A proof of this theorem can be found in textbooks such as *Discrete Mathematics with Applications* by H. E. Mattson, Jr. (Wiley, 1993), Chapter 11.

SECTION 8.3 Divide-and-Conquer Algorithms and Recurrence Relations

2. The recurrence relation here is $f(n) = 2f(n/2) + 2$, where $f(1) = 0$, since no comparisons are needed for a set with 1 element. Iterating, we find that $f(2) = 2\cdot 0 + 2 = 2$, $f(4) = 2\cdot 2 + 2 = 6$, $f(8) = 2\cdot 6 + 2 = 14$, $f(16) = 2\cdot 14 + 2 = 30$, $f(32) = 2\cdot 30 + 2 = 62$, $f(64) = 2\cdot 62 + 2 = 126$, and $f(128) = 2\cdot 126 + 2 = 254$.

4. In this algorithm we assume that $a = (a_{2n-1}a_{2n-2}\ldots a_1a_0)_2$ and $b = (b_{2n-1}b_{2n-2}\ldots b_1b_0)_2$.

procedure *fast multiply*$(a, b :$ nonnegative integers)
if $a \le 1$ and $b \le 1$ **then return** ab
else
  $A_1 := \lfloor a/2^n \rfloor$
  $A_0 := a - 2^n A_1$
  $B_1 := \lfloor b/2^n \rfloor$
  $B_0 := b - 2^n B_1$
  {we assume that these four numbers have length n; pad if necessary}
  $x :=$ *fast multiply*(A_1, B_1)
  answer := (x shifted left $2n$ places) + (x shifted left n places)
  $x :=$ *fast multiply*(A_0, B_0)
  answer := *answer* + x + (x shifted left n places)
  if $A_1 \ge A_0$ **then** $A_2 := A_1 - A_0$ **else** $A_2 := A_0 - A_1$
  if $B_0 \ge B_1$ **then** $B_2 := B_0 - B_1$ **else** $B_2 := B_1 - B_0$
  $x :=$ *fast multiply*(A_2, B_2) shifted left n places
  if $(A_1 \ge A_0 \wedge B_0 \ge B_1) \vee (A_1 < A_0 \wedge B_0 < B_1)$ **then** *answer* := *answer* + x
  else *answer* := *answer* − x
  return *answer*

6. The recurrence relation is $f(n) = 7f(n/2) + 15n^2/4$, with $f(1) = 1$. Thus we have, iterating, $f(2) = 7\cdot 1 + 15\cdot 2^2/4 = 22$, $f(4) = 7\cdot 22 + 15\cdot 4^2/4 = 214$, $f(8) = 7\cdot 214 + 15\cdot 8^2/4 = 1738$, $f(16) = 7\cdot 1738 + 15\cdot 16^2/4 = 13126$, and $f(32) = 7\cdot 13126 + 15\cdot 32^2/4 = 95{,}722$.

8. a) $f(2) = 2\cdot 5 + 3 = 13$ **b)** $f(4) = 2\cdot 13 + 3 = 29$, $f(8) = 2\cdot 29 + 3 = 61$
c) $f(16) = 2\cdot 61 + 3 = 125$, $f(32) = 2\cdot 125 + 3 = 253$, $f(64) = 2\cdot 253 + 3 = 509$
d) $f(128) = 2\cdot 509 + 3 = 1021$, $f(256) = 2\cdot 1021 + 3 = 2045$, $f(512) = 2\cdot 2045 + 3 = 4093$, $f(1024) = 2\cdot 4093 + 3 = 8189$

10. Since f increases one for each factor of 2 in n, it is clear that $f(2^k) = k + 1$.

12. An exact formula comes from the proof of Theorem 1, namely $f(n) = [f(1) + c/(a-1)]n^{\log_b a} - c/(a-1)$, where $a = 2$, $b = 3$, and $c = 4$ in this exercise. Therefore the answer is $f(n) = 5n^{\log_3 2} - 4$.

14. If there is only one team, then no rounds are needed, so the base case is $R(1) = 0$. Since it takes one round to cut the number of teams in half, we have $R(n) = 1 + R(n/2)$.

16. The solution of this recurrence relation for $n = 2^k$ is $R(2^k) = k$, for the same reason as in Exercise 10.

18. a) Our recursive algorithm will take a sequence of $2n$ names (two different names provided by each of n voters) and determine whether the two top vote-getters occur on our list more than $n/2$ times each, and if so, who they are. We assume that our list has the votes of each voter adjacent (the first voter's choices are in positions 1 and 2, the second voter's choices are in positions 3 and 4, and so on). Note that it is possible for more than two candidates to receive more than $n/2$ votes; for example, three voters could have choices AB, AC, and BC, and then all three would qualify. However, there cannot be more than three candidates qualifying, since the sum of four numbers each larger than $n/2$ is larger than $2n$, the total number of votes cast. If $n = 1$, then the two people on the list are both winners. For the recursive step, divide the list into two parts of even size—the first half and the second half—as equally as possible. As is pointed out in the hint in Exercise 17, no one could have gotten a majority (here that means more than $n/2$ votes) on the whole list without having a majority in one half or the other, since if a candidate got approval from less than or equal to half of the voters in each half, then he got approval from less than or equal to half of the voters in all (this is essentially just the distributive law). Apply the algorithm recursively to each half to come up with at most six names (three from each half). Then run through the entire list to count the number of occurrences of each of those names to decide which, if any, are the winners. This requires at most $12n$ additional comparisons for a list of length $2n$. At the outermost stage of this recursion (i.e., when dealing with the entire list), we have to compare the actual numbers of votes each of the candidates in the running got, since only the top two can be declared winners (subject to the anomaly of three people tied, as illustrated above).

b) We apply the master theorem with $a = 2$, $b = 2$, $c = 12$, and $d = 1$. Since $a = b^d$, we know that the number of comparisons is $O(n^d \log n) = O(n \log n)$.

20. **a)** We compute a^n **mod** m, when n is even, by first computing $y := a^{n/2}$ **mod** m recursively and then doing one modular multiplication, namely $y \cdot y$. When n is odd, we first compute $y := a^{(n-1)/2}$ recursively and then do two multiplications, namely $y \cdot y \cdot a$. So if $f(n)$ is the number of multiplications required, assuming the worst, then we have essentially $f(n) = f(n/2) + 2$.

b) By the master theorem, with $a = 1$, $b = 2$, $c = 2$, and $d = 0$, we see that $f(n)$ is $O(n^0 \log n) = O(\log n)$.

22. **a)** $f(16) = 2f(4) + 4 = 2(2f(2) + 2) + 4 = 2(2 \cdot 1 + 2) + 4 = 12$

b) Let $m = \log n$, so that $n = 2^m$. Also, let $g(m) = f(2^m)$. Then our recurrence becomes $f(2^m) = 2f(2^{m/2}) + m$, since $\sqrt{2^m} = (2^m)^{1/2} = 2^{m/2}$. Rewriting this in terms of g we have $g(m) = 2g(m/2) + m$. Theorem 2 (with $a = 2$, $b = 2$, $c = 1$, and $d = 1$ now tells us that $g(m)$ is $O(m \log m)$. Since $m = \log n$, this says that our function is $O(\log n \cdot \log \log n)$.

24. To carry this down to its base level would require applying the algorithm three times, so we will show only the outermost step. The points are already sorted for us, and so we divide them into two groups, using x coordinate. The left side will have the first four points listed in it (they all have x coordinates less than 2.5), and the right side will have the rest, all of which have x coordinates greater than 2.5. Thus our vertical line will be taken to be $x = 2.5$. Now assume that we have already applied the algorithm recursively to find the minimum distance between two points on the left, and the minimum distance on the right. It turns out that $d_L = \sqrt{2}$ and $d_R = \sqrt{5}$, so $d = \sqrt{2}$. This is achieved by the points $(1,3)$ and $(2,4)$. Thus we want to concentrate on the strip from $x = 2.5 - \sqrt{2} \approx 1.1$ to $x = 2.5 + \sqrt{2} \approx 3.9$ of width $2d$. The only points in this strip are $(2,4)$, $(2,9)$, $(3,1)$, and $(3,5)$, Working from the bottom up, we compute distances from these points to points as much as $d = \sqrt{2} \approx 1.4$ vertical units above them. According to the discussion in the text, there can never be more than seven such computations for each point in the strip. In this case there is in fact only one, namely $\overline{(2,4)(3,5)}$. This distance is again $\sqrt{2}$, and it ties the minimum distance already obtained. So the minimum distance is $\sqrt{2}$.

26. In our algorithm d contains the shortest distance and is the value returned by the algorithm. We assume a function *dist* that computes Euclidean distance given two points (a,b) and (c,d), namely $\sqrt{(a-c)^2 + (b-d)^2}$. We also assume that some global preprocessing has been done to sort the points in nondecreasing order of x coordinates before calling this program, and to produce a separate list P of the points in nondecreasing order of y coordinates, but having an identification as to which points in the original list they are.

procedure $closest((x_1, y_1), \ldots, (x_n, y_n)$: points in the plane)
if $n = 2$ **then** $d := dist((x_1, y_1), (x_2, y_2))$
else
    $m := (x_{\lfloor n/2 \rfloor} + x_{\lceil n/2 \rceil})/2$
    $d_L := closest((x_1, y_1), \ldots, (x_{\lfloor n/2 \rfloor}, y_{\lfloor n/2 \rfloor}))$
    $d_R := closest((x_{\lceil n/2 \rceil}, y_{\lceil n/2 \rceil}), \ldots, (x_n, y_n))$
    $d := \min(d_L, d_R)$
    form the sublist P' of P consisting of those points whose x-coordinates are within d of m
    for each point (x, y) in P'
        for each point (x', y') in P' after (x, y) such that $y' - y < d$
            if $dist((x, y), (x', y')) < d$ then $d := dist((x, y), (x', y'))$
return d $\{d$ is the minimum distance between the points in the list$\}$

28. **a)** We follow the discussion given here. At each stage, we ask the question twice, "Is x in this part of the set?" if the two answers agree, then we know that they are truthful, and we proceed recursively on the half we then know contains the number. If the two answers disagree, then we ask the question a third time to determine the truth (the first person cannot lie twice, so the third answer is truthful). After we have detected the lie, we no longer need to ask each question twice, since all answers have to be truthful. If the lie occurs on our last query, however, then we have used a full $2 \log n + 1$ questions (the last 1 being the third question when the lie was detected).

b) Divide the set into four (nearly) equal-sized parts, A, B, C, and D. To determine which of the four subsets contains the first person's number, ask these questions: "Is your number in $A \cup B$?" and "Is your number in $A \cup C$?" If the answers are both "yes," then we can eliminate D, since we know that at least one of these answers was truthful and therefore the secret number is in $A \cup B \cup C$. By similar reasoning, if both answers are "no," then we can eliminate A; if the answers are first "yes" and then "no," then we can eliminate C; and if the answers are first "no" and then "yes," then we can eliminate B. Therefore after two questions we have a problem of size about $3n/4$ (exactly this when $4 \mid n$).

c) Since we reduce the problem to one problem of size $3n/4$ at each stage, the number $f(n)$ of questions satisfies $f(n) = f(3n/4) + 2$ when n is divisible by 4.

d) Using iteration, we solve the recurrence relation in part **(c)**. We have $f(n) = 2 + f((3/4)n) = 2 + 2 + f((3/4)^2 n) = 2 + 2 + 2 + f((3/4)^3 n) = \cdots = 2 + 2 + \cdots + 2$, where there are about $\log_{4/3} n$ 2's in the sum. Noting that $\log_{4/3} n = \log n / \log 4/3 \approx 2.4 \log n$, we have that $f(n) \approx 4.8 \log n$.

e) The naive way is better, with fewer than half the number of questions. Another way to see this is to observe that after four questions in the second method, the size of our set is down to $9/16$ of its original size, but after only two questions in the first method, the size of the set is even smaller $(1/2)$.

30. The second term obviously dominates the first. Also, $\log_b n$ is just a constant times $\log n$. The statement now follows from the fact that f is increasing.

32. If $a < b^d$, then $\log_b a < d$, so the first term dominates. The statement now follows from the fact that f is increasing.

34. From Exercise 31 (note that here $a = 5$, $b = 4$, $c = 6$, and $d = 1$) we have $f(n) = -24n + 25n^{\log_4 5}$.

36. From Exercise 31 (note that here $a = 8$, $b = 2$, $c = 1$, and $d = 2$) we have $f(n) = -n^2 + 2n^{\log 8} = -n^2 + 2n^3$.

SECTION 8.4 Generating Functions

2. The generating function is $f(x) = 1 + 4x + 16x^2 + 64x^3 + 256x^4$. Since the i^{th} term in this sequence (the coefficient of x^i) is 4^i for $0 \le i \le 4$, we can also write the generating function as

$$f(x) = \sum_{i=0}^{4} (4x)^i = \frac{1-(4x)^5}{1-4x}.$$

4. We will use Table 1 in much of this solution.

a) Apparently all the terms are 0 except for the seven -1's shown. Thus $f(x) = -1-x-x^2-x^3-x^4-x^5-x^6$. This is already in closed form, but we can also write it more compactly as $f(x) = -(1-x^7)/(1-x)$, making use of the identity from Example 2.

b) This sequence fits the pattern in Table 1 for $1/(1-ax)$ with $a = 3$. Therefore the generating function is $1/(1-3x)$.

c) We can factor out $3x^2$ and write the generating function as $3x^2(1-x+x^2-x^3+\cdots) = 3x^2/(1+x)$, again using the identity in Table 1.

d) Except for the extra x (the coefficient of x is 2 rather than 1), the generating function is just $1/(1-x)$. Therefore the answer is $x + (1/(1-x))$.

e) From Table 1, we see that the binomial theorem applies and we can write this as $(1+2x)^7$.

f) We can factor out -3 and write the generating function as $-3(1-x+x^2-x^3+\cdots) = -3/(1+x)$, using the identity in Table 1.

g) We can factor out x and write the generating function as $x(1-2x+4x^2-8x^3+\cdots) = x/(1+2x)$, using the sixth identity in Table 1 with $a = -2$.

h) From Table 1 we see that the generating function here is $1/(1-x^2)$.

6. a) Since the sequence with $a_n = 1$ for all n has generating function $1/(1-x)$, this sequence has generating function $-1/(1-x)$.

b) By Table 1, the generating function for the sequence in which $a_n = 2^n$ for *all* n is $1/(1-2x)$. Here we can either think of subtracting out the missing constant term (since $a_0 = 0$) or factoring out $2x$. Therefore the answer can be written as either $1/(1-2x)-1$ or $2x/(1-2x)$, which are of course algebraically equivalent.

c) We need to split this into two parts. Since we know that the generating function for the sequence $\{n+1\}$ is $1/(1-x)^2$, we write $n-1 = (n+1)-2$. Therefore the generating function is $(1/(1-x)^2) - (2/(1-x))$. We can combine terms and write this function as $(2x-1)/(1-x)^2$, but there is no particular reason to prefer that form in general.

d) The power series for the function e^x is $\sum_{n=0}^{\infty} x^n/n!$. That is almost what we have here; the difference is that the denominator is $(n+1)!$ instead of $n!$. So we have

$$\sum_{n=0}^{\infty} \frac{x^n}{(n+1)!} = \frac{1}{x}\sum_{n=0}^{\infty} \frac{x^{n+1}}{(n+1)!} = \frac{1}{x}\sum_{n=1}^{\infty} \frac{x^n}{n!}$$

by a change of variable. This last sum is $e^x - 1$ (only the first term is missing), so our answer is $(e^x-1)/x$.

e) Let $f(x)$ be the generating function we seek. From Table 1 we know that $1/(1-x)^3 = \sum_{n=0}^{\infty} C(n+2,2)x^n$, and that is almost what we have here. To transform this to $f(x)$ need to factor out x^2 and change the variable of summation:

$$\frac{1}{(1-x)^3} = \sum_{n=0}^{\infty} C(n+2,2)x^n = \frac{1}{x^2}\sum_{n=0}^{\infty} C(n+2,2)x^{n+2} = \frac{1}{x^2}\sum_{n=2}^{\infty} C(n,2)x^n = \frac{1}{x^2}\cdot(f(x)-f(0)-f(1))$$

Noting that $f(0) = f(1) = 0$ by definition, we have $f(x) = x^2/(1-x)^3$.

f) We again use Table 1:

$$\sum_{n=0}^{\infty} C(10,n+1)x^n = \sum_{n=1}^{\infty} C(10,n)x^{n-1} = \frac{1}{x}\sum_{n=1}^{\infty} C(10,n)x^n = \frac{1}{x}((1+x)^{10}-1)$$

8. **a)** By the binomial theorem (the third line of Table 1) we get $a_{2n} = C(3,n)$ for $n = 0, 1, 2, 3$, and the other coefficients are all 0. Alternatively, we could just multiply out this finite polynomial and note the nonzero coefficients: $a_0 = 1$, $a_2 = 3$, $a_4 = 3$, $a_6 = 1$.

b) This is like part **(a)**. First we need to factor out -1 and write this as $-(1-3x)^3$. Then by the binomial theorem (the second line of Table 1) we get $a_n = -C(3,n)(-3)^n$ for $n = 0, 1, 2, 3$, and the other coefficients are all 0. Alternatively, we could (by hand or with *Maple*) just multiply out this finite polynomial and note the nonzero coefficients: $a_0 = -1$, $a_1 = 9$, $a_2 = -27$, $a_3 = 27$.

c) This problem requires a combination of the results of the sixth and seventh identities in Table 1. The coefficient of x^{2n} is 2^n, and the odd coefficients are all 0.

d) We know that $x^2/(1-x)^3 = x^2\sum_{n=0}^{\infty} C(n+2,2)x^n = \sum_{n=0}^{\infty} C(n+2,2)x^{n+2} = \sum_{n=2}^{\infty} C(n,2)x^n$. Therefore $a_n = C(n,2) = n(n-1)/2$ for $n \geq 2$ and $a_0 = a_1 = 0$. (Actually, since $C(0,2) = C(1,2) = 0$, we really don't need to make a special statement for $n < 2$.)

e) The last term gives us, from Table 1, $a_n = 3^n$. We need to adjust this for $n = 0$ and $n = 1$ because of the first two terms. Thus $a_0 = -1 + 3^0 = 0$, and $a_1 = 1 + 3^1 = 4$.

f) We split this into two parts and proceed as in part **(d)**:

$$\begin{aligned}
\frac{1}{(1+x)^3} + \frac{x^3}{(1+x)^3} &= \sum_{n=0}^{\infty}(-1)^n C(n+2,2)x^n + x^3\sum_{n=0}^{\infty}(-1)^n C(n+2,2)x^n \\
&= \sum_{n=0}^{\infty}(-1)^n C(n+2,2)x^n + \sum_{n=0}^{\infty}(-1)^n C(n+2,2)x^{n+3} \\
&= \sum_{n=0}^{\infty}(-1)^n C(n+2,2)x^n + \sum_{n=3}^{\infty}(-1)^{n-3} C(n-1,2)x^n
\end{aligned}$$

Note that n and $n-3$ have opposite parities. Therefore $a_n = (-1)^n C(n+2,2) + (-1)^{n-3}C(n-1,2) = (-1)^n(C(n+2,2) - C(n-1,2)) = (-1)^n 3n$ for $n \geq 3$ and $a_n = (-1)^n C(n+2,2) = (-1)^n(n+2)(n+1)/2$ for $n < 3$. This answer can be confirmed using the `series` command in *Maple*.

g) The key here is to recall the algebraic identity $1 - x^3 = (1-x)(1+x+x^2)$. Therefore the given function can be rewritten as $x(1-x)/(1-x^3)$, which can then be split into $x/(1-x^3)$ plus $-x^2/(1-x^3)$. From Table 1 we know that $1/(1-x^3) = 1 + x^3 + x^6 + x^9 + \cdots$. Therefore $x/(1-x^3) = x + x^4 + x^7 + x^{10} + \cdots$, and $-x^2/(1-x^3) = -x^2 - x^5 - x^8 - x^{11} - \cdots$. Thus we see that a_n is 0 when n is a multiple of 3, it is 1 when n is 1 greater than a multiple of 3, and it is -1 when n is 2 greater than a multiple of 3. One can check this answer with *Maple*.

h) From Table 1 we know that $e^x = 1 + x + x^2/2! + x^3/3! + \cdots$. It follows that

$$e^{3x^2} = 1 + 3x^2 + \frac{(3x^2)^2}{2!} + \frac{(3x^2)^3}{3!} + \cdots.$$

We can therefore read off the coefficients of the generating function for $e^{3x^2} - 1$. First, clearly $a_0 = 0$. Second, $a_n = 0$ when n is odd. Finally, when n is even, we have $a_{2m} = 3^m/m!$.

10. Different approaches are possible for obtaining these answers. One can use brute force algebra and just multiply everything out, either by hand or with computer algebra software such as *Maple*. One can view the problem as asking for the solution to a particular combinatorial problem and solve the problem by other means (e.g., listing all the possibilities). Or one can get a closed form expression for the coefficients, using the generating function theory developed in this section.

a) First we view this combinatorially. By brute force we can list the ten ways to obtain x^9 when this product is multiplied out (where "ijk" means choose an x^i term from the first factor, an x^j term from the second factor, and an x^k term from the third factor): 009, 036, 063, 090, 306, 333, 360, 603, 630, 900. Second, it is clear that we can view this problem as asking for the coefficient of x^3 in $(1+x+x^2+x^3+\cdots)^3$, since each x^3 in the original is playing the role of x here. Since $(1+x+x^2+x^3+\cdots)^3 = 1/(1-x)^3 = \sum_{n=0}^{\infty} C(n+2,2)x^n$, the answer is clearly $C(3+2,2) = C(5,2) = 10$. A third way to get the answer is to ask *Maple* to expand $(1+x^3+x^6+x^9)^3$ and look at the coefficient of x^9, which will turn out to be 10. Note that we don't have to go beyond x^9 in each factor, because the higher terms can't contribute to an x^9 term in the answer.

b) If we factor out x^2 from each factor, we can write this as $x^6(1+x+x^2+\cdots)^3$. Thus we are seeking the coefficient of x^3 in $(1+x+x^2+\cdots)^3 = \sum_{n=0}^{\infty} C(n+2,2)x^n$, so the answer is $C(3+2,2) = 10$. The other two methods explained in part **(a)** work here as well.

c) If we factor out as high a power of x from each factor as we can, then we can write this as

$$x^7(1+x^2+x^3)(1+x)(1+x+x^2+x^3+\cdots)\,,$$

and so we seek the coefficient of x^2 in $(1+x^2+x^3)(1+x)(1+x+x^2+x^3+\cdots)$. We could do this by brute force, but let's try it more analytically. We write our expression in closed form as

$$\frac{(1+x^2+x^3)(1+x)}{1-x} = \frac{1+x+x^2+\text{higher order terms}}{1-x} = \frac{1}{1-x} + x\cdot\frac{1}{1-x} + x^2\cdot\frac{1}{1-x} + \text{irrelevant terms.}$$

The coefficient of x^2 in this power series comes either from the coefficient of x^2 in the first term in the final expression displayed above, or from the coefficient of x^1 in the second factor of the second term of that expression, or from the coefficient of x^0 in the second factor of the third term. Each of these coefficients is 1, so our answer is 3. This could also be confirmed by having *Maple* multiply out ("`expand`") the original expression (truncating the last factor at x^3).

d) The easiest approach here is simply to note that there are only two combinations of terms that will give us an x^9 term in the product: $x\cdot x^8$ and $x^7\cdot x^2$. So the answer is 2.

e) The highest power of x appearing in this expression when multiplied out is x^6. Therefore the answer is 0.

12. These can all be checked by using the `series` command in *Maple*.

a) By Table 1, the coefficient of x^n in this power series is $(-3)^n$. Therefore the answer is $(-3)^{12} = 531{,}441$.

b) By Table 1, the coefficient of x^n in this power series is $2^nC(n+1,1)$. Thus the answer is $2^{12}C(12+1,1) = 53{,}248$.

c) By Table 1, the coefficient of x^n in this power series is $(-1)^nC(n+7,7)$. Therefore the answer is $(-1)^{12}C(12+7,7) = 50{,}388$.

d) By Table 1, the coefficient of x^n in this power series is $4^nC(n+2,2)$. Thus the answer is $4^{12}C(12+2,2) = 1{,}526{,}726{,}656$.

e) This is really asking for the coefficient of x^9 in $1/(1+4x)^2$. Following the same idea as in part **(d)**, we see that the answer is $(-4)^9C(9+1,1) = -2{,}621{,}440$.

14. Each child will correspond to a factor in our generating function. We can give 0, 1, 2, or 3 figures to the child; therefore the generating function for each child is $1+x+x^2+x^3$. We want to find the coefficient of x^{12} in the expansion of $(1+x+x^2+x^3)^5$. We can multiply this out (preferably with a computer algebra package such as *Maple*), and the coefficient of x^{12} turns out to be 35. To solve it analytically, we write our generating function as

$$\left(\frac{1-x^4}{1-x}\right)^5 = \frac{1-5x^4+10x^8-10x^{12}+\text{higher order terms}}{(1-x)^5}.$$

There are four contributions to the coefficient of x^{12}, one for each term in the numerator, from the power series for $1/(1-x)^5$. Since the coefficient of x^n in $1/(1-x)^5$ is $C(n+4,4)$, our answer is $C(12+4,4) - 5C(8+4,4) + 10C(4+4,4) - 10C(0+4,4) = 1820 - 2475 + 700 - 10 = 35$.

16. The factors in the generating function for choosing the egg and plain bagels are both $x^2 + x^3 + x^4 + \cdots$. The factor for choosing the salty bagels is $x^2 + x^3$. Therefore the generating function for this problem is $(x^2 + x^3 + x^4 + \cdots)^2(x^2 + x^3)$. We want to find the coefficient of x^{12}, since we want 12 bagels. This is equivalent to finding the coefficient of x^6 in $(1 + x + x^2 + \cdots)^2(1 + x)$ This function is $(1 + x)/(1 - x)^2$, so we want the coefficient of x^6 in $1/(1 - x)^2$, which is 7, plus the coefficient of x^5 in $1/(1 - x)^2$, which is 6. Thus the answer is 13.

18. Without changing the answer, we can assume that the jar has an infinite number of balls of each color; this will make the algebra easier. For the red and green balls the generating function is $1 + x + x^2 + \cdots$, but for the blue balls the generating function is $x^3 + x^4 + \cdots + x^{10}$, so the generating function for the whole problem is $(1 + x + x^2 + \cdots)^2(x^3 + x^4 + \cdots + x^{10})$. We seek the coefficient of x^{14}. This is the same as the coefficient of x^{11} in

$$(1 + x + x^2 + \cdots)^2(1 + x + \cdots + x^7) = \frac{1 - x^8}{(1 - x)^3}.$$

Since the coefficient of x^n in $1/(1 - x)^3$ is $C(n + 2, 2)$, and we have two contributing terms determined by the numerator, our answer is $C(11 + 2, 2) - C(3 + 2, 2) = 68$.

20. We want the coefficient of x^k to be the number of ways to make change for k pesos. Ten-peso bills contribute 10 each to the exponent of x. Thus we can model the choice of the number of 10-peso bills by the choice of a term from $1 + x^{10} + x^{20} + x^{30} + \cdots$. Twenty-peso bills contribute 20 each to the exponent of x. Thus we can model the choice of the number of 20-peso bills by the choice of a term from $1 + x^{20} + x^{40} + x^{60} + \cdots$. Similarly, 50-peso bills contribute 50 each to the exponent of x, so we can model the choice of the number of 50-peso bills by the choice of a term from $1 + x^{50} + x^{100} + x^{150} + \cdots$. Similar reasoning applies to 100-peso bills. Thus the generating function is $f(x) = (1 + x^{10} + x^{20} + x^{30} + \cdots)(1 + x^{20} + x^{40} + x^{60} + \cdots)(1 + x^{50} + x^{100} + x^{150} + \cdots)(1 + x^{100} + x^{200} + x^{300} + \cdots)$, which can also be written as

$$f(x) = \frac{1}{(1 - x^{10})(1 - x^{20})(1 - x^{50})(1 - x^{100})}$$

by Table 1. Note that $c_k = 0$ unless k is a multiple of 10, and the power series has no terms whose exponents are not powers of 10.

22. Let e_i, for $i = 1, 2, \ldots, n$, be the exponent of x taken from the i^{th} factor in forming a term x^6 in the expansion. Thus $e_1 + e_2 + \cdots + e_n = 6$. The coefficient of x^6 is therefore the number of ways to solve this equation with nonnegative integers, which, from Section 6.5, is $C(n + 6 - 1, 6) = C(n + 5, 6)$. Its value, of course, depends on n.

24. **a)** The restriction on x_1 gives us the factor $x^3 + x^4 + x^5 + \cdots$. The restriction on x_2 gives us the factor $x + x^2 + x^3 + x^4 + x^5$. The restriction on x_3 gives us the factor $1 + x + x^2 + x^3 + x^4$. And the restriction on x_4 gives us the factor $x + x^2 + x^3 + \cdots$. Thus the answer is the product of these:

$$(x^3 + x^4 + x^5 + \cdots)(x + x^2 + x^3 + x^4 + x^5)(1 + x + x^2 + x^3 + x^4)(x + x^2 + x^3 + \cdots)$$

We can use algebra to rewrite this in closed form as $x^5(1 + x + x^2 + x^3 + x^4)^2/(1 - x)^2$.

b) We want the coefficient of x^7 in this series, which is the same as the coefficient of x^2 in the series for

$$\frac{(1 + x + x^2 + x^3 + x^4)^2}{(1 - x)^2} = \frac{1 + 2x + 3x^2 + \text{higher order terms}}{(1 - x)^2}.$$

Since the coefficient of x^n in $1/(1 - x)^2$ is $n + 1$, our answer is $1 \cdot 3 + 2 \cdot 2 + 3 \cdot 1 = 10$.

26. **a)** On each roll, we can get a total of one pip, two pips, ..., six pips. So the generating function for each roll is $x + x^2 + x^3 + x^4 + x^5 + x^6$. The exponent on x gives the number of pips. If we want to achieve a total of k pips in n rolls, then we need the coefficient of x^k in $(x + x^2 + x^3 + x^4 + x^5 + x^6)^n$. Since n is free to vary here, we must add these generating functions for all possible values of n. Therefore the generating function for this problem is $\sum_{n=0}^{\infty}(x + x^2 + x^3 + x^4 + x^5 + x^6)^n$. By the formula for summing a geometric series, this is the same as $1/(1 - (x + x^2 + x^3 + x^4 + x^5 + x^6)) = 1/(1 - x - x^2 - x^3 - x^4 - x^5 - x^6)$.

b) We seek the coefficient of x^8 in the power series for our answer to part **(a)**. The best way to get the answer is probably asking *Maple* or another computer algebra package to find this power series, which it will probably do using calculus. If we do so, the answer turns out to be 125 (the series starts out $1 + x + 2x^2 + 4x^3 + 8x^4 + 16x^5 + 32x^6 + 63x^7 + 125x^8 + 248x^9$).

28. In each case, the generating function for the choice of pennies is $1 + x + x^2 + \cdots = 1/(1 - x)$ or some portion of this to account for restrictions on the number of pennies used. Similarly, the generating function for the choice of nickels is $1 + x^5 + x^{10} + \cdots = 1/(1 - x^5)$ (or some portion); and similarly for the dimes and quarters. For each part we will write down the generating function (a product of the generating functions for each coin) and then invoke a computer algebra system to get the answer.

a) The generating function for the pennies is $1 + x + x^2 + \cdots + x^{10} = (1 - x^{11})/(1 - x)$. Thus our entire generating function is

$$\frac{1 - x^{11}}{1 - x} \cdot \frac{1}{1 - x^5} \cdot \frac{1}{1 - x^{10}} \cdot \frac{1}{1 - x^{25}}\,.$$

Maple says that the coefficient of x^{100} in this is 79.

b) This is just like part **(a)**, except that now the generating function is

$$\frac{1 - x^{11}}{1 - x} \cdot \frac{1 - (x^5)^{11}}{1 - x^5} \cdot \frac{1}{1 - x^{10}} \cdot \frac{1}{1 - x^{25}}\,.$$

This time *Maple* reports that the answer is 58.

c) This problem can be solved by using a generating function with two variables, one for the number of coins (say y) and one for the values (say x). Then the generating function for nickels, for instance, is

$$1 + x^5y + x^{10}y^2 + \cdots = \frac{1}{1 - x^5y}\,.$$

We multiply the four generating functions together, for the four different denominations, and get a function of x and y. Then we ask *Maple* to expand this as a power series and get the coefficient of x^{100}. This coefficient is a polynomial in y. We ask *Maple* to extract and simplify this polynomial and it turns out to be $y^4 + y^6 + 2y^7 + 2y^8 + 2y^9 + 4y^{10}$ plus higher order terms that we don't want, since we need the number of coins (which is what the exponent on y tells us) to be less than 11. Since the total of these coefficients is 12, the answer is 12, which can be confirmed by brute force enumeration.

30. **a)** Multiplication distributes over addition, even when we are talking about infinite sums, so the generating function is just $2G(x)$.

b) What used to be the coefficient of x^0 is now the coefficient of x^1, and similarly for the other terms. The way that happened is that the whole series got multiplied by x. Therefore the generating function for this series is $xG(x)$. In symbols,

$$a_0x + a_1x^2 + a_2x^3 + \cdots = x(a_0 + a_1x + a_2x^2 + \cdots) = xG(x)\,.$$

c) The terms involving a_0 and a_1 are missing; $G(x) - a_0 - a_1x = a_2x^2 + a_3x^3 + \cdots$. Here, however, we want a_2 to be the coefficient of x^4, not x^2 (and similarly for the other powers), so we must throw in an extra factor. Thus the answer is $x^2(G(x) - a_0 - a_1x)$.

d) This is just like part **(c)**, except that we slide the powers down. Thus the answer is $(G(x) - a_0 - a_1x)/x^2$.

e) Following the hint, we differentiate $G(x) = \sum_{n=0}^{\infty} a_n x^n$ to obtain $G'(x) = \sum_{n=0}^{\infty} n\, a_n x^{n-1}$. By a change of variable this becomes $\sum_{n=0}^{\infty}(n+1)a_{n+1}x^n = a_1 + 2a_2x + 3a_3x^2 + \cdots$, which is the generating function for precisely the sequence we are given. Thus $G'(x)$ is the generating function for this sequence.

f) If we look at Theorem 1, it is not hard to see that the sequence shown here is precisely the coefficients of $G(x) \cdot G(x)$.

32. This problem is like Example 16. First let $G(x) = \sum_{k=0}^{\infty} a_k x^k$. Then $xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1}x^k$ (by changing the name of the variable from k to $k+1$). Thus

$$G(x) - 7xG(x) = \sum_{k=0}^{\infty} a_k x^k - \sum_{k=1}^{\infty} 7a_{k-1}x^k = a_0 + \sum_{k=1}^{\infty}(a_k - 7a_{k-1})x^k = a_0 + 0 = 5\,,$$

because of the given recurrence relation and initial condition. Thus $G(x)(1-7x) = 5$, so $G(x) = 5/(1-7x)$. From Table 1 we know then that $a_k = 5 \cdot 7^k$.

34. Let $G(x) = \sum_{k=0}^{\infty} a_k x^k$. Then $xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1}x^k$ (by changing the name of the variable from k to $k+1$). Thus

$$\begin{aligned} G(x) - 3xG(x) &= \sum_{k=0}^{\infty} a_k x^k - \sum_{k=1}^{\infty} 3a_{k-1}x^k = a_0 + \sum_{k=1}^{\infty}(a_k - 3a_{k-1})x^k = 1 + \sum_{k=1}^{\infty} 4^{k-1}x^k \\ &= 1 + x\sum_{k=1}^{\infty} 4^{k-1}x^{k-1} = 1 + x\sum_{k=0}^{\infty} 4^k x^k = 1 + x \cdot \frac{1}{1-4x} = \frac{1-3x}{1-4x}\,. \end{aligned}$$

Thus $G(x)(1-3x) = (1-3x)/(1-4x)$, so $G(x) = 1/(1-4x)$. Therefore $a_k = 4^k$, from Table 1.

36. Let $G(x) = \sum_{k=0}^{\infty} a_k x^k$. Then $xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1}x^k$ (by changing the name of the variable from k to $k+1$), and $x^2G(x) = \sum_{k=0}^{\infty} a_k x^{k+2} = \sum_{k=2}^{\infty} a_{k-2}x^k$. Thus

$$\begin{aligned} G(x) - xG(x) - 2x^2G(x) &= \sum_{k=0}^{\infty} a_k x^k - \sum_{k=1}^{\infty} a_{k-1}x^k - \sum_{k=2}^{\infty} 2a_{k-2}x^k = a_0 + a_1x - a_0x + \sum_{k=2}^{\infty} 2^k \cdot x^k \\ &= 4 + 8x + \frac{1}{1-2x} - 1 - 2x = \frac{4-12x^2}{1-2x}\,, \end{aligned}$$

because of the given recurrence relation, the initial conditions, Table 1, and algebra. Since the left-hand side of this equation factors as $G(x)(1-2x)(1+x)$, we have $G(x) = (4-12x^2)/((1+x)(1-2x)^2)$. At this point we must use partial fractions to break up the denominator. Setting

$$\frac{4-12x^2}{(1+x)(1-2x)^2} = \frac{A}{1+x} + \frac{B}{1-2x} + \frac{C}{(1-2x)^2}\,,$$

multiplying through by the common denominator, and equating coefficients, we find that $A = -8/9$, $B = 38/9$, and $C = 2/3$. Thus

$$G(x) = \frac{-8/9}{1+x} + \frac{38/9}{1-2x} + \frac{2/3}{(1-2x)^2} = \sum_{k=0}^{\infty}\left(-\frac{8}{9}(-1)^k + \frac{38}{9}\cdot 2^k + \frac{2}{3}(k+1)2^k\right)x^k$$

(from Table 1). Therefore $a_k = (-8/9)(-1)^k + (38/9)2^k + (2/3)(k+1)2^k$. Incidentally, it would be wise to check our answers, either with a computer algebra package, or by computing the next term of the sequence from both the recurrence and the formula (here $a_2 = 24$ both ways).

38. Let $G(x) = \sum_{k=0}^{\infty} a_k x^k$. Then $xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1}x^k$ (by changing the name of the variable from k to $k+1$), and similarly $x^2G(x) = \sum_{k=0}^{\infty} a_k x^{k+2} = \sum_{k=2}^{\infty} a_{k-2}x^k$. Thus

$$\begin{aligned} G(x) - 2xG(x) - 3x^2G(x) &= \sum_{k=0}^{\infty} a_k x^k - \sum_{k=1}^{\infty} 2a_{k-1}x^k - \sum_{k=2}^{\infty} 3a_{k-2}x^k = a_0 + a_1x - 2a_0x + \sum_{k=2}^{\infty}(4^k+6)\cdot x^k \\ &= 20 + 20x + \frac{1}{1-4x} + \frac{6}{1-x} - 7 - 10x = 13 + 10x + \frac{1}{1-4x} + \frac{6}{1-x} \\ &= \frac{20 - 80x + 2x^2 + 40x^3}{(1-4x)(1-x)}, \end{aligned}$$

because of the given recurrence relation, the initial conditions, and Table 1. Since the left-hand side of this equation factors as $G(x)(1-3x)(1+x)$, we know that

$$G(x) = \frac{20 - 80x + 2x^2 + 40x^3}{(1-4x)(1-x)(1+x)(1-3x)}.$$

At this point we must use partial fractions to break up the denominator. Setting this last expression equal to

$$\frac{A}{1-4x} + \frac{B}{1-x} + \frac{C}{1+x} + \frac{D}{1-3x},$$

multiplying through by the common denominator, and equating coefficients, we find that $A = 16/5$, $B = -3/2$, $C = 31/20$, and $D = 67/4$. Thus

$$G(x) = \frac{16/5}{1-4x} + \frac{-3/2}{1-x} + \frac{31/20}{1+x} + \frac{67/4}{1-3x} = \sum_{k=0}^{\infty}\left(\frac{16}{5}\cdot 4^k - \frac{3}{2} + \frac{31}{20}(-1)^k + \frac{67}{4}\cdot 3^k\right)x^k$$

(from Table 1). Therefore $a_k = (16/5)4^k - (3/2) + (31/20)(-1)^k + (67/4)3^k$. We check our answer by computing the next term of the sequence from both the recurrence and the formula (here $a_2 = 202$ both ways). Alternatively, we ask *Maple* for the solution:

```
rsolve({a(k) = 2 * a(k - 1) + 3 * a(k - 2) + 4^k + 6, a(0) = 20, a(1) = 60}, a(k));
```

40. **a)** By definition,

$$\begin{aligned} \binom{-1/2}{n} &= \frac{(-1/2)(-3/2)(-5/2)\cdots(-(2n-1)/2)}{n!} \\ &= (-1)^n \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n\, n!} \\ &= (-1)^n \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n\, n!}\cdot\frac{2\cdot 4\cdot 6\cdot(2n)}{2^n\, n!} \\ &= (-1)^n \frac{(2n)!}{n!\, n!\, 4^n} \\ &= (-1)^n \binom{2n}{n}\frac{1}{4^n} = \binom{2n}{n}\frac{1}{(-4)^n} \end{aligned}$$

b) By the extended binomial theorem (Theorem 2), with $-4x$ in place of x and $u = -1/2$, we have

$$(1-4x)^{-1/2} = \sum_{n=0}^{\infty}\binom{-1/2}{n}(-4x)^n = \sum_{n=0}^{\infty}\frac{\binom{2n}{n}}{(-4)^n}(-4x)^n = \sum_{n=0}^{\infty}\binom{2n}{n}x^n.$$

42. First we note, as the hint suggests, that $(1+x)^n = (1+x)(1+x)^{n-1} = (1+x)^{n-1} + x(1+x)^{n-1}$. Expanding both sides of this equality using the binomial theorem, we have

$$\begin{aligned} \sum_{r=0}^{n} C(n,r)x^r &= \sum_{r=0}^{n-1} C(n-1,r)x^r + \sum_{r=0}^{n-1} C(n-1,r)x^{r+1} \\ &= \sum_{r=0}^{n-1} C(n-1,r)x^r + \sum_{r=1}^{n} C(n-1,r-1)x^r. \end{aligned}$$

Thus

$$1 + \left(\sum_{r=1}^{n-1} C(n,r)x^r \right) + x^n = 1 + \left(\sum_{r=1}^{n-1} (C(n-1,r) + C(n-1,r-1))x^r \right) + x^n .$$

Comparing these two expressions, coefficient by coefficient, we see that $C(n,r)$ must equal $C(n-1,r)+C(n-1,r-1)$ for $1 \le r \le n-1$, as desired.

44. Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$ be the generating function for the sequence $\{a_n\}$, where $a_n = 1^2 + 2^2 + 3^2 + \cdots + n^2$.
a) We use the method of generating functions to solve the recurrence relation and initial condition that our sequence satisfies: $a_n = a_{n-1} + n^2$ with $a_0 = 0$ (as in, for example, Exercise 34):

$$G(x) - xG(x) = \sum_{n=0}^{\infty} a_n x^n - \sum_{n=1}^{\infty} a_{n-1} x^n = \sum_{n=0}^{\infty} n^2 x^n .$$

By Exercise 37, the generating function for $\{n^2\}$ is

$$\frac{2}{(1-x)^3} - \frac{3}{(1-x)^2} + \frac{1}{1-x} = \frac{x^2+x}{(1-x)^3} ,$$

so $(1-x)G(x) = (x^2+x)/(1-x)^3$. Dividing both sides by $1-x$ gives the desired expression for $G(x)$.
b) We split the generating function we found for $G(x) = \sum_{n=0}^{\infty} a_n x^n$ into two pieces and use Table 1:

$$\begin{aligned}
\frac{x^2}{(1-x)^4} + \frac{x}{(1-x)^4} &= \sum_{n=0}^{\infty} C(n+3,3)x^{n+2} + \sum_{n=0}^{\infty} C(n+3,3)x^{n+1} \\
&= \sum_{n=0}^{\infty} C(n+1,3)x^n + \sum_{n=0}^{\infty} C(n+2,3)x^n \\
&= \sum_{n=0}^{\infty} \frac{(n+1)n(n-1) + (n+2)(n+1)n}{6} x^n \\
&= \sum_{n=0}^{\infty} \frac{n(n+1)(2n+1)}{6} x^n ,
\end{aligned}$$

as desired. (Note that we did not need to change the limits of summation in line 3 because $C(1,3) = C(2,3) = 0$.)

46. We will make heavy use of the identity $e^x = \displaystyle\sum_{n=0}^{\infty} \frac{1}{n!} x^n$.

a) $\displaystyle\sum_{n=0}^{\infty} \frac{(-2)^n}{n!} x^n = 2\sum_{n=0}^{\infty} \frac{1}{n!}(-2x)^n = e^{-2x}$

b) $\displaystyle\sum_{n=0}^{\infty} \frac{-1}{n!} x^n = -\sum_{n=0}^{\infty} \frac{1}{n!} x^n = -e^x$

c) $\displaystyle\sum_{n=0}^{\infty} \frac{n}{n!} x^n = \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} = x\sum_{n=0}^{\infty} \frac{x^n}{n!} = xe^x$, by a change of variable (This could also be done using calculus.)

d) This generating function can be obtained either with calculus or without. To do it without calculus, write $\displaystyle\sum_{n=0}^{\infty} n(n-1)\frac{x^n}{n!} = \sum_{n=2}^{\infty} \frac{x^n}{(n-2)!} = x^2 \sum_{n=0}^{\infty} \frac{x^n}{n!} = x^2 e^x$, by a change of variable. To do it with calculus, start with $e^x = \displaystyle\sum_{n=0}^{\infty} \frac{x^n}{n!}$ and differentiate both sides twice to obtain $e^x = \displaystyle\sum_{n=0}^{\infty} \frac{n(n-1)}{n!} x^{n-2} = \frac{1}{x^2}\sum_{n=0}^{\infty} n(n-1)\frac{x^n}{n!}$. Therefore $\displaystyle\sum_{n=0}^{\infty} n(n-1)\frac{x^n}{n!} = x^2 e^x$.

e) This generating function can be obtained either with calculus or without. To do it without calculus, write

$$\sum_{n=0}^{\infty} \frac{1}{(n+1)(n+2)} \cdot \frac{x^n}{n!} = \sum_{n=0}^{\infty} \frac{x^n}{(n+2)!} = \frac{1}{x^2} \sum_{n=0}^{\infty} \frac{x^{n+2}}{(n+2)!} = \frac{1}{x^2} \sum_{n=2}^{\infty} \frac{x^n}{n!} = \frac{1}{x^2}(e^x - x - 1).$$

To do it with calculus, integrate $e^s = \sum_{n=0}^{\infty} \frac{s^n}{n!}$ from 0 to t to obtain

$$e^t - 1 = \sum_{n=0}^{\infty} \frac{t^{n+1}}{n+1} \cdot \frac{1}{n!}.$$

Then differentiate again, from 0 to x, to obtain

$$e^x - x - 1 = \sum_{n=0}^{\infty} \frac{x^{n+2}}{(n+2)(n+1)n!} = x^2 \sum_{n=0}^{\infty} \frac{x^n}{(n+2)(n+1)n!}.$$

Thus $\sum_{n=0}^{\infty} \frac{1}{(n+1)(n+2)} \cdot \frac{x^n}{n!} = (e^x - x - 1)/x^2$.

48. In many of these cases, it's a matter of plugging the exponent of e into the generating function for e^x. We let a_n denote the n^{th} term of the sequence whose generating function is given.

a) The generating function is $e^{3x} = \sum_{n=0}^{\infty} \frac{(3x)^n}{n!} = \sum_{n=0}^{\infty} 3^n \frac{x^n}{n!}$, so the sequence is $a_n = 3^n$.

b) The generating function is $2e^{-3x+1} = (2e)e^{-3x} = 2e \sum_{n=0}^{\infty} \frac{(-3x)^n}{n!} = \sum_{n=0}^{\infty} (2e(-3)^n) \frac{x^n}{n!}$, so the sequence is $a_n = 2e(-3)^n$.

c) The generating function is $e^{4x} + e^{-4x} = \sum_{n=0}^{\infty} \frac{(4x)^n}{n!} + \sum_{n=0}^{\infty} \frac{(-4x)^n}{n!} = \sum_{n=0}^{\infty} (4^n + (-4)^n) \frac{x^n}{n!}$, so the sequence is $a_n = 4^n + (-4)^n$.

d) The sequence whose exponential generating function is e^{3x} is clearly $\{3^n\}$, as in part **(a)**. Since

$$1 + 2x = \frac{1}{0!}x^0 + \frac{2}{1!}x^1 + \sum_{n=2}^{\infty} \frac{0}{n!} x^n,$$

we know that $a_n = 3^n$ for $n \geq 2$, with $a_1 = 3^1 + 2 = 5$ and $a_0 = 3^0 + 1 = 2$.

e) We know that

$$\frac{1}{1+x} = \sum_{n=0}^{\infty} (-1)^n x^n = \sum_{n=0}^{\infty} \frac{(-1)^n n!}{n!} x^n,$$

so the sequence for which $1/(1+x)$ is the exponential generating function is $\{(-1)^n n!\}$. Combining this with the rest of the function (where the generating function is just $\{1\}$), we have $a_n = 1 - (-1)^n n!$.

f) Note that

$$xe^x = \sum_{n=0}^{\infty} x \cdot \frac{x^n}{n!} = \sum_{n=0}^{\infty} \frac{x^{n+1}}{n!} = \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} = \sum_{n=1}^{\infty} n \cdot \frac{x^n}{n!} = \sum_{n=0}^{\infty} n \cdot \frac{x^n}{n!}.$$

(We changed variable in the middle.) Therefore $a_n = n$, as in Exercise 46c.

g) First we note that

$$e^{x^3} = \sum_{n=0}^{\infty} \frac{(x^3)^n}{n!} = 1 + \frac{x^3}{1!} + \frac{x^6}{2!} + \frac{x^9}{3!} + \cdots$$

$$= \frac{x^0}{0!} \cdot \frac{0!}{0!} + \frac{x^3}{3!} \cdot \frac{3!}{1!} + \frac{x^6}{6!} \cdot \frac{6!}{2!} + \frac{x^9}{9!} \cdot \frac{9!}{3!} + \cdots.$$

Therefore we see that $a_n = 0$ if n is not a multiple of 3, and $a_n = n!/(n/3)!$ if n is a multiple of 3.

50. a) Since all 4^n base-four strings of length n fall into one of the four categories counted by a_n, b_n, c_n, and d_n, obviously $d_n = 4^n - a_n - b_n - c_n$. Next let's see how a string of various types of length $n+1$ can be obtained from a string of length n by adding one digit. To get a string of length $n+1$ with an even number of 0s and an even number of 1s, we can take a string of length n with these same parities and append a 2 or a 3 (thus there are $2a_n$ such strings of this type), or we can take a string of length n with an even number of 0s and an odd number of 1s and append a 1 (thus there are b_n such strings of this type), or we can take a string of length n with an odd number of 0s and an even number of 1s and append a 0 (thus there are c_n such strings of this type). Therefore we have $a_{n+1} = 2a_n + b_n + c_n$. In the same way we find that $b_{n+1} = 2b_n + a_n + d_n$, which equals $b_n - c_n + 4^n$ after substituting the identity with which we began this solution. Similarly, $c_{n+1} = 2c_n + a_n + d_n = c_n - b_n + 4^n$.

b) The strings of length 1 are 0, 1, 2, and 3. So clearly $a_1 = 2$, $b_1 = c_1 = 1$, and $d_1 = 0$. (Note that 0 is an even number.) In fact we can also say that $a_0 = 1$ (the empty string) and $b_0 = c_0 = d_0 = 0$.

c) We apply the recurrences from part **(a)** twice:

$$a_2 = 2\cdot 2 + 1 + 1 = 6 \qquad a_3 = 2\cdot 6 + 4 + 4 = 20$$
$$b_2 = 1 - 1 + 4 = 4 \qquad b_3 = 4 + 16 - 4 = 16$$
$$c_2 = 1 - 1 + 4 = 4 \qquad c_3 = 4 + 16 - 4 = 16$$
$$d_2 = 16 - 6 - 4 - 4 = 2 \qquad d_3 = 64 - 20 - 16 - 16 = 12$$

d) Before proceeding as the problem asks, we note a shortcut. By symmetry, b_n must be the same as c_n. Substituting this into our recurrences, we find immediately that $b_n = c_n = 4^{n-1}$ for $n \geq 1$. Therefore $a_n = 2a_{n-1} + 2\cdot 4^{n-2}$. This recurrence with the initial condition $a_1 = 2$ can easily be solved by the methods of either this section or Section 8.2 to give $a_n = 2^{n-1} + 4^{n-1}$. But let's proceed as instructed.

Let $A(x)$, $B(x)$, and $C(x)$ be the desired generating functions. Then $xA(x) = \sum_{n=0}^{\infty} a_n x^{n+1} = \sum_{n=1}^{\infty} a_{n-1}x^n$ and similarly for B and C, so we have

$$A(x) - xB(x) - xC(x) - 2xA(x) = \sum_{n=0}^{\infty} a_n x^n - \sum_{n=1}^{\infty} b_{n-1}x^n - \sum_{n=1}^{\infty} c_{n-1}x^n - \sum_{n=1}^{\infty} 2a_{n-1}x^n = a_0 = 1\,.$$

Similarly,

$$\begin{aligned} B(x) - xB(x) + xC(x) &= \sum_{n=0}^{\infty} b_n x^n - \sum_{n=1}^{\infty} b_{n-1}x^n + \sum_{n=1}^{\infty} c_{n-1}x^n \\ &= b_0 + \sum_{n=1}^{\infty} 4^{n-1}x^n = 0 + x\sum_{n=0}^{\infty} 4^n x^n = \frac{x}{1-4x}\,. \end{aligned}$$

Obviously C satisfies the same equation. Therefore our system of three equations (suppressing the arguments on A, B, and C) is

$$\begin{aligned} (1-2x)A - xB - xC &= 1 \\ (1-x)B + xC &= \frac{x}{1-4x} \\ xB + (1-x)C &= \frac{x}{1-4x}\,. \end{aligned}$$

e) Subtracting the third equation in part **(d)** from the second shows that $B = C$, and then plugging that back into the second equation immediately gives

$$B(x) = C(x) = \frac{x}{1-4x}\,.$$

Plugging these into the first equation yields

$$(1-2x)A - 2x\cdot\frac{x}{1-4x} = 1\,,$$

and solving for A gives us

$$A(x) = \frac{1-4x+2x^2}{(1-2x)(1-4x)}\,.$$

Now that we know the generating functions, we can recover the coefficients. For B and C (using Table 1) we immediately get a coefficient of 4^{n-1} for all $n \geq 1$, with $b_0 = c_0 = 0$. We rewrite $A(x)$ using partial fractions as

$$A(x) = \frac{1}{4} + \frac{1/2}{1-2x} + \frac{1/4}{1-4x}\,,$$

so we have $a_n = \frac{1}{2} \cdot 2^n + \frac{1}{4} \cdot 4^n = 2^{n-1} + 4^{n-1}$ for $n \geq 1$, with $a_0 = \frac{1}{4} + \frac{1}{2} + \frac{1}{4} = 1$.

52. To form a partition of n using only odd-sized parts, we must choose some 1s, some 3s, some 5s, and so on. The generating function for choosing 1s is

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}$$

(the exponent gives the number so obtained). Similarly, the generating function for choosing 3s is

$$1 + x^3 + x^6 + x^9 + \cdots = \frac{1}{1-x^3}$$

(again the exponent gives the number so obtained). The other choices have analogous generating functions. Therefore the generating function for the entire problem, so that the coefficient of x^n will give $p_o(n)$, the number of partitions of n into odd-sized part, is the infinite product

$$\frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \frac{1}{1-x^5} \cdots\,.$$

54. We need to carefully organize our work so as not to miss any of the partitions. We start with largest-sized parts first in all cases. For $n = 1$, we have $1 = 1$ as the only partition of either type, and so $p_o(1) = p_d(1) = 1$. For $n = 2$, we have $2 = 2$ as the only partition into distinct parts, and $2 = 1 + 1$ as the only partition into odd parts, so $p_o(1) = p_d(1) = 1$. For $n = 3$, we have $3 = 3$ and $3 = 2 + 1$ as the only partitions into distinct parts, and $3 = 3$ and $3 = 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 2$. For $n = 4$, we have $4 = 4$ and $4 = 3 + 1$ as the only partitions into distinct parts, and $4 = 3 + 1$ and $4 = 1 + 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 2$. For $n = 5$, we have $5 = 5$, $5 = 4 + 1$, and $5 = 3 + 2$ as the only partitions into distinct parts, and $5 = 5$, $5 = 3 + 1 + 1$, and $5 = 1 + 1 + 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 3$. For $n = 6$, we have $6 = 6$, $6 = 5 + 1$, $6 = 4 + 2$, and $6 = 3 + 2 + 1$ as the only partitions into distinct parts, and $6 = 5 + 1$, $6 = 3 + 3$, $6 = 3 + 1 + 1 + 1$, and $6 = 1 + 1 + 1 + 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 4$. For $n = 7$, we have $7 = 7$, $7 = 6 + 1$, $7 = 5 + 2$, $7 = 4 + 3$, and $7 = 4 + 2 + 1$ as the only partitions into distinct parts, and $7 = 7$, $7 = 5 + 1 + 1$, $7 = 3 + 3 + 1$, $7 = 3 + 1 + 1 + 1 + 1$, and $7 = 1 + 1 + 1 + 1 + 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 5$. Finally, for $n = 8$, we have $8 = 8$, $8 = 7 + 1$, $8 = 6 + 2$, $8 = 5 + 3$, $8 = 5 + 2 + 1$, and $8 = 4 + 3 + 1$ as the only partitions into distinct parts, and $8 = 7 + 1$, $8 = 5 + 3$ $8 = 5 + 1 + 1 + 1$, $8 = 3 + 3 + 1 + 1$, $8 = 3 + 1 + 1 + 1 + 1 + 1$, and $8 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$ as the only partitions into odd parts, so $p_o(1) = p_d(1) = 6$. As we will prove in Exercise 55, it is no coincidence that these numbers all agree.

56. This is a very difficult problem. A solution can be found in *The Theory of Partitions* by George Andrews (Addison-Wesley, 1976), Chapter 6.

58. **a)** In order to have the first success on the n^{th} trial, where $n \geq 1$, we must have $n - 1$ failures followed by a success. Therefore $p(X = n) = q^{n-1}p$, where p is the probability of success and $q = 1 - p$ is the probability of failure. Therefore the probability generating function is

$$G(x) = \sum_{n=1}^{\infty} q^{n-1} p x^n = px \sum_{n=1}^{\infty} (qx)^{n-1} = px \sum_{n=0}^{\infty} (qx)^n = \frac{px}{1-qx}\,.$$

b) By Exercise 57, $E(X)$ is the derivative of $G(x)$ at $x = 1$. Here we have

$$G'(x) = \frac{p}{(1-qx)^2}, \quad \text{so} \quad G'(1) = \frac{p}{(1-q)^2} = \frac{p}{p^2} = \frac{1}{p}.$$

From the same exercise, we know that the variance is $G''(1) + G'(1) - G'(1)^2$; so we compute:

$$G''(x) = \frac{2pq}{(1-qx)^3}, \quad \text{so} \quad G''(1) = \frac{2pq}{(1-q)^3} = \frac{2pq}{p^3} = \frac{2q}{p^2},$$

and therefore

$$V(X) = G''(1) + G'(1) - G'(1)^2 = \frac{2q}{p^2} + \frac{1}{p} - \frac{1}{p^2} = \frac{q}{p^2}.$$

60. We start with the definition and then use the fact that the only way for the sum of two nonnegative integers to be k is for one of them to be i and the other to be $k-i$, for some i between 0 and k, inclusive. We then invoke independence, and finally the definition of multiplication of infinite series:

$$\begin{aligned} G_{X+Y}(x) &= \sum_{k=0}^{\infty} p(X+Y=k)x^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} p(X=i \text{ and } Y=k-i) \right) x^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} p(X=i) \cdot p(Y=k-i) \right) x^k \\ &= G_X(x) \cdot G_Y(x) \end{aligned}$$

SECTION 8.5 Inclusion–Exclusion

2. $|C \cup D| = |C| + |D| - |C \cap D| = 345 + 212 - 188 = 369$

4. $|P \cap S| = |P| + |S| - |P \cup S| = 650{,}000 + 1{,}250{,}000 - 1{,}450{,}000 = 450{,}000$

6. **a)** In this case the union is just A_3, so the answer is $|A_3| = 10{,}000$.
b) The cardinality of the union is the sum of the cardinalities in this case, so the answer is $100+1000+10000 = 11{,}100$.
c) $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| = 100 + 1000 + 10000 - 2 - 2 - 2 + 1 = 11{,}095$

8. $270 - 64 - 94 - 58 + 26 + 28 + 22 - 14 = 116$

10. $100 - \lfloor 100/5 \rfloor - \lfloor 100/7 \rfloor + \lfloor 100/(5 \cdot 7) \rfloor = 100 - 20 - 14 + 2 = 68$

12. There are $\lfloor \sqrt{1000} \rfloor = 31$ squares and $\lfloor \sqrt[3]{1000} \rfloor = 10$ cubes. Furthermore there are $\lfloor \sqrt[6]{1000} \rfloor = 3$ numbers that are both squares and cubes, i.e., sixth powers. Therefore the answer is $31 + 10 - 3 = 38$.

14. There are 26! strings in all. To count the strings that contain *fish*, we glue these four letters together as one and permute it and the 22 other letters, so there are 23! such strings. Similarly there are 24! strings that contain *rat* and 23! strings that contain *bird*. Furthermore, there are 21! strings that contain both *fish* and *rat* (glue each of these sets of letters together), but there are no strings that contain both *bird* and another of these strings. Therefore the answer is $26! - 23! - 24! - 23! + 21! \approx 4.0 \times 10^{26}$.

16. $4 \cdot 100 - 6 \cdot 50 + 4 \cdot 25 - 5 = 195$

18. There are $C(10,1) + C(10,2) + \cdots + C(10,10) = 2^{10} - C(10,0) = 1023$ terms on the right-hand side of the equation.

20. $5 \cdot 10000 - 10 \cdot 1000 + 10 \cdot 100 - 5 \cdot 10 + 1 = 40{,}951$

22. The base case is $n = 2$, for which we already know the formula to be valid. Assume that the formula is true for n sets. Look at a situation with $n+1$ sets, and temporarily consider $A_n \cup A_{n+1}$ as one set. Then by the inductive hypothesis we have

$$\begin{aligned}|A_1 \cup \cdots \cup A_{n+1}| = \sum_{i<n} |A_i| + |A_n \cup A_{n+1}| - \sum_{i<j<n} |A_i \cap A_j| \\ - \sum_{i<n} |A_i \cap (A_n \cup A_{n+1})| + \cdots + (-1)^n |A_1 \cap \cdots \cap A_{n-1} \cap (A_n \cup A_{n+1})| \,.\end{aligned}$$

Next we apply the distributive law to each term on the right involving $A_n \cup A_{n+1}$, giving us

$$\sum |(A_{i_1} \cap \cdots \cap A_{i_m}) \cap (A_n \cup A_{n+1})| = \sum |(A_{i_1} \cap \cdots \cap A_{i_m} \cap A_n) \cup (A_{i_1} \cap \cdots \cap A_{i_m} \cap A_{n+1})| \,.$$

Now we apply the basis step to rewrite each of these terms as

$$\sum |A_{i_1} \cap \cdots \cap A_{i_m} \cap A_n| + \sum |A_{i_1} \cap \cdots \cap A_{i_m} \cap A_{n+1}| - \sum |A_{i_1} \cap \cdots \cap A_{i_m} \cap A_n \cap A_{n+1}| \,,$$

which gives us precisely the summation we want.

24. Let E_1, E_2, and E_3 be these three events, in the order given. Then $p(E_1) = C(5,3)/2^5 = 10/32$; $p(E_2) = 2^3/2^5 = 8/32$; and $p(E_3) = 2^3/2^5 = 8/32$. Furthermore $p(E_1 \cap E_2) = C(3,1)/2^5 = 3/32$; $p(E_1 \cap E_3) = 1/32$; and $p(E_2 \cap E_3) = 2/32$. Finally $p(E_1 \cap E_2 \cap E_3) = 1/32$. Therefore the probability that at least one of these events occurs is $(10 + 8 + 8 - 3 - 1 - 2 + 1)/32 = 21/32$.

26. We only need to list the terms that have one or two events in them. Thus we have

$$p(E_1 \cup E_2 \cup E_3 \cup E_4) = \sum_{1 \le i \le 4} p(E_i) - \sum_{1 \le i < j \le 4} p(E_i \cap E_j) \,,$$

or, explicitly, $p(E_1 \cup E_2 \cup E_3 \cup E_4) = p(E_1) + p(E_2) + p(E_3) + p(E_4) - p(E_1 \cap E_2) - p(E_1 \cap E_3) - p(E_1 \cap E_4) - p(E_2 \cap E_3) - p(E_2 \cap E_4) - p(E_3 \cap E_4)$.

28. The probability of the union, in this case, is the sum of the probabilities of the events:

$$p(E_1 \cup E_2 \cup \cdots \cup E_n) = \sum_{i=1}^{n} p(E_i) = p(E_1) + p(E_2) + \cdots + p(E_n)$$

SECTION 8.6 Applications of Inclusion–Exclusion

2. $1000 - 450 - 622 - 30 + 111 + 14 + 18 - 9 = 32$

4. $C(4+17-1,17) - C(4+13-1,13) - C(4+12-1,12) - C(4+11-1,11) - C(4+8-1,8) + C(4+8-1,8) + C(4+7-1,7) + C(4+4-1,4) + C(4+6-1,6) + C(4+3-1,3) + C(4+2-1,2) - C(4+2-1,2) = 20$

6. Square-free numbers are those not divisible by the square of a prime. We count them as follows: $99 - \lfloor 99/2^2 \rfloor - \lfloor 99/3^2 \rfloor - \lfloor 99/5^2 \rfloor - \lfloor 99/7^2 \rfloor + \lfloor 99/(2^2 3^2) \rfloor = 61$.

8. $5^7 - C(5,1)4^7 + C(5,2)3^7 - C(5,3)2^7 + C(5,4)1^7 = 16{,}800$

10. This problem is asking for the number of onto functions from a set with 8 elements (the balls) to a set with 3 elements (the urns). Therefore the answer is $3^8 - C(3,1)2^8 + C(3,2)1^8 = 5796$.

12. 2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321

14. We use Theorem 2 with $n = 10$, which gives us

$$\frac{D_{10}}{10!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{1}{10!} = \frac{1334961}{3628800} = \frac{16481}{44800} \approx 0.3678794643\,,$$

which is almost exactly $e^{-1} \approx 0.3678794412\ldots$.

16. There are $n!$ ways to make the first assignment. We can think of this first seating as assigning student n to a chair we will label n. Then the next seating must be a derangement with respect to this numbering, so there are D_n second seatings possible. Therefore the answer is $n!D_n$.

18. In a derangement of the numbers from 1 to n, the number 1 cannot go first, so let $k \neq 1$ be the number that goes first. There are $n-1$ choices for k. Now there are two ways to get a derangement with k first. One way is to have 1 in the k^{th} position. If we do this, then there are exactly D_{n-2} ways to derange the rest of the numbers. On the other hand, if 1 does not go into the k^{th} position, then think of the number 1 as being temporarily relabeled k. A derangement is completed in this case by finding a derangement of the numbers 2 through n in positions 2 through n, so there are D_{n-1} of them. Combining all this, by the product rule and the sum rule, we obtain the desired recurrence relation. The initial conditions are $D_0 = 1$ and $D_1 = 0$.

20. We apply iteration to the formula $D_n = nD_{n-1} + (-1)^n$, obtaining

$$\begin{aligned}
D_n &= n\big((n-1)D_{n-2} + (-1)^{n-1}\big) + (-1)^n \\
&= n(n-1)D_{n-2} + n(-1)^{n-1} + (-1)^n \\
&= n(n-1)\big((n-2)D_{n-3} + (-1)^{n-2}\big) + n(-1)^{n-1} + (-1)^n \\
&= n(n-1)(n-2)D_{n-3} + n(n-1)(-1)^{n-2} + n(-1)^{n-1} + (-1)^n \\
&\ \ \vdots \\
&= n(n-1)\cdots 2D_1 + n(n-1)\cdots 3 - n(n-1)\cdots 4 + \cdots + n(-1)^{n-1} + (-1)^n \\
&= n(n-1)\cdots 3 - n(n-1)\cdots 4 + \cdots + n(-1)^{n-1} + (-1)^n\,,
\end{aligned}$$

which yields the formula in Theorem 2 after factoring out $n!$.

22. The numbers not relatively prime to pq are the ones that have p and/or q as a factor. Thus we have

$$\phi(pq) = pq - \frac{pq}{p} - \frac{pq}{q} + \frac{pq}{pq} = pq - q - p + 1 = (p-1)(q-1)\,.$$

24. The left-hand side of course counts the number of permutations of the set of integers from 1 to n. The right-hand side counts it, too, by a two-step process: first decide how many and which elements are to be fixed (this can be done in $C(n,k)$ ways, for each of $k = 0, 1, \ldots, n$), and in each case derange the remaining elements (which can be done in D_{n-k} ways).

26. This permutation starts with $4, 5, 6$ in some order ($3! = 6$ ways to choose this), followed by $1, 2, 3$ in some order ($3! = 6$ ways to decide this). Therefore the answer is $6 \cdot 6 = 36$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 8

2. **a)** Let a_n be the amount that remains after n hours. Then $a_n = 0.99a_{n-1}$.
b) By iteration we find the solution $a_n = (0.99)^n a_0$, where a_0 is the original amount of the isotope.

4. **a)** Let B_n be the number of bacteria after n hours. The initial conditions are $B_0 = 100$ and $B_1 = 300$. Thereafter, $B_n = B_{n-1} + 2B_{n-1} - B_{n-2} = 3B_{n-1} - B_{n-2}$.
b) The characteristic equation is $r^2 - 3r + 1 = 0$, which has roots $(3 \pm \sqrt{5})/2$. Therefore the general solution is $B_n = \alpha_1((3+\sqrt{5})/2)^n + \alpha_2((3-\sqrt{5})/2)^n$. Plugging in the initial conditions we determine that $\alpha_1 = 50 + 30\sqrt{5}$ and $\alpha_2 = 50 - 30\sqrt{5}$. Therefore the solution is $B_n = (50+30\sqrt{5})((3+\sqrt{5})/2)^n + (50-30\sqrt{5})((3-\sqrt{5})/2)^n$.
c) Plugging in small values of n, we find that $B_9 = 676{,}500$ and $B_{10} = 1{,}771{,}100$. Therefore the colony will contain more than one million bacteria after 10 hours.

6. We can put any of the stamps on first, leaving a problem with a smaller number of cents to solve. Thus the recurrence relation is $a_n = a_{n-4} + a_{n-6} + a_{n-10}$. We need 10 initial conditions, and it is easy to see that $a_0 = 1$, $a_1 = a_2 = a_3 = a_5 = a_7 = a_9 = 0$, and $a_4 = a_6 = a_8 = 1$.

8. If we add the equations, we obtain $a_n + b_n = 2a_{n-1}$, which means that $b_n = 2a_{n-1} - a_n$. If we now substitute this back into the first equation, we have $a_n = a_{n-1} + (2a_{n-2} - a_{n-1}) = 2a_{n-2}$. The initial conditions are $a_0 = 1$ (given) and $a_1 = 3$ (follows from the first recurrence relation and the given initial conditions). We can solve this using the characteristic equation $r^2 - 2 = 0$, but a simpler approach, that avoids irrational numbers, is as follows. It is clear that $a_{2n} = 2^n a_0 = 2^n$, and $a_{2n+1} = 2^n a_1 = 3 \cdot 2^n$. This is a nice explicit formula, which is all that "solution" really means. We also need a formula for b_n, of course. From $b_n = 2a_{n-1} - a_n$ (obtained above), we have $b_{2n} = 3 \cdot 2^n - 2^n = 2^{n+1}$, and $b_{2n+1} = 2 \cdot 2^n - 3 \cdot 2^n = -2^n$.

10. Following the hint, we let $b_n = \log a_n$. Then the recurrence relation becomes $b_n = 3b_{n-1} + 2b_{n-2}$, with initial conditions $b_0 = b_1 = 1$. This is solved in the usual manner. The characteristic equation is $r^2 - 3r - 2 = 0$, which gives roots $(3 \pm \sqrt{17})/2$. Plugging the initial conditions into the general solution and doing some messy algebra gives

$$b_n = \frac{17 - \sqrt{17}}{34}\left(\frac{3+\sqrt{17}}{2}\right)^n + \frac{17+\sqrt{17}}{34}\left(\frac{3-\sqrt{17}}{2}\right)^n .$$

The solution to the original problem is then $a_n = 2^{b_n}$.

12. The characteristic equation is $r^3 - 3r^2 + 3r - 1 = 0$. This factors as $(r-1)^3 = 0$, so there is only one root, 1, and its multiplicity is 3. Therefore the general solution is $a_n = \alpha_1 + \alpha_2 n + \alpha_3 n^2$. Plugging in the initial conditions gives us $2 = \alpha_1$, $2 = \alpha_1 + \alpha_2 + \alpha_3$, and $4 = \alpha_1 + 2\alpha_2 + 4\alpha_3$. Solving yields $\alpha_1 = 2$, $\alpha_2 = -1$, and $\alpha_3 = 1$. Therefore the solution is $a_n = 2 - n + n^2$.

14. The success of this algorithm relies heavily on the fact that the weights are integers. The time complexity is nW. If the weights are real numbers (or, what effectively amounts to the same thing, W is prohibitively large), then no efficient algorithm is known for solving the knapsack problem. Indeed, the problem is NP-complete.

a) In this case the weight of item j by itself exceeds w, so no subset of the first j items whose total weight does not exceed w can contain item j. Therefore the maximum total weight not exceeding w among the first j items is achieved by a subset of the first $j-1$ items, and $M(j-1,w)$ is that maximum.

b) The maximum total weight not exceeding w among the first j items either is achieved by using item j or is achieved without using item j. In the latter case, that maximum is the same as the maximum total weight not exceeding w among the first $j-1$ items, namely $M(j-1,w)$. In the latter case, the maximum weight that a subset of the first $j-1$ items can contribute is $M(j-1,w-w_j)$, so $M(j,w) = w_j + M(j-1,w-w_j)$ in this case.

c) Without loss of generality, we can assume that each $w_j \le W$; overweight items cannot contribute to the desired subset, so they can be discarded before we start. We need to compute $M(j,w)$ for all $1 \le j \le n$ and all $0 \le w \le W$. To initialize, we set $M(1,w) = w_1$ for $w_1 \le w \le W$, set $M(1,w) = 0$ for $0 \le w < w_1$, and set $M(j,0) = 0$ for $1 \le j \le n$. We then loop through $j = 2,3,\ldots,n$, and for each j loop through $w = 1,2,\ldots,W$, computing the values of $M(j,w)$ according to the rules given in parts **(a)** and **(b)**.

d) The maximum total weight is given by $M(n,W)$. By the way the algorithm works, that value is either $M(n-1,W)$ or it is $w_n + M(n-1,W-w_n)$. By computing those two quantities, we can determine which it is; in the former case we know that item n is not in the optimal subset, and we can proceed with this same calculation by looking at $M(n-1,W)$, whereas in the latter case we know that item n is in the optimal subset and we can proceed with this same calculation by looking at $M(n-1,W-w_n)$.

16. The initial conditions $L(i,0) = L(0,j) = 0$ are trivial. That $L(i,j) = L(i-1,j-1)+1$ when the last symbols match follows immediately from Exercise 15a. That $L(i,j) = \max(L(i,j-1), L(i-1,j))$ when the last symbols do not match follows immediately from Exercise 15b.

18. The length of the longest common subsequence is given by $L(m,n)$. If $a_m = b_n$ then we know that the longest common subsequence ends with that symbol, and the first $L(m,n)-1$ symbols can then be found by proceeding with this same calculation by looking at $L(m-1,n-1)$. Otherwise we compare $L(m,n-1)$ and $L(m-1,n)$ and proceed with this same calculation at the location in the table at which the larger value is located (that value will be the same as $L(m,n)$).

20. We use the result of Exercise 31 in Section 8.3, with $a=3$, $b=5$, $c=2$, and $d=4$. Thus the solution is $f(n) = 625n^4/311 - 314n^{\log_5 3}/311$.

22. The algorithm compares the largest elements of the two halves (this is one comparison), and then it compares the smaller largest element with the second largest element of the other half (one more comparison). This is sufficient to determine the largest and second largest elements of the list. (If the list has only one element in it, then the second largest element is declared to be $-\infty$.) Let $f(n)$ be the number of comparisons used by this algorithm on a list of size n. The list is split into two lists, of size $\lfloor n/2 \rfloor$ and $\lceil n/2 \rceil$, respectively. Thus our recurrence relation is $f(n) = f(\lfloor n/2 \rfloor) + f(\lceil n/2 \rceil) + 2$, with initial condition $f(1) = 0$. (This algorithm could be made slightly more efficient by having the base cases be $n=2$ and $n=3$, rather than $n=1$.)

24. **a)** That a_m is greater than a_{m-1} and greater than a_{m+1} follows immediately from the definition given. Note that it might happen that $a_m = a_1$ or $a_m = a_n$, in which case half of the condition is satisfied vacuously. Furthermore, because the terms strictly increase up to a_m and strictly decrease afterwards, there cannot be two terms satisfying this condition.

b) If m were less than or equal to i, then the condition $a_i < a_{i+1}$ would violate the fact that the terms in the sequence must decrease once a_m is encountered.

c) If m were greater than i, then the condition $a_i > a_{i+1}$ would violate the fact that the terms in the sequence must increase until a_m is encountered.

d) The algorithm is similar to binary search. Suppose we have narrowed the search down to $a_i, a_{i+1}, \ldots, a_j$, where initially $i = 1$ and $j = n$. If $j - i = 1$, then $a_m = a_i$; and if $j - i = 2$, then a_m is the larger of a_i and a_j. Otherwise, we look at the middle term in that sequence, a_k, where $k = \lfloor (i+j)/2 \rfloor$. By part **(b)**, if $a_{k-1} < a_k$, then we know that a_m must be in $a_k, a_{k+1}, \ldots, a_j$, so we can replace i by k and iterate. By part **(c)**, if $a_k > a_{k+1}$, then we know that a_m must be in $a_i, a_{i+1}, \ldots, a_k$, so we can replace j by k and iterate. (And if we wish, we could declare that $a_m = a_k$ if both of these conditions are met.) The algorithm could also be written recursively.

26. **a)** $\Delta a_n = 3 - 3 = 0$ **b)** $\Delta a_n = 4(n+1) + 7 - (4n+7) = 4$
c) $\Delta a_n = \big((n+1)^2 + (n+1) + 1\big) - (n^2 + n + 1) = 2n + 2$

28. We prove something a bit stronger. If $a_n = P(n)$ is a polynomial of degree at most d, then Δa_n is a polynomial of degree at most $d - 1$. To see this, let $P(n) = c_d n^d + (\text{lower order terms})$. Then

$$\begin{aligned}\Delta P(n) &= c_d(n+1)^d + (\text{lower order terms}) - c_d n^d + (\text{lower order terms})\\ &= c_d n^d + (\text{lower order terms}) - c_d n^d + (\text{lower order terms})\\ &= (\text{lower order terms}).\end{aligned}$$

If we apply this result $d + 1$ times, then we get that $\Delta^{d+1} a_n$ has degree at most -1, i.e., is identically 0.

30. Since it is valid to use the commutative, associative, and distributive laws for absolutely convergent infinite series, we simply write

$$(cF + dG)(x) = cF(x) + dG(x) = c\sum_{k=0}^{\infty} a_k x^k + d\sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (ca_k + db_k)x^k .$$

32. $14 + 18 - 22 = 10$

34. If the queries are correct, then by inclusion–exclusion the number of students who are freshmen and have not taken courses in either subject must equal $2175 - 1675 - 1074 - 444 + 607 + 350 + 201 - 143 = -3$. Since a negative number here is not possible, we conclude that the responses cannot all be accurate.

36. There will be $C(7,i)$ terms involving combinations of i of the sets at a time. Therefore the answer is $C(7,1) + C(7,2) + C(7,3) + C(7,4) + C(7,5) = 119$.

38. For a more compact notation, let us write 1,000,000 as M.
a) $\lfloor M/2 \rfloor + \lfloor M/3 \rfloor + \lfloor M/5 \rfloor - \lfloor M/(2\cdot 3) \rfloor - \lfloor M/(2\cdot 5) \rfloor - \lfloor M/(3\cdot 5) \rfloor + \lfloor M/(2\cdot 3\cdot 5) \rfloor = 733{,}334$
b) $M - \lfloor M/7 \rfloor - \lfloor M/11 \rfloor - \lfloor M/13 \rfloor + \lfloor M/(7\cdot 11) \rfloor + \lfloor M/(7\cdot 13) \rfloor + \lfloor M/(11\cdot 13) \rfloor - \lfloor M/(7\cdot 11\cdot 13) \rfloor = 719{,}281$
c) This is asking for numbers divisible by 3 but not by 21. Since the set of numbers divisible by 21 is a subset of the set of numbers divisible by 3, this is simply $\lfloor M/3 \rfloor - \lfloor M/21 \rfloor = 285{,}714$.

40. After the assignments of the hardest and easiest job have been made, there are 4 different jobs to assign to 3 different employees. No restrictions are stated, so we assume that there are none. Therefore we are just looking for the number of functions from a set with 4 elements to a set with 3 elements, and there are $3^4 = 81$ such functions. (If we impose the restriction that every employee must get at least one job, then it is a little harder. In particular, we must rule out all the assignments in which the jobs go only to the two employees that already have jobs. There are $2^4 = 16$ such assignments, so the answer would be $81 - 16 = 65$ in this case.)

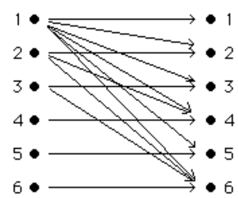
42. We will count the number of bit strings that do contain four consecutive 1's. Bits 1 through 4 could be 1's, or bits 2 through 5, or bits 3 through 6, and in each case there are 4 strings meeting those conditions (since the other two bits are free). This gives a total of 12. However we overcounted, since there are ways in which more than one of these can happen. There are 2 strings in which bits 1 through 4 and bits 2 through 5 are 1's, 2 strings in which bits 2 through 5 and bits 3 through 6 are 1's, and 1 string in which bits 1 through 4 and bits 3 through 6 are 1's. Finally, there is 1 string in which all three substrings are 1's. Thus the number of bit strings with 4 consecutive 1's is $12 - 2 - 2 - 1 + 1 = 8$. Therefore the answer to the exercise is $2^6 - 8 = 56$.

CHAPTER 9
Relations

SECTION 9.1 Relations and Their Properties

2. a) $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(2,2)$, $(2,4)$, $(2,6)$, $(3,3)$, $(3,6)$, $(4,4)$, $(5,5)$, $(6,6)$

b) We draw a line from a to b whenever a divides b, using separate sets of points; an alternate form of this graph would have just one set of points.



c) We put an $\times$ in the i^{th} row and j^{th} column if and only if i divides j.

R	1	2	3	4	5	6
1	×	×	×	×	×	×
2		×		×		×
3			×			×
4				×		
5					×	
6						×

4. a) Being taller than is not reflexive (I am not taller than myself), nor symmetric (I am taller than my daughter, but she is not taller than I). It is antisymmetric (vacuously, since we never have A taller than B, and B taller than A, even if $A = B$). It is clearly transitive.

b) This is clearly reflexive, symmetric, and transitive (it is an equivalence relation—see Section 9.5). It is not antisymmetric, since twins, for example, are unequal people born on the same day.

c) This has exactly the same answers as part **(b)**, since having the same first name is just like having the same birthday.

d) This is clearly reflexive and symmetric. It is not antisymmetric, since my cousin and I have a common grandparent, and I and my cousin have a common grandparent, but I am not equal to my cousin. This relation is not transitive. My cousin and I have a common grandparent; my cousin and her cousin on the other side of her family have a common grandparent. My cousin's cousin and I do not have a common grandparent.

6. a) Since $1+1 \neq 0$, this relation is not reflexive. Since $x+y = y+x$, it follows that $x+y=0$ if and only if $y+x=0$, so the relation is symmetric. Since $(1,-1)$ and $(-1,1)$ are both in R, the relation is not antisymmetric. The relation is not transitive; for example, $(1,-1) \in R$ and $(-1,1) \in R$, but $(1,1) \notin R$.

b) Since $x = \pm x$ (choosing the plus sign), the relation is reflexive. Since $x = \pm y$ if and only if $y = \pm x$, the relation is symmetric. Since $(1,-1)$ and $(-1,1)$ are both in R, the relation is not antisymmetric. The relation is transitive, essentially because the product of 1's and -1's is ± 1.

c) The relation is reflexive, since $x - x = 0$ is a rational number. The relation is symmetric, because if $x - y$ is rational, then so is $-(x-y) = y - x$. Since $(1,-1)$ and $(-1,1)$ are both in R, the relation is not antisymmetric. To see that the relation is transitive, note that if $(x,y) \in R$ and $(y,z) \in R$, then $x - y$ and $y - z$ are rational numbers. Therefore their sum $x - z$ is rational, and that means that $(x,z) \in R$.

d) Since $1 \neq 2 \cdot 1$, this relation is not reflexive. It is not symmetric, since $(2,1) \in R$, but $(1,2) \notin R$. To see that it is antisymmetric, suppose that $x = 2y$ and $y = 2x$. Then $y = 4y$, from which it follows that $y = 0$ and hence $x = 0$. Thus the only time that (x,y) and (y,x) are both is R is when $x = y$ (and both are 0). This relation is clearly not transitive, since $(4,2) \in R$ and $(2,1) \in R$, but $(4,1) \notin R$.

e) This relation is reflexive since squares are always nonnegative. It is clearly symmetric (the roles of x and y in the statement are interchangeable). It is not antisymmetric, since $(2,3)$ and $(3,2)$ are both in R. It is not transitive; for example, $(1,0) \in R$ and $(0,-2) \in R$, but $(1,-2) \notin R$.

f) This is not reflexive, since $(1,1) \notin R$. It is clearly symmetric (the roles of x and y in the statement are interchangeable). It is not antisymmetric, since $(2,0)$ and $(0,2)$ are both in R. It is not transitive; for example, $(1,0) \in R$ and $(0,-2) \in R$, but $(1,-2) \notin R$.

g) This is not reflexive, since $(2,2) \notin R$. It is not symmetric, since $(1,2) \in R$ but $(2,1) \notin R$. It is antisymmetric, because if $(x,y) \in R$ and $(y,x) \in R$, then $x = 1$ and $y = 1$, so $x = y$. It is transitive, because if $(x,y) \in R$ and $(y,z) \in R$, then $x = 1$ (and $y = 1$, although that doesn't matter), so $(x,z) \in R$.

h) This is not reflexive, since $(2,2) \notin R$. It is clearly symmetric (the roles of x and y in the statement are interchangeable). It is not antisymmetric, since $(2,1)$ and $(1,2)$ are both in R. It is not transitive; for example, $(3,1) \in R$ and $(1,7) \in R$, but $(3,7) \notin R$.

8. If $R = \emptyset$, then the hypotheses of the conditional statements in the definitions of *symmetric* and *transitive* are never true, so those statements are always true by definition. Because $S \neq \emptyset$, the statement $(a,a) \in R$ is false for an element of S, so $\forall a\,(a,a) \in R$ is not true; thus R is not reflexive.

10. We give the simplest example in each case.

a) the empty set on $\{a\}$ (vacuously symmetric and antisymmetric)

b) $\{(a,b),(b,a),(a,c)\}$ on $\{a,b,c\}$

12. Only the relation in part **(a)** is irreflexive (the others are all reflexive).

14. **a)** not irreflexive, since $(0,0) \in R$. **b)** not irreflexive, since $(0,0) \in R$.
c) not irreflexive, since $(0,0) \in R$. **d)** not irreflexive, since $(0,0) \in R$.
e) not irreflexive, since $(0,0) \in R$. **f)** not irreflexive, since $(0,0) \in R$.
g) not irreflexive, since $(1,1) \in R$. **h)** not irreflexive, since $(1,1) \in R$.

16. $\forall x\,((x,x) \notin R)$

18. The relations in parts **(a)**, **(b)**, and **(e)** are not asymmetric since they contain pairs of the form (x,x). Clearly the relation in part **(c)** is not asymmetric. The relation in part **(f)** is not asymmetric (both $(1,3)$ and $(3,1)$ are in the relation). It is easy to see that the relation in part **(d)** is asymmetric.

20. According to the preamble to Exercise 18, an asymmetric relation is one for which $(a,b) \in R$ and $(b,a) \in R$ can never hold simultaneously, even if $a = b$. Thus R is asymmetric if and only if R is antisymmetric and also irreflexive.

a) This is not asymmetric, since in fact (a,a) is always in R.

b) For any page a with no links, $(a,a) \in R$, so this is not asymmetric.

c) For any page a with links, $(a,a) \in R$, so this is not asymmetric.

d) For any page a that is linked to, $(a,a) \in R$, so this is not asymmetric.

22. An asymmetric relation must be antisymmetric, since the hypothesis of the condition for antisymmetry is false if the relation is asymmetric. The relation $\{(a,a)\}$ on $\{a\}$ is antisymmetric but not asymmetric, however, so the answer to the second question is no. In fact, it is easy to see that R is asymmetric if and only if R is antisymmetric and irreflexive.

24. Of course many answers are possible. The empty relation is always asymmetric (x is never related to y). A less trivial example would be $(a,b) \in R$ if and only if a is taller than b. Clearly it is impossible that both a is taller than b and b is taller than a at the same time.

26. **a)** $R^{-1} = \{\,(b,a) \mid (a,b) \in R\,\} = \{\,(b,a) \mid a < b\,\} = \{\,(a,b) \mid a > b\,\}$
b) $\overline{R} = \{\,(a,b) \mid (a,b) \notin R\,\} = \{\,(a,b) \mid a \not< b\,\} = \{\,(a,b) \mid a \geq b\,\}$

28. **a)** Since this relation is symmetric, $R^{-1} = R$.
b) This relation consists of all pairs (a,b) in which state a does not border state b.

30. These are merely routine exercises in set theory. Note that $R_1 \subseteq R_2$.
a) $\{(1,1),(1,2),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3),(3,4)\} = R_2$ **b)** $\{(1,2),(2,3),(3,4)\} = R_1$
c) $\emptyset$ **d)** $\{(1,1),(2,1),(2,2),(3,1),(3,2),(3,3)\}$

32. Since $(1,2) \in R$ and $(2,1) \in S$, we have $(1,1) \in S \circ R$. We use similar reasoning to form the rest of the pairs in the composition, giving us the answer $\{(1,1),(1,2),(2,1),(2,2)\}$.

34. **a)** The union of two relations is the union of these sets. Thus $R_1 \cup R_3$ holds between two real numbers if R_1 holds or R_3 holds (or both, it goes without saying). Here this means that the first number is greater than the second or vice versa—in other words, that the two numbers are not equal. This is just relation R_6.

b) For (a,b) to be in $R_3 \cup R_6$, we must have $a > b$ or $a = b$. Since this happens precisely when $a \geq b$, we see that the answer is R_2.

c) The intersection of two relations is the intersection of these sets. Thus $R_2 \cap R_4$ holds between two real numbers if R_2 holds and R_4 holds as well. Thus for (a,b) to be in $R_2 \cap R_4$, we must have $a \geq b$ and $a \leq b$. Since this happens precisely when $a = b$, we see that the answer is R_5.

d) For (a,b) to be in $R_3 \cap R_5$, we must have $a < b$ and $a = b$. It is impossible for $a < b$ and $a = b$ to hold at the same time, so the answer is $\emptyset$, i.e., the relation that never holds.

e) Recall that $R_1 - R_2 = R_1 \cap \overline{R_2}$. But $\overline{R_2} = R_3$, so we are asked for $R_1 \cap R_3$. It is impossible for $a > b$ and $a < b$ to hold at the same time, so the answer is $\emptyset$, i.e., the relation that never holds.

f) Reasoning as in part **(f)**, we want $R_2 \cap \overline{R_1} = R_2 \cap R_4$, which is R_5 (this was part **(c)**).

g) Recall that $R_1 \oplus R_3 = (R_1 \cap \overline{R_3}) \cup (R_3 \cap \overline{R_1})$. We see that $R_1 \cap \overline{R_3} = R_1 \cap R_2 = R_1$, and $R_3 \cap \overline{R_1} = R_3 \cap R_4 = R_3$. Thus our answer is $R_1 \cup R_3 = R_6$ (as in part **(a)**).

h) Recall that $R_2 \oplus R_4 = (R_2 \cap \overline{R_4}) \cup (R_4 \cap \overline{R_2})$. We see that $R_2 \cap \overline{R_4} = R_2 \cap R_1 = R_1$, and $R_4 \cap \overline{R_2} = R_4 \cap R_3 = R_3$. Thus our answer is $R_1 \cup R_3 = R_6$ (as in part **(a)**).

36. Recall that the composition of two relations all defined on a common set is defined as follows: $(a,c) \in S \circ R$ if and only if there is some element b such that $(a,b) \in R$ and $(b,c) \in S$. We have to apply this in each case.

a) For (a,c) to be in $R_1 \circ R_1$, we must find an element b such that $(a,b) \in R_1$ and $(b,c) \in R_1$. This means that $a > b$ and $b > c$. Clearly this can be done if and only if $a > c$ to begin with. But that is precisely the statement that $(a,c) \in R_1$. Therefore we have $R_1 \circ R_1 = R_1$. We can interpret (part of) this as showing that R_1 is transitive.

b) For (a,c) to be in $R_1 \circ R_2$, we must find an element b such that $(a,b) \in R_2$ and $(b,c) \in R_1$. This means that $a \geq b$ and $b > c$. Clearly this can be done if and only if $a > c$ to begin with. But that is precisely the statement that $(a,c) \in R_1$. Therefore we have $R_1 \circ R_2 = R_1$.

c) For (a,c) to be in $R_1 \circ R_3$, we must find an element b such that $(a,b) \in R_3$ and $(b,c) \in R_1$. This means that $a < b$ and $b > c$. Clearly this can always be done simply by choosing b to be large enough. Therefore we have $R_1 \circ R_3 = \mathbf{R}^2$, the relation that always holds.

d) For (a,c) to be in $R_1 \circ R_4$, we must find an element b such that $(a,b) \in R_4$ and $(b,c) \in R_1$. This means that $a \leq b$ and $b > c$. Clearly this can always be done simply by choosing b to be large enough. Therefore we have $R_1 \circ R_4 = \mathbf{R}^2$, the relation that always holds.

e) For (a,c) to be in $R_1 \circ R_5$, we must find an element b such that $(a,b) \in R_5$ and $(b,c) \in R_1$. This means that $a = b$ and $b > c$. Clearly this can be done if and only if $a > c$ to begin with (choose $b = a$). But that is precisely the statement that $(a,c) \in R_1$. Therefore we have $R_1 \circ R_5 = R_1$. One way to look at this is to say that R_5, the equality relation, acts as an identity for the composition operation (on the right—although it is also an identity on the left as well).

f) For (a,c) to be in $R_1 \circ R_6$, we must find an element b such that $(a,b) \in R_6$ and $(b,c) \in R_1$. This means that $a \neq b$ and $b > c$. Clearly this can always be done simply by choosing b to be large enough. Therefore we have $R_1 \circ R_6 = \mathbf{R}^2$, the relation that always holds.

g) For (a,c) to be in $R_2 \circ R_3$, we must find an element b such that $(a,b) \in R_3$ and $(b,c) \in R_2$. This means that $a < b$ and $b \geq c$. Clearly this can always be done simply by choosing b to be large enough. Therefore we have $R_2 \circ R_3 = \mathbf{R}^2$, the relation that always holds.

h) For (a,c) to be in $R_3 \circ R_3$, we must find an element b such that $(a,b) \in R_3$ and $(b,c) \in R_3$. This means that $a < b$ and $b < c$. Clearly this can be done if and only if $a < c$ to begin with. But that is precisely the statement that $(a,c) \in R_3$. Therefore we have $R_3 \circ R_3 = R_3$. We can interpret (part of) this as showing that R_3 is transitive.

38. For (a,b) to be an element of R^3, we must find people c and d such that $(a,c) \in R$, $(c,d) \in R$, and $(d,b) \in R$. In words, this says that a is the parent of someone who is the parent of someone who is the parent of b. More simply, a is a great-grandparent of b.

40. Note that these two relations are inverses of each other, since a is a multiple of b if and only if b divides a (see the preamble to Exercise 26).

a) The union of two relations is the union of these sets. Thus $R_1 \cup R_2$ holds between two integers if R_1 holds or R_2 holds (or both, it goes without saying). Thus $(a,b) \in R_1 \cup R_2$ if and only if $a \mid b$ or $b \mid a$. There is not a good easier way to state this.

b) The intersection of two relations is the intersection of these sets. Thus $R_1 \cap R_2$ holds between two integers if R_1 holds and R_2 holds. Thus $(a,b) \in R_1 \cap R_2$ if and only if $a \mid b$ and $b \mid a$. This happens if and only if $a = \pm b$ and $a \neq 0$.

c) By definition $R_1 - R_2 = R_1 \cap \overline{R_2}$. Thus this relation holds between two integers if R_1 holds and R_2 does not hold. We can write this in symbols by saying that $(a,b) \in R_1 - R_2$ if and only if $a \mid b$ and $b \nmid a$. This is equivalent to saying that $a \mid b$ and $a \neq \pm b$.

d) By definition $R_2 - R_1 = R_2 \cap \overline{R_1}$. Thus this relation holds between two integers if R_2 holds and R_1 does not hold. We can write this in symbols by saying that $(a,b) \in R_2 - R_1$ if and only if $b \mid a$ and $a \nmid b$. This is equivalent to saying that $b \mid a$ and $a \neq \pm b$.

e) We know that $R_1 \oplus R_2 = (R_1 - R_2) \cup (R_2 - R_1)$, so we look at our solutions to part **(c)** and part **(d)**. Thus this relation holds between two integers if R_1 holds and R_2 does not hold, or vice versa. This happens if and only if $a \mid b$ or $b \mid a$, but $a \neq \pm b$.

42. These are just the 16 different subsets of $\{(0,0),(0,1),(1,0),(1,1)\}$.

1. $\emptyset$
2. $\{(0,0)\}$
3. $\{(0,1)\}$
4. $\{(1,0)\}$
5. $\{(1,1)\}$
6. $\{(0,0),(0,1)\}$
7. $\{(0,0),(1,0)\}$
8. $\{(0,0),(1,1)\}$
9. $\{(0,1),(1,0)\}$
10. $\{(0,1),(1,1)\}$
11. $\{(1,0),(1,1)\}$
12. $\{(0,0),(0,1),(1,0)\}$
13. $\{(0,0),(0,1),(1,1)\}$
14. $\{(0,0),(1,0),(1,1)\}$
15. $\{(0,1),(1,0),(1,1)\}$
16. $\{(0,0),(0,1),(1,0),(1,1)\}$

44. We list the relations by number as given in the solution above.
a) 8, 13, 14, 16 **b)** 1, 3, 4, 9 **c)** 1, 2, 5, 8, 9, 12, 15, 16
d) 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14 **e)** 1, 3, 4 **f)** 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 16

46. This is similar to Example 16 in this section. A relation on a set S with n elements is a subset of $S \times S$. Since $S \times S$ has n^2 elements, so there are 2^{n^2} relations on S if no restrictions are imposed. One might observe here that the condition that $a \neq b$ is not relevant.

a) Half of these relations contain (a,b) and half do not, so the answer is $2^{n^2}/2 = 2^{n^2-1}$. Looking at it another way, we see that there are $n^2 - 1$ choices involved in specifying such a relation, since we have no choice about (a,b).

b) The analysis and answer are exactly the same as in part **(a)**.

c) Of the n^2 possible pairs to put in R, exactly n of them have a as their first element. We must use none of these, so there are $n^2 - n$ pairs that we are free to work with. Therefore there are 2^{n^2-n} possible choices for R.

d) By part **(c)** we know that there are 2^{n^2-n} relations that do not contain at least one ordered pair with a as its first element, so all the other relations, namely $2^{n^2} - 2^{n^2-n}$ of them, do contain at least one ordered pair with a as its first element.

e) We reason as in part **(c)**. There are n ordered pairs that have a as their first element, and n more that have b as their second element, although this counts (a,b) twice, so there are a total of $2n-1$ pairs that violate the condition. This means that there are $n^2 - 2n + 1 = (n-1)^2$ pairs that we are free to choose for R. Thus the answer is $2^{(n-1)^2}$. Another way to look at this is to visualize the matrix representing R. The a^{th} row must be all 0's, as must the b^{th} column. If we cross out that row and column we have in effect an $n-1$ by $n-1$ matrix, with $(n-1)^2$ entries. Since we can fill each entry with either a 0 or a 1, there are $2^{(n-1)^2}$ choices for specifying S.

f) This is the opposite condition from part **(e)**. Therefore reasoning as in part **(d)**, we have $2^{n^2} - 2^{(n-1)^2}$ possible relations.

48. a) There are two relations on a set with only one element, and they are both transitive.
b) There are 16 relations on a set with two elements, and we saw in Exercise 42f that 13 of them are transitive.
c) For $n = 3$ there are $2^{3^2} = 512$ relations. One way to find out how many of them are transitive is to use

a computer to generate them all and check each one for transitivity. If we do this, then we find that 171 of them are transitive. Doing this by hand is not pleasant, since there are many cases to consider.

50. **a)** Since R contains all the pairs (x,x), so does $R \cup S$. Therefore $R \cup S$ is reflexive.
b) Since R and S each contain all the pairs (x,x), so does $R \cap S$. Therefore $R \cap S$ is reflexive.
c) Since R and S each contain all the pairs (x,x), we know that $R \oplus S$ contains none of these pairs. Therefore $R \oplus S$ is irreflexive.
d) Since R and S each contain all the pairs (x,x), we know that $R - S$ contains none of these pairs. Therefore $R - S$ is irreflexive.
e) Since R and S each contain all the pairs (x,x), so does $S \circ R$. Therefore $S \circ R$ is reflexive.

52. By definition, to say that R is antisymmetric is to say that $R \cap R^{-1}$ contains only pairs of the form (a,a). The statement we are asked to prove is just a rephrasing of this.

54. This is immediate from the definition, since R is reflexive if and only if it contains all the pairs (x,x), which in turn happens if and only if $\overline{R}$ contains none of these pairs, i.e., $\overline{R}$ is irreflexive.

56. We just apply the definition each time. We find that R^2 contains all the pairs in $\{1,2,3,4,5\} \times \{1,2,3,4,5\}$ except $(2,3)$ and $(4,5)$; and R^3, R^4, and R^5 contain all the pairs.

58. We prove this by induction on n. There is nothing to prove in the basis step ($n = 1$). Assume the inductive hypothesis that R^n is symmetric, and let $(a,c) \in R^{n+1} = R^n \circ R$. Then there is a $b \in A$ such that $(a,b) \in R$ and $(b,c) \in R^n$. Since R^n and R are symmetric, $(b,a) \in R$ and $(c,b) \in R^n$. Thus by definition $(c,a) \in R \circ R^n$. We will have completed the proof if we can show that $R \circ R^n = R^{n+1}$. This we do in two steps. First, composition of relations is associative, that is, $(R \circ S) \circ T = R \circ (S \circ T)$ for all relations with appropriate domains and codomains. (The proof of this is straightforward applications of the definition.) Second we show that $R \circ R^n = R^{n+1}$ by induction on n. Again the basis step is trivial. Under the inductive hypothesis, then, $R \circ R^{n+1} = R \circ (R^n \circ R) = (R \circ R^n) \circ R = R^{n+1} \circ R = R^{n+2}$, as desired.

SECTION 9.2 *n*-ary Relations and Their Applications

2. We have to find all the solutions to this equation, making sure to include all the permutations. The 4-tuples are $(6,1,1,1)$, $(1,6,1,1)$, $(1,1,6,1)$, $(1,1,1,6)$, $(3,2,1,1)$, $(3,1,2,1)$, $(3,1,1,2)$, $(2,3,1,1)$, $(2,1,3,1)$, $(2,1,1,3)$, $(1,3,2,1)$, $(1,3,1,2)$, $(1,2,3,1)$, $(1,2,1,3)$, $(1,1,3,2)$, and $(1,1,2,3)$.

4. Primary keys are the domains that have all different entries.
a) The only primary key is *Course*. **b)** The only primary key is *Course_number*.
c) The only primary key is *Course_number*. **d)** The only primary key is *Departure_time*.

6. We see that the *Professor* field by itself is not a key, since there is more than one 5-tuple containing the same professor. We can make the identification of the tuple unique by including the course number as well, or by including the time as well. Thus either *Professor–Course_number* or *Professor–Time* will work. Note, however, that either of these might not work if more data are added, since different departments can have the same course number, and a professor can be teaching two courses in the same room at the same time (e.g., a graduate course and the undergraduate version of that same course).

8. **a)** The ISBN is unique for each book, and it is probably the one and only primary key (and certainly the best one in any case).

b) This would work as long as there were not two books published the same year (date is usually given only as a year) with the same title. In practice, this could easily not happen.

c) This would work as long as there were not two books with the same title and the same number of pages. In practice, this could possibly not happen, although it is perhaps less likely than in part **(b)**.

10. The selection operator picks out all the tuples that match the criteria. The 5-tuples in Table 7 that have A100 as their room are (Cruz, Zoology, 335, A100, 9: 00 A.M.), (Cruz, Zoology, 412, A100, 8: 00 A.M.), and (Farber, Psychology, 501, A100, 3: 00 P.M.).

12. The selection operator picks out all the tuples that match the criteria. There is only one 4-tuple in Table 10 that has a quantity of at least 50 and project number 2, namely $(9191, 2, 80, 4)$.

14. We keep only the second, third, and fifth columns, obtaining (b, c, e).

16. The table uses columns 1, 2, and 4 of Table 8. We start by deleting columns 3 and 5 from Table 8. Since no rows are duplicates of earlier rows, this table is the answer.

Airline	*Flight_number*	*Destination*
Nadir	122	Detroit
Acme	221	Denver
Acme	122	Anchorage
Acme	323	Honolulu
Nadir	199	Detroit
Acme	222	Denver
Nadir	322	Detroit

18. By definition, there are $5 + 8 - 3 = 10$ components.

20. Both sides of this equation pick out the subset of R consisting of those n-tuples satisfying both conditions C_1 and C_2. This follows immediately from the definitions of conjunction and the selection operator.

22. Both sides of this equation pick out the set of n-tuples that satisfy condition C, and furthermore are in R or S (or both, of course). This follows immediately from the definitions of union and the selection operator.

24. Both sides of this equation pick out the set of n-tuples that satisfy condition C, and are in R and are not in S. This follows immediately from the definitions of set difference and the selection operator.

26. Note that we lose information when we delete columns. Therefore we might have more in the second set than in the first, since it could be easier to be in the intersection in the second case. A simple example would be to let $R = \{(a, b)\}$ and $S = \{(a, c)\}$, $n = 2$, $m = 1$, and $i_1 = 1$. Then $R \cap S = \emptyset$, so $P_1(R \cap S) = \emptyset$. On the other hand, $P_1(R) = P_1(S) = \{(a)\}$, so $P_1(R) \cap P_1(S) = \{(a)\}$.

28. This is similar to Example 13.

a) We apply the selection operator with the condition "$1000 \leq$ Part_number ≤ 5000" to the 3-tuples given in Table 9, picking out those rows that have a part number in the indicated range. Then we choose the supplier field from those rows, and delete duplicates.

b) Five of the 3-tuples in the joined database satisfy the condition, namely $(23, 1092, 1)$, $(23, 1101, 3)$, $(31, 4975, 3)$, $(31, 3477, 2)$, and $(33, 1001, 1)$. The suppliers appearing here are $23, 31, 33$.

30. A primary key is a domain whose value determines the values of all the other domains. For this relation, this does not happen. The first domain is not a primary key, because, for example, the triples $(1,2,3)$ and $(1,3,5)$ are both in the relation (the terms form an arithmetic progression). Similarly, the triples $(1,3,5)$ and $(2,3,4)$ are both in the relation, so the second domain is not a key; and the triples $(1,3,5)$ and $(3,4,5)$ are both in the relation, so the third domain is not a key.

32. The primary key uniquely determines the n-tuple. Thus we can think of the n-tuple as a pair consisting of the primary key (in whichever field it lies) followed by the $(n-1)$-tuple consisting of the values from the other domains. The set of all such pairs is by definition the graph of the function from the subset of the domain of the primary key consisting of those values that appear, to the Cartesian product of the other $n-1$ domains.

SECTION 9.3 Representing Relations

2. In each case we use a 4×4 matrix, putting a 1 in position (i,j) if the pair (i,j) is in the relation and a 0 in position (i,j) if the pair (i,j) is not in the relation.

a) $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ **b)** $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ **c)** $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ **d)** $\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

4. a) Since the $(1,1)^{\text{th}}$ entry is a 1, $(1,1)$ is in the relation. Since $(1,3)^{\text{th}}$ entry is a 0, $(1,3)$ is not in the relation. Continuing in this manner, we see that the relation contains $(1,1)$, $(1,2)$, $(1,4)$, $(2,1)$, $(2,3)$, $(3,2)$, $(3,3)$, $(3,4)$, $(4,1)$, $(4,3)$, and $(4,4)$.

b) $(1,1)$, $(1,2)$, $(1,3)$, $(2,2)$, $(3,3)$, $(3,4)$, $(4,1)$, and $(1,4)$

c) $(1,2)$, $(1,4)$, $(2,1)$, $(2,3)$, $(3,2)$, $(3,4)$, $(4,1)$, and $(4,3)$

6. An asymmetric relation (see the preamble to Exercise 18 in Section 9.1) is one for which $(a,b) \in R$ and $(b,a) \in R$ can never hold simultaneously, even if $a = b$. In the matrix, this means that there are no 1's on the main diagonal (position m_{ii} for some i), and there is no pair of 1's symmetrically placed around the main diagonal (i.e., we cannot have $m_{ij} = m_{ji} = 1$ for any values of i and j).

8. For reflexivity we want all 1's on the main diagonal; for irreflexivity we want all 0's on the main diagonal; for symmetry, we want the matrix to be symmetric about the main diagonal (equivalently, the matrix equals its transpose); for antisymmetry we want there never to be two 1's symmetrically placed about the main diagonal (equivalently, the meet of the matrix and its transpose has no 1's off the main diagonal); and for transitivity we want the Boolean square of the matrix (the Boolean product of the matrix and itself) to be "less than or equal to" the original matrix in the sense that there is a 1 in the original matrix at every location where there is a 1 in the Boolean square.

a) Since some 1's and some 0's on the main diagonal, this relation is neither reflexive nor irreflexive. Since the matrix is symmetric, the relation is symmetric. The relation is not antisymmetric—look at positions $(1,2)$ and $(2,1)$. Finally, the relation is not transitive; for example, the 1's in positions $(1,2)$ and $(2,3)$ would require a 1 in position $(1,3)$ if the relation were to be transitive.

b) Since there are all 1's on the main diagonal, this relation is reflexive and not irreflexive. Since the matrix is not symmetric, the relation is not symmetric (look at positions $(1,2)$ and $(2,1)$, for example). The relation is antisymmetric since there are never two 1's symmetrically placed with respect to the main diagonal. Finally, the Boolean square of this matrix is not itself (look at position $(1,4)$ in the square), so the relation is not transitive.

c) Since there are all 0's on the main diagonal, this relation is not reflexive but is irreflexive. Since the matrix is symmetric, the relation is symmetric. The relation is not antisymmetric—look at positions $(1,2)$ and $(2,1)$, for example. Finally, the Boolean square of this matrix has a 1 in position $(1,1)$, so the relation is not transitive.

10. Note that the total number of entries in the matrix is $1000^2 = 1{,}000{,}000$.

a) There is a 1 in the matrix for each pair of distinct positive integers not exceeding 1000, namely in position (a,b) where $a \le b$, as well as 1's along the diagonal. Thus the answer is the number of subsets of size 2 from a set of 1000 elements, plus 1000, i.e., $C(1000,2) + 1000 = 499500 + 1000 = 500{,}500$.

b) There two 1's in each row of the matrix except the first and last rows, in which there is one 1. Therefore the answer is $998 \cdot 2 + 2 = 1998$.

c) There is a 1 in the matrix at each entry just above and to the left of the "anti-diagonal" (i.e., in positions $(1,999)$, $(2,998)$, ..., $(999,1)$. Therefore the answer is 999.

d) There is a 1 in the matrix at each entry on or above (to the left of) the "anti-diagonal." This is the same number of 1's as in part **(a)**, so the answer is again 500,500.

e) The condition is trivially true (since $1 \le a \le 1000$), so all 1,000,000 entries are 1.

12. We take the transpose of the matrix, since we want the $(i,j)^{\text{th}}$ entry of the matrix for R^{-1} to be 1 if and only if the $(j,i)^{\text{th}}$ entry of R is 1.

14. a) The matrix for the union is formed by taking the join: $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

b) The matrix for the intersection is formed by taking the meet: $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

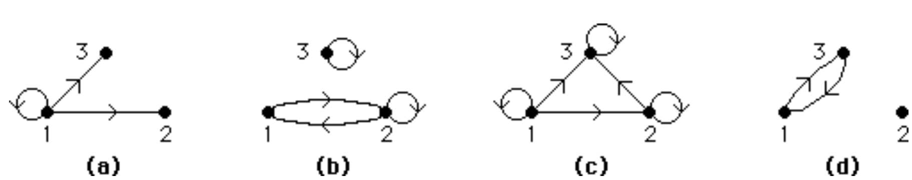
c) The matrix is the Boolean product $\mathbf{M}_{R_1} \odot \mathbf{M}_{R_2} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

d) The matrix is the Boolean product $\mathbf{M}_{R_1} \odot \mathbf{M}_{R_1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

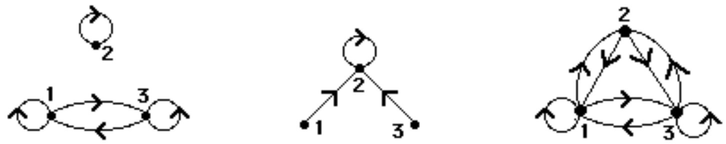
e) The matrix is the entrywise XOR: $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

16. Since the matrix for R^{-1} is just the transpose of the matrix for R (see Exercise 12), the entries are the same collection of 0's and 1's, so there are k nonzero entries in $\mathbf{M}_{R^{-1}}$ as well.

18. We draw the directed graphs, in each case with the vertex set being $\{1,2,3\}$ and an edge from i to j whenever (i,j) is in the relation.

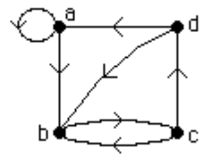


20. In each case we draw a directed graph on three vertices with an edge from a to b for each pair (a,b) in the relation, i.e., whenever there is a 1 in position (a,b) in the matrix. In part **(a)**, for instance, we need an edge from 1 to itself since there is a 1 in position $(1,1)$ in the matrix, and an edge from 1 to 3, but no edge from 1 to 2.



(a) (b) (c)

22. We draw the directed graph with the vertex set being $\{a,b,c,d\}$ and an edge from i to j whenever (i,j) is in the relation.



24. We list all the pairs (x,y) for which there is an edge from x to y in the directed graph: $\{(a,a),(a,c),(b,a),(b,b),(b,c),(c,c)\}$.

26. We list all the pairs (x,y) for which there is an edge from x to y in the directed graph: $\{(a,a),(a,b),(b,a),(b,b),(c,a),(c,c),(c,d),(d,d)\}$.

28. We list all the pairs (x,y) for which there is an edge from x to y in the directed graph: $\{(a,a),(a,b),(b,a),(b,b),(c,c),(c,d),(d,c),(d,d)\}$.

30. Clearly R is irreflexive if and only if there are no loops in the directed graph for R.

32. Recall that the relation is reflexive if there is a loop at each vertex; irreflexive if there are no loops at all; symmetric if edges appear only in **antiparallel** pairs (edges from one vertex to a second vertex and from the second back to the first); antisymmetric if there is no pair of antiparallel edges; asymmetric if is both antisymmetric and irreflexive; and transitive if all paths of length 2 (a pair of edges (x,y) and (y,z)) are accompanied by the corresponding path of length 1 (the edge (x,z)). The relation drawn in Exercise 26 is reflexive but not irreflexive since there are loops at each vertex. It is not symmetric, since, for instance, the edge (c,a) is present but not the edge (a,c). It is not antisymmetric, since both edges (a,b) and (b,a) are present. So it is not asymmetric either. It is not transitive, since the path $(c,a),(a,b)$ from c to b is not accompanied by the edge (c,b). The relation drawn in Exercise 27 is neither reflexive nor irreflexive since there are some loops but not a loop at each vertex. It is symmetric, since the edges appear in antiparallel pairs. It is not antisymmetric, since, for instance, both edges (a,b) and (b,a) are present. So it is not asymmetric either. It is not transitive, since edges (c,a) and (a,c) are present, but not (c,c). The relation drawn in Exercise 28 is reflexive and not irreflexive since there are loops at all vertices. It is symmetric but not antisymmetric or asymmetric. It is transitive; the only nontrivial paths of length 2 have the necessary loop shortcuts.

34. For each pair (a,b) of vertices (including the pairs (a,a) in which the two vertices are the same), if there is an edge from a to b, then erase it, and if there is no edge from a to b, put add it in.

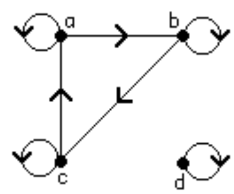
36. We assume that the two relations are on the same set. For the union, we simply take the union of the directed graphs, i.e., take the directed graph on the same vertices and put in an edge from i to j whenever there is an edge from i to j in either of them. For intersection, we simply take the intersection of the directed graphs, i.e., take the directed graph on the same vertices and put in an edge from i to j whenever there are edges from i to j in both of them. For symmetric difference, we simply take the symmetric difference of the directed graphs, i.e., take the directed graph on the same vertices and put in an edge from i to j whenever there is an edge from i to j in one, but not both, of them. Similarly, to form the difference, we take the difference of the directed graphs, i.e., take the directed graph on the same vertices and put in an edge from i to j whenever there is an edge from i to j in the first but not the second. To form the directed graph for the composition $S \circ R$ of relations R and S, we draw a directed graph on the same set of vertices and put in an edge from i to j whenever there is a vertex k such that there is an edge from i to k in R, and an edge from k to j in S.

SECTION 9.4 Closures of Relations

2. When we add all the pairs (x,x) to the given relation we have all of $\mathbf{Z} \times \mathbf{Z}$; in other words, we have the relation that always holds.

4. To form the reflexive closure, we simply need to add a loop at each vertex that does not already have one.

6. We form the reflexive closure by taking the given directed graph and appending loops at all vertices at which there are not already loops.



8. To form the digraph of the symmetric closure, we simply need to add an edge from x to y whenever this edge is not already in the directed graph but the edge from y to x is.

10. The symmetric closure was found in Example 2 to be the "is not equal to" relation. If we now make this relation reflexive as well, we will have the relation that always holds.

12. $\mathbf{M}_R \vee \mathbf{I}_n$ is by definition the same as $\mathbf{M}_R$ except that it has all 1's on the main diagonal. This must represent the reflexive closure of R, since this closure is the same as R except for the addition of all the pairs (x,x) that were not already present.

14. Suppose that the closure C exists. We must show that C is the intersection I of all the relations S that have property $\mathbf{P}$ and contain R. Certainly $I \subseteq C$, since C is one of the sets in the intersection. Conversely, by definition of closure, C is a subset of every relation S that has property $\mathbf{P}$ and contains R; therefore C is contained in their intersection.

16. In each case, the sequence is a path if and only if there is an edge from each vertex in the sequence to the vertex following it.

a) This is a path. **b)** This is not a path (there is no edge from e to c). **c)** This is a path.
d) This is not a path (there is no edge from d to a). **e)** This is a path.
f) This is not a path (there is no loop at b).

18. In the language of Chapter 10, this digraph is strongly connected, so there will be a path from every vertex to every other vertex.

a) One path is a, b. **b)** One path is b, e, a. **c)** One path is b, c, b; a shorter one is just b.

d) One path is a, b, e. **e)** One path is b, e, d. **f)** One path is c, e, d.

g) One path is d, e, d. Another is the path of length 0 from d to itself.

h) One path is e, a. Another is $e, a, b, e, a, b, e, a, b, e, a$. **i)** One path is e, a, b, c.

20. **a)** The pair (a, b) is in R^2 precisely when there is a city c such that there is a direct flight from a to c and a direct flight from c to b—in other words, when it is possible to fly from a to b with a scheduled stop (and possibly a plane change) in some intermediate city.

b) The pair (a, b) is in R^3 precisely when there are cities c and d such that there is a direct flight from a to c, a direct flight from c to d, and a direct flight from d to b—in other words, when it is possible to fly from a to b with two scheduled stops (and possibly a plane change at one or both) in intermediate cities.

c) The pair (a, b) is in R^* precisely when it is possible to fly from a to b.

22. Since $R \subseteq R^*$, clearly if $\Delta \subseteq R$, then $\Delta \subseteq R^*$.

24. It is certainly possibly for R^2 to contain some pairs (a, a). For example, let $R = \{(1,2),(2,1)\}$.

26. **a)** We show the various matrices that are involved. First,

$$\mathbf{A} = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{bmatrix}, \quad \mathbf{A}^{[2]} \begin{bmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&1&0&0&0 \end{bmatrix}, \text{ and } \mathbf{A}^{[3]} = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{bmatrix} = \mathbf{A}.$$

It follows that $\mathbf{A}^{[4]} = \mathbf{A}^{[2]}$ and $\mathbf{A}^{[5]} = \mathbf{A}^{[3]}$. Therefore the answer $\mathbf{B}$, the meet of all the $\mathbf{A}$'s, is $\mathbf{A} \vee \mathbf{A}^{[2]}$, namely

$$\begin{bmatrix} 1&0&1&0&0\\ 0&1&0&1&0\\ 1&0&1&0&0\\ 0&1&0&1&0\\ 0&1&0&1&0 \end{bmatrix}.$$

b) For this and the remaining parts we just exhibit the matrices that arise.

$$\mathbf{A} = \begin{bmatrix} 0&0&0&0&0\\ 0&0&1&0&1\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&1&0&0 \end{bmatrix} \quad \mathbf{A}^{[2]} = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&1&1&0&0\\ 0&0&0&0&0\\ 0&0&1&0&1 \end{bmatrix} \quad \mathbf{A}^{[3]} = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&0&1&0&1\\ 0&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix}$$

$$\mathbf{A}^{[4]} = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&1&1&0&1\\ 0&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix} = \mathbf{A}^{[5]} \qquad \mathbf{B} = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&1&1&0&1\\ 1&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix}$$

c)

$$\mathbf{A} = \begin{bmatrix} 0&1&1&0&1\\ 1&0&1&0&0\\ 1&1&0&0&0\\ 1&0&0&0&0\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{A}^{[2]} = \begin{bmatrix} 1&1&1&1&0\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 0&1&1&0&1\\ 1&0&0&0&0 \end{bmatrix} \quad \mathbf{A}^{[3]} = \begin{bmatrix} 1&1&1&0&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&0\\ 0&1&1&0&1 \end{bmatrix}$$

$$\mathbf{A}^{[4]} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&0&1\\ 1&1&1&1&0 \end{bmatrix} \quad \mathbf{A}^{[5]} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&0&1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{bmatrix}$$

d)

$$\mathbf{A} = \begin{bmatrix} 0&0&0&0&1\\ 1&0&0&1&0\\ 0&0&0&1&0\\ 1&0&1&0&0\\ 1&1&1&0&1 \end{bmatrix} \quad \mathbf{A}^{[2]} = \begin{bmatrix} 1&1&1&0&1\\ 1&0&1&0&1\\ 1&0&1&0&0\\ 0&0&0&1&1\\ 1&1&1&1&1 \end{bmatrix} \quad \mathbf{A}^{[3]} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 0&0&0&1&1\\ 1&1&1&0&1\\ 1&1&1&1&1 \end{bmatrix}$$

$$\mathbf{A}^{[4]} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&0&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{bmatrix} \quad \mathbf{A}^{[5]} = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{bmatrix} = \mathbf{B}$$

28. We compute the matrices $\mathbf{W}_i$ for $i = 0, 1, 2, 3, 4, 5$, and then $\mathbf{W}_5$ is the answer.

a)

$$\mathbf{W}_0 = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{W}_1 = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 1&0&1&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{W}_2 = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 1&0&1&0&0\\ 0&1&0&1&0\\ 0&0&0&1&0 \end{bmatrix}$$

$$\mathbf{W}_3 = \begin{bmatrix} 1&0&1&0&0\\ 0&0&0&1&0\\ 1&0&1&0&0\\ 0&1&0&1&0\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{W}_4 = \begin{bmatrix} 1&0&1&0&0\\ 0&1&0&1&0\\ 1&0&1&0&0\\ 0&1&0&1&0\\ 0&1&0&1&0 \end{bmatrix} = \mathbf{W}_5$$

b)

$$\mathbf{W}_0 = \begin{bmatrix} 0&0&0&0&0\\ 0&0&1&0&1\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&1&0&0 \end{bmatrix} = \mathbf{W}_1 \quad \mathbf{W}_2 = \begin{bmatrix} 0&0&0&0&0\\ 0&0&1&0&1\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix} = \mathbf{W}_3 = \mathbf{W}_4$$

$$\mathbf{W}_5 = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&1&1&0&1\\ 1&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix}$$

c)

$$\mathbf{W}_0 = \begin{bmatrix} 0&1&1&0&1\\ 1&0&1&0&0\\ 1&1&0&0&0\\ 1&0&0&0&0\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{W}_1 = \begin{bmatrix} 0&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 0&0&0&1&0 \end{bmatrix} \quad \mathbf{W}_2 = \begin{bmatrix} 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 0&0&0&1&0 \end{bmatrix} = \mathbf{W}_3$$

$$\mathbf{W}_4 = \begin{bmatrix} 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&0&1\\ 1&1&1&1&1 \end{bmatrix} \quad \mathbf{W}_5 = \begin{bmatrix} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{bmatrix}$$

d)

$$\mathbf{W}_0 = \begin{bmatrix} 0&0&0&0&1\\ 1&0&0&1&0\\ 0&0&0&1&0\\ 1&0&1&0&0\\ 1&1&1&0&1 \end{bmatrix} \quad \mathbf{W}_1 = \begin{bmatrix} 0&0&0&0&1\\ 1&0&0&1&1\\ 0&0&0&1&0\\ 1&0&1&0&1\\ 1&1&1&0&1 \end{bmatrix} \quad \mathbf{W}_2 = \begin{bmatrix} 0&0&0&0&1\\ 1&0&0&1&1\\ 0&0&0&1&0\\ 1&0&1&0&1\\ 1&1&1&1&1 \end{bmatrix}$$

$$\mathbf{W}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \mathbf{W}_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \mathbf{W}_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

30. Let m be the length of the shortest path from a to b, and let $a = x_0, x_1, \ldots, x_{m-1}, x_m = b$ be such a path. If $m > n-1$, then $m \geq n$, so $m+1 \geq n+1$, which means that not all of the vertices x_0, x_1, x_2, $\ldots$, x_m are distinct. Thus $x_i = x_j$ for some i and j with $0 \leq i < j \leq m$ (but not both $i = 0$ and $j = m$, since $a \neq b$). We can then excise the circuit from x_i to x_j, leaving a shorter path from a to b, namely $x_0, \ldots, x_i, x_{j+1}, \ldots, x_m$. This contradicts the choice of m. Therefore $m \leq n-1$, as desired.

32. Warshall's algorithm determines the existence of paths. If instead we keep track of the lengths of paths, then we can get the desired information. Thus we make the following changes in Algorithm 2. First, instead of initializing $\mathbf{W}$ to be $\mathbf{M}_R$, we initialize it to be $\mathbf{M}_R$ with each 0 replaced by ∞. Second, the computational step becomes $w_{ij} := \min(w_{ij}, w_{ik} + w_{kj})$.

34. All we need to do is make sure that all the pairs (x, x) are included. An easy way to accomplish this is to add them at the end, by setting $\mathbf{W} := \mathbf{W} \vee \mathbf{I}_n$.

SECTION 9.5 Equivalence Relations

2. **a)** This is an equivalence relation by Exercise 9 ($f(x)$ is x's age).

b) This is an equivalence relation by Exercise 9 ($f(x)$ is x's parents).

c) This is not an equivalence relation, since it need not be transitive. (We assume that biological parentage is at issue here, so it is possible for A to be the child of W and X, B to be the child of X and Y, and C to be the child of Y and Z. Then A is related to B, and B is related to C, but A is not related to C.)

d) This is not an equivalence relation since it is clearly not transitive.

e) Again, just as in part **(c)**, this is not transitive.

4. One relation is that a and b are related if they were born in the same U.S. state (with "not in a state of the U.S." counting as one state). Here the equivalence classes are the nonempty sets of students from each state. Another example is for a to be related to b if a and b have lived the same number of complete decades. The equivalence classes are the set of all 10-to-19 year-olds, the set of all 20-to-29 year-olds, and so on (the sets among these that are nonempty, that is). A third example is for a to be related to b if 10 is a divisor of the difference between a's age and b's age, where "age" means the whole number of years since birth, as of the first day of class. For each $i = 0, 1, \ldots, 9$, there is the equivalence class (if it is nonempty) of those students whose age ends with the digit i.

6. One way to partition the classes would be by level. At many schools, classes have three-digit numbers, the first digit of which is approximately the level of the course, so that courses numbered 100–199 are taken by freshman, 200–299 by sophomores, and so on. Formally, two classes are related if their numbers have the same digit in the hundreds column; the equivalence classes are the set of all 100-level classes, the set of all 200-level classes, and so on. A second example would focus on department. Two classes are equivalent if they are offered by the same department; for example, MATH 154 is equivalent to MATH 372, but not to EGR 141. The equivalence classes are the sets of classes offered by each department (the set of math classes, the set of engineering classes, and so on). A third—and more egocentric—classification would be to have one equivalence class be the set of classes that you have completed successfully and the other equivalence class to be all the other classes. Formally, two classes are equivalent if they have the same answer to the question, "Have I completed this class successfully?"

8. Recall (Definition 1 in Section 2.5) that two sets have the same cardinality if there is a bijection (one-to-one and onto function) from one set to the other. We must show that R is reflexive, symmetric, and transitive. Every set has the same cardinality as itself because of the identity function. If f is a bijection from S to T, then f^{-1} is a bijection from T to S, so R is symmetric. Finally, if f is a bijection from S to T and g is a bijection from T to U, then $g \circ f$ is a bijection from T to U, so R is transitive (see Exercise 33 in Section 2.3).

The equivalence class of $\{1, 2, 3\}$ is the set of all three-element sets of real numbers, including such sets as $\{4, 25, 1948\}$ and $\{e, \pi, \sqrt{2}\}$. Similarly, $[\mathbf{Z}]$ is the set of all infinite countable sets of real numbers (see Section 2.5), such as the set of natural numbers, the set of rational numbers, and the set of the prime numbers, but not including the set $\{1, 2, 3\}$ (it's too small) or the set of all real numbers (it's too big). See Section 2.5 for more on countable sets.

10. The function that sends each $x \in A$ to its equivalence class $[x]$ is obviously such a function.

12. This follows from Exercise 9, where f is the function that takes a bit string of length $n \geq 3$ to its last $n - 3$ bits.

14. This follows from Exercise 9, where f is the function that takes a string of uppercase and lowercase English letters and changes all the lower case letters to their uppercase equivalents (and leaves the uppercase letters unchanged).

16. This follows from Exercise 9, where f is the function from the set of pairs of positive integers to the set of positive rational numbers that takes (a, b) to a/b, since clearly $ad = bc$ if and only if $a/b = c/d$.

If we want an explicit proof, we can argue as follows. For reflexivity, $((a, b), (a, b)) \in R$ because $a \cdot b = b \cdot a$. If $((a, b), (c, d)) \in R$ then $ad = bc$, which also means that $cb = da$, so $((c, d), (a, b)) \in R$; this tells us that R is symmetric. Finally, if $((a, b), (c, d)) \in R$ and $((c, d), (e, f)) \in R$ then $ad = bc$ and $cf = de$. Multiplying these equations gives $acdf = bcde$, and since all these numbers are nonzero, we have $af = be$, so $((a, b), (e, f)) \in R$; this tells us that R is transitive.

18. **a)** This follows from Exercise 9, where the function f from the set of polynomials to the set of polynomials is the operator that takes the derivative n times—i.e., f of a function g is the function $g^{(n)}$. The best way to think about this is that any relation defined by a statement of the form "a and b are equivalent if they have the same whatever" is an equivalence relation. Here "whatever" is "n^{th} derivative"; in the general situation of Exercise 9, "whatever" is "function value under f."
b) The third derivative of x^4 is $24x$. Since the third derivative of a polynomial of degree 2 or less is 0, the polynomials of the form $x^4 + ax^2 + bx + c$ have the same third derivative. Thus these are the functions in the same equivalence class as f.

20. This follows from Exercise 9, where the function f from the set of people to the set of Web-traversing behaviors starting at the given particular Web page takes the person to the behavior that person exhibited.

22. We need to observe whether the relation is reflexive (there is a loop at each vertex), symmetric (every edge that appears is accompanied by its antiparallel mate—an edge involving the same two vertices but pointing in the opposite direction), and transitive (paths of length 2 are accompanied by the path of length 1—i.e., edge—between the same two vertices in the same direction). We see that this relation is an equivalence relation, satisfying all three properties. The equivalence classes are $\{a, d\}$ and $\{b, c\}$.

24. **a)** This is not an equivalence relation, since it is not symmetric.

b) This is an equivalence relation; one equivalence class consists of the first and third elements, and the other consists of the second and fourth elements.

c) This is an equivalence relation; one equivalence class consists of the first, second, and third elements, and the other consists of the fourth element.

26. Only part **(a)** and part **(c)** are equivalence relations. In part **(a)** each element is in an equivalence class by itself. In part **(c)** the elements 1 and 2 are in one equivalence class, and 0 and 3 are each in their own equivalence class.

28. Only part **(a)** and part **(d)** are equivalence relations. In part **(a)** there is one equivalence class for each $n \in \mathbf{Z}$, and it contains all those functions whose value at 1 is n. In part **(d)** there really is no good way to describe the equivalence classes. For one thing, the set of equivalence classes is uncountable. For each function $f : \mathbf{Z} \to \mathbf{Z}$, there is the equivalence class consisting of all those functions g for which there is a constant C such that $g(n) = f(n) + C$ for all $n \in \mathbf{Z}$.

30. **a)** all the strings whose first three bits are 010 **b)** all the strings whose first three bits are 101
c) all the strings whose first three bits are 111 **d)** all the strings whose first three bits are 010

32. Since two bit strings are related if and only if they agree in their first and third bits, the equivalence class of a bit string $xyzt$, where x, y, and z are bits and t is a bit string, is the set of all bit strings of the form $xy'zt'$, where y' is any bit and t' is any bit string.

a) the set of all bit strings that start 010 or 000

b) the set of all bit strings that start 101 or 111

c) the set of all bit strings that start 101 or 111

d) the set of all bit strings that start 000 or 010

34. **a)** Since this string has length less than 5, its equivalence class consists only of itself.

b) This is similar to part **(a)**: $[1011]_{R_5} = \{1011\}$.

c) Since this string has length 5, its equivalence class consists of all strings that start 11111.

d) This is similar to part **(c)**: $[01010101]_{R_5} = \{\, 01010s \mid s \text{ is any bit string} \,\}$.

36. In each case, the equivalence class of 4 is the set of all integers congruent to 4, modulo m.

a) $\{\, 4 + 2n \mid n \in \mathbf{Z} \,\} = \{\ldots, -2, 0, 2, 4, \ldots\}$ **b)** $\{\, 4 + 3n \mid n \in \mathbf{Z} \,\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
c) $\{\, 4 + 6n \mid n \in \mathbf{Z} \,\} = \{\ldots, -2, 4, 10, 16, \ldots\}$ **d)** $\{\, 4 + 8n \mid n \in \mathbf{Z} \,\} = \{\ldots, -4, 4, 12, 20, \ldots\}$

38. In each case we need to allow all strings that agree with the given string if we ignore the case in which the letters occur.

a) $\{NO, No, nO, no\}$

b) $\{\,YES, YEs, YeS, Yes, yES, yEs, yeS, yes\}$

c) $\{HELP, HELp, HElP, HElp, HeLP, HeLp, HelP, Help, hELP, hELp, hElP, hElp, heLP, heLp, helP, help\}$

40. **a)** By our observation in the solution to Exercise 16, the equivalence class of $(1, 2)$ is the set of all pairs (a, b) such that the fraction a/b equals $1/2$.

b) Again by our observation, the equivalence classes are the positive rational numbers. (Indeed, this is the way one can rigorously define what a rational number is, and this is why fractions are so difficult for children to understand.)

42. **a)** This is a partition, since it satisfies the definition.
b) This is not a partition, since the subsets are not disjoint.
c) This is a partition, since it satisfies the definition.
d) This is not a partition, since the union of the subsets leaves out 0.

44. **a)** This is clearly a partition. **b)** This is not a partition, since 0 is in neither set.
c) This is a partition by the division algorithm.
d) This is a partition, since the second set mentioned is the set of all number between -100 and 100, inclusive.
e) The first two sets are not disjoint (4 is in both), so this is not a partition.

46. **a)** This is a partition, since it satisfies the definition.
b) This is a partition, since it satisfies the definition.
c) This is not a partition, since the intervals are not disjoint (they share endpoints).
d) This is not a partition, since the union of the subsets leaves out the integers.
e) This is a partition, since it satisfies the definition.
f) This is a partition, since it satisfies the definition. Each equivalence class consists of all real numbers with a fixed fractional part.

48. In each case, we need to list all the pairs we can where both coordinates are chosen from the same subset. We should proceed in an organized fashion, listing all the pairs corresponding to each part of the partition.
a) $\{(a,a),(a,b),(b,a),(b,b),(c,c),(c,d),(d,c),(d,d),(e,e),(e,f),(e,g),(f,e),(f,f),(f,g),(g,e),(g,f),(g,g)\}$
b) $\{(a,a),(b,b),(c,c),(c,d),(d,c),(d,d),(e,e),(e,f),(f,e),(f,f),(g,g)\}$
c) $\{(a,a),(a,b),(a,c),(a,d),(b,a),(b,b),(b,c),(b,d),(c,a),(c,b),(c,c),(c,d),(d,a),(d,b),(d,c),(d,d),$ $(e,e),(e,f),(e,g),(f,e),(f,f),(f,g),(g,e),(g,f),(g,g)\}$
d) $\{(a,a),(a,c),(a,e),(a,g),(c,a),(c,c),(c,e),(c,g),(e,a),(e,c),(e,e),(e,g),(g,a),(g,c),(g,e),(g,g),$ $(b,b),(b,d),(d,b),(d,d),(f,f)\}$

50. We need to show that every equivalence class consisting of people living in the same county (or parish) and same state is contained in an equivalence class of all people living in the same state. This is clear. The equivalence class of all people living in county c in state s is a subset of the set of people living in state s.

52. We are asked to show that every equivalence class for R_4 is a subset of some equivalence class for R_3. Let $[y]_{R_4}$ be an arbitrary equivalence class for R_4. We claim that $[y]_{R_4} \subseteq [y]_{R_3}$; proving this claim finishes the proof. To show that one set is a subset of another set, we choose an arbitrary bit string x in the first set and show that it is also an element of the second set. In this case since $y \in [x]_{R_4}$, we know that y is equivalent to x under R_4, that is, that either $y = x$ or y and x are each at least 4 bits long and agree on their first 4 bits. Because strings that are at least 4 bits long and agree on their first 4 bits perforce are at least 3 bits long and agree on their first 3 bits, we know that either $y = x$ or y and x are each at least 3 bits long and agree on their first 3 bits. This means that y is equivalent to x under R_3, that is, that $y \in [x]_{R_3}$.

54. First, suppose that $R_1 \subseteq R_2$. We must show that P_1 is a refinement of P_2. Let $[a]_{R_1}$ be an equivalence class in P_1. We must show that $[a]_{R_1}$ is contained in an equivalence class in P_2. In fact, we will show that $[a]_{R_1} \subseteq [a]_{R_2}$. To this end, let $b \in [a]_{R_1}$. Then $(a,b) \in R_1 \subseteq R_2$. Therefore $b \in [a]_{R_2}$, as desired.

Conversely, suppose that P_1 is a refinement of P_2. Since $a \in [a]_{R_2}$, the definition of "refinement" forces $[a]_{R_1} \subseteq [a]_{R_2}$ for all $a \in A$. This means that for all $b \in A$ we have $(a,b) \in R_1 \to (a,b) \in R_2$; in other words, $R_1 \subseteq R_2$.

56. **a)** This need not be an equivalence relation, since it need not be transitive.

b) Since the intersection of reflexive, symmetric, and transitive relations also have these properties (see Section 9.1), the intersection of equivalence relations is an equivalence relation.

c) This will never be an equivalence relation on a nonempty set, since it is not reflexive.

58. This exercise is very similar to Exercise 59, and the reader should look at the solution there for details.

a) As in Exercise 59, the motions of the bracelet form a dihedral group, in this case consisting of six motions: rotations of 0°, 120°, and 240°, and three reflections, each keeping one bead fixed and interchanging the other two. The composition of any two of these operations is again one of these operations. The 0° rotation plays the role of the identity, which says that the relation is reflexive. Each operation has an inverse (reflections are their own inverses, the 0° rotation is its own inverse, and the 120° and 240° rotations are inverses of each other); this proves symmetry. And transitivity follows from the group table.

b) The equivalence classes are the indistinguishable bracelets. If we denote a bracelet by the colors of its beads, then these classes can be described as RRR, WWW, BBB, RRW, RRB, WWR, WWB, BBR, BBW, and RWB. Note that once we specify the colors, then every two bracelets with those colors are equivalent. This would not be the case if there were four or more beads, however. For example, in a 4-bead bracelet with two reds and two whites, the bracelet in which the red beads are adjacent is not equivalent to the one in which they are not.

60. **a)** In Exercise 31 of Section 3.2, we showed that $f(x)$ is $\Theta(g(x))$ if and only if $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$. To show that R is reflexive, we need to show that $f(x)$ is $O(f(x))$, which is clear by taking $C = 1$ and $k = 1$ in the definition. Symmetry is immediate from the definition, since if $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$, then $g(x)$ is $O(f(x))$ and $f(x)$ is $O(g(x))$. Finally, transitivity follows immediately from the transitive of the "is big-O of" relation, which was proved in Exercise 17 of Section 3.2.

b) This is the class of all functions that asymptotically (i.e., as $n \to \infty$) grow just as fast as a multiple of $f(n) = n^2$. So, for example, functions such as $g(n) = 5n^2 + \log n$, or $g(n) = (n^3 - 17)/(100n + 10^{10})$ belong to this class, but $g(n) = n^{2.01}$ does not (it grows too fast), and $g(n) = n^2/\log n$ does not (it grows too slowly). Another way to express this class is to say that it is the set of all functions g such that there exist constants positive C_1 and C_2 such that the ratio $f(n)/g(n)$ always lies between C_1 and C_2.

62. We will count partitions instead, since equivalence relations are in one-to-one correspondence with partitions. Without loss of generality let the set be $\{1,2,3,4\}$. There is 1 partition in which all the elements are in the same set, namely $\{\{1,2,3,4\}\}$. There are 4 partitions in which the sizes of the sets are 1 and 3, namely $\{\{1\},\{2,3,4\}\}$ and three more like it. There are 3 partitions in which the sizes of the sets are 2 and 2, namely $\{\{1,2\},\{3,4\}\}$ and two more like it. There are 6 partitions in which the sizes of the sets are 2, 1, and 1, namely $\{\{1,2\},\{3\},\{4\}\}$ and five more like it. Finally, there is 1 partition in which all the elements are in separate sets. This gives a total of 15. To actually list the 15 relations would be tedious.

64. No. Here is a counterexample. Start with $\{(1,2),(3,2)\}$ on the set $\{1,2,3\}$. Its transitive closure is itself. The reflexive closure of that is $\{(1,1),(1,2),(2,2),(3,2),(3,3)\}$. The symmetric closure of that is $\{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3)\}$. The result is not transitive; for example, $(1,3)$ is missing. Therefore this is not an equivalence relation.

66. We end up with the original partition P.

68. We will develop this recurrence relation in the context of partitions of the set $\{1,2,\ldots,n\}$. Note that $p(0) = 1$, since there is only one way to partition the empty set (namely, into the empty collection of subsets). For warm-up, we also note that $p(1) = 1$, since $\{\{1\}\}$ is the only partition of $\{1\}$; that $p(2) = 2$, since we can partition $\{1,2\}$ either as $\{\{1,2\}\}$ or as $\{\{1\},\{2\}\}$; and that $p(3)=5$, since there are the following partitions: $\{\{1,2,3\}\}$, $\{\{1,2\},\{3\}\}$, $\{\{1,3\},\{2\}\}$, $\{\{2,3\},\{1\}\}$, $\{\{1\},\{2\},\{3\}\}$. Now to partition $\{1,2,\ldots,n\}$, we first decide how many other elements of this set will go into the same subset as n goes into. Call this number j, and note that j can take any value from 0 through $n-1$. Once we have determined j, we can specify the partition by deciding on the subset of j elements from $\{1,2,\ldots,n-1\}$ that will go into the same subset as n (and this can be done in $C(n-1,j)$ ways), and then we need to decide how to partition the remaining $n-1-j$ elements (and this can be done in $p(n-j-1)$ ways). The given recurrence relation now follows.

SECTION 9.6 Partial Orderings

2. The question in each case is whether the relation is reflexive, antisymmetric, and transitive. Suppose the relation is called R.

a) This relation is not reflexive because 1 is not related to itself. Therefore R is not a partial ordering. The relation is antisymmetric, because the only way for a to be related to b is for a to equal b. Similarly, the relation is transitive, because if a is related to b, and b is related to c, then necessarily $a=b=c\neq 1$ so a is related to c.

b) This is a partial ordering, because it is reflexive and the pairs $(2,0)$ and $(2,3)$ will not introduce any violations of antisymmetry or transitivity.

c) This is not a partial ordering, because it is not transitive: $3\,R\,1$ and $1\,R\,2$, but 3 is not related to 2. It is reflexive and the pairs $(1,2)$ and $(3,1)$ will not introduce any violations of antisymmetry.

d) This is not a partial ordering, because it is not transitive: $1\,R\,2$ and $2\,R\,0$, but 1 is not related to 0. It is reflexive and the nonreflexive pairs will not introduce any violations of antisymmetry.

e) The relation is clearly reflexive, but it is not antisymmetric ($0\,R\,1$ and $1\,R\,0$, but $0\neq 1$) and not transitive ($2\,R\,0$ and $0\,R\,1$, but 2 is not related to 1).

4. The question in each case is whether the relation is reflexive, antisymmetric, and transitive.

a) Since there surely are unequal people of the same height (to whatever degree of precision heights are measured), this relation is not antisymmetric, so (S,R) cannot be a poset.

b) Since nobody weighs more than herself, this relation is not reflexive, so (S,R) cannot be a poset.

c) This is a poset. The equality clause in the definition of R guarantees that R is reflexive. To check antisymmetry and transitivity it suffices to consider unequal elements (these rules hold for equal elements trivially). If a is a descendant of b, then b cannot be a descendant of a (for one thing, a descendant needs to be born after any ancestor), so the relation is vacuously antisymmetric. If a is a descendant of b, and b is a descendant of c, then by the way "descendant" is defined, we know that a is a descendant of c; thus R is transitive.

d) This relation is not reflexive, because anyone and himself have a common friend.

6. The question in each case is whether the relation is reflexive, antisymmetric, and transitive.

a) The equality relation on any set satisfies all three conditions and is therefore a partial order. (It is the smallest partial order; reflexivity insures that every partial order contains at least all the pairs (a,a).)

b) This is not a poset, since the relation is not reflexive, although it is antisymmetric and transitive. Any relation of this sort can be turned into a partial ordering by adding in all the pairs (a,a).

c) This is a poset, very similar to Example 1.

d) This is not a poset, since the relation is not reflexive, not antisymmetric, and not transitive (the absence of one of these properties would have been enough to give a negative answer).

8. **a)** This relation is $\{(1,1),(1,3),(2,1),(2,2),(3,3)\}$. It is clearly reflexive and antisymmetric. The only pairs that might present problems with transitivity are the nondiagonal pairs, $(2,1)$ and $(1,3)$. If the relation were to be transitive, then we would also need the pair $(2,3)$ in the relation. Since it is not there, the relation is not a partial order.

b) Reasoning as in part **(a)**, we see that this relation is a partial order, since the pair $(3,1)$ can cause no problem with transitivity.

c) A little trial and error shows that this relation is not transitive ($(1,3)$ and $(3,4)$ are present, but not $(1,4)$) and therefore not a partial order.

10. This relation is not transitive (there is no arrow from c to b), so it is not a partial order.

12. This follows immediately from the definition. Clearly R^{-1} is reflexive if R is. For antisymmetry, suppose that $(a,b) \in R^{-1}$ and $a \neq b$. Then $(b,a) \in R$, so $(a,b) \notin R$, whence $(b,a) \notin R^{-1}$. Finally, if $(a,b) \in R^{-1}$ and $(b,c) \in R^{-1}$, then $(b,a) \in R$ and $(c,b) \in R$, so $(c,a) \in R$ (since R is transitive), and therefore $(a,c) \in R^{-1}$; thus R^{-1} is transitive.

14. **a)** These are comparable, since $5 \mid 15$.

b) These are not comparable since neither divides the other.

c) These are comparable, since $8 \mid 16$.

d) These are comparable, since $7 \mid 7$.

16. **a)** We need either a number less than 2 in the first coordinate, or a 2 in the first coordinate and a number less than 3 in the second coordinate. Therefore the answer is $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$, $(2,1)$, and $(2,2)$.

b) We need either a number greater than 3 in the first coordinate, or a 3 in the first coordinate and a number greater than 1 in the second coordinate. Therefore the answer is $(4,1)$, $(4,2)$, $(4,3)$, $(4,4)$, $(3,2)$, $(3,3)$, and $(3,4)$.

c) The Hasse diagram is a straight line with 16 points on it, since this is a total order. The pair $(4,4)$ is at the top, $(4,3)$ beneath it, $(4,2)$ beneath that, and so on, with $(1,1)$ at the bottom. To save space, we will not actually draw this picture.

18. **a)** The string *quack* comes first, since it is an initial substring of *quacking*, which comes next (since the other three strings all begin *qui*, not *qua*). Similarly, these last three strings are in the order *quick*, *quicksand*, *quicksilver*.

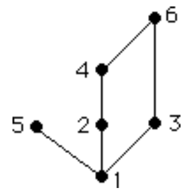
b) The order is *open*, *opened*, *opener*, *opera*, *operand*.

c) The order is *zero*, *zoo*, *zoological*, *zoology*, *zoom*.

20. The Hasse diagram for this total order is a straight line, as shown, with 0 at the top (it is the "largest" element under the "is greater than or equal to" relation) and 5 at the bottom.

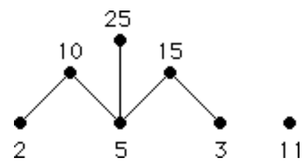
22. In each case we put a above b and draw a line between them if $b \mid a$ but there is no element c other than a and b such that $b \mid c$ and $c \mid a$.

a) Note that 1 divides all numbers, so the numbers on the second level from the bottom are the primes.

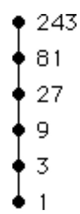


b) In this case these numbers are pairwise relatively prime, so there are no lines in the Hasse diagram.

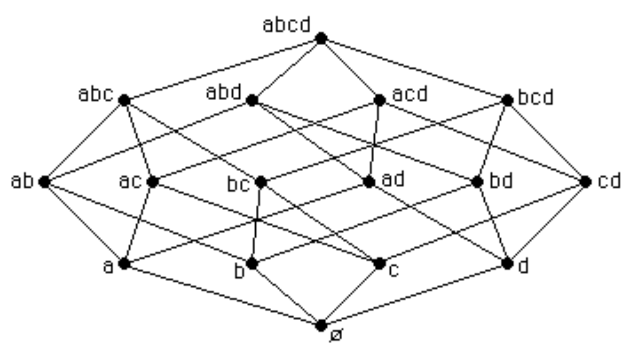
c) Note that we can place the points as we wish, as long as a is above b when $b \mid a$.



d) In this case these numbers each divide the next, so the Hasse diagram is a straight line.



24. This picture is a four-dimensional cube. We draw the sets with k elements at level k: the empty set at level 0 (the bottom), the entire set at level 4 (the top).



26. The procedure is the same as in Exercise 25: $\{(a,a),(a,b),(a,c),(a,d),(a,e),(b,b),(b,d),(b,e),(c,c),(c,d),(d,d),(e,e)\}$

28. In this problem $a \preceq b$ when $a \mid b$. For (a,b) to be in the covering relation, we need a to be a proper divisor of b but we also must have no element in our set $\{1, 2, 3, 4, 6, 12\}$ being a proper multiple of a and a proper divisor of b. For example, $(2,12)$ is not in the covering relation, since $2 \mid 6$ and $6 \mid 12$. With this understanding it is easy to list the pairs in the covering relation: $(1,2)$, $(1,3)$, $(2,4)$, $(2,6)$, $(3,6)$, $(4,12)$,and $(6,12)$.

30. This poset has 32 elements, consisting of all pairs (A, C) where A is one of 0, 1, 2, and 3 (here representing unclassified, confidential, secret, and top secret) and C is one of the eight subsets of $\{s, m, d\}$ (where these letters represent spies, moles, and double agents). The following list gives the covering relation: $(0, \emptyset) \prec (0, \{s\})$, $(0, \emptyset) \prec (0, \{m\})$, $(0, \emptyset) \prec (0, \{d\})$, $(0, \{s\}) \prec (0, \{s, m\})$, $(0, \{s\}) \prec (0, \{s, d\})$, $(0, \{m\}) \prec (0, \{s, m\})$, $(0, \{m\}) \prec (0, \{m, d\})$, $(0, \{d\}) \prec (0, \{s, d\})$, $(0, \{d\}) \prec (0, \{m, d\})$, $(0, \{s, m\}) \prec (0, \{s, m, d\})$, $(0, \{s, d\}) \prec (0, \{s, m, d\})$, $(0, \{m, d\}) \prec (0, \{s, m, d\})$, and 36 more of this form with 0 replaced successively by 1, 2, and 3, together with 8 statements of each of the forms $(0, C) \prec (1, C)$, $(1, C) \prec (2, C)$, and $(2, C) \prec (3, C)$ where $C \subseteq \{s, m, d\}$. In all, the covering relation has 72 pairs.

32. **a)** The maximal elements are the ones with no other elements above them, namely l and m.

b) The minimal elements are the ones with no other elements below them, namely a, b, and c.

c) There is no greatest element, since neither l nor m is greater than the other.

d) There is no least element, since neither a nor b is less than the other.

e) We need to find elements from which we can find downward paths to all of a, b, and c. It is clear that k, l, and m are the elements fitting this description.

f) Since k is less than both l and m, it is the least upper bound of a, b, and c.

g) No element is less than both f and h, so there are no lower bounds.

h) Since there are no lower bounds, there can be no greatest lower bound.

34. The reader should draw the Hasse diagram to aid in answering these questions.

a) Clearly the numbers 27, 48, 60, and 72 are maximal, since each divides no number in the list other than itself. All of the other numbers divide 72, however, so they are not maximal.

b) Only 2 and 9 are minimal. Every other element is divisible by either 2 or 9.

c) There is no greatest element, since, for example, there is no number in the set that both 60 and 72 divide.

d) There is no least element, since there is no number in the set that divides both 2 and 9.

e) We need to find numbers in the list that are multiples of both 2 and 9. Clearly 18, 36, and 72 are the numbers we are looking for.

f) Of the numbers we found in the previous part, 18 satisfies the definition of the least upper bound, since it divides the other two upper bounds.

g) We need to find numbers in the list that are divisors of both 60 and 72. Clearly 2, 4, 6, and 12 are the numbers we are looking for.

h) Of the numbers we found in the previous part, 12 satisfies the definition of the greatest lower bound, since the other three lower bounds divide it.

36. **a)** One example is the natural numbers under "is less than or equal to." Here 1 is the (only) minimal element, and there are no maximal elements.

b) Dual to part **(a)**, the answer is the natural numbers under "is greater than or equal to."

c) Combining the answers for the first two parts, we look at the set of integers under "is less than or equal to." Clearly there are no maximal or minimal elements.

38. Reflexivity is clear from the definition. To show antisymmetry, suppose that $a_1 \ldots a_m < b_1 \ldots b_n$, and let $t = \min(m, n)$. This means that either $a_1 \ldots a_t = b_1 \ldots b_t$ and $m < n$, so that $b_1 \ldots b_n \not< a_1 \ldots a_m$, or else $a_1 \ldots a_t < b_1 \ldots b_t$, so that $b_1 \ldots b_t \not< a_1 \ldots a_t$ and hence again $b_1 \ldots b_n \not< a_1 \ldots a_m$. Finally for transitivity, suppose that $a_1 \ldots a_m < b_1 \ldots b_n < c_1 \ldots c_p$. Let $t = \min(m, n)$, $r = \min(n, p)$, $s = \min(m, p)$, and $l = \min(m, n, p)$. Now if $a_1 \ldots a_l < b_1 \ldots b_l < c_1 \ldots c_l$, then clearly $a_1 \ldots a_m < c_1 \ldots c_p$. Otherwise, without loss of generality we may assume that $a_1 \ldots a_l = b_1 \ldots b_l$. If $l = t$, then $m < n$ and $m \leq p$. Furthermore, either $b_1 \ldots b_r < c_1 \ldots c_r$, or $b_1 \ldots b_r = c_1 \ldots c_r$ and $n < p$. In the former case, if $r > l$, then since $p > m$ we have $a_1 \ldots a_m < c_1 \ldots c_p$, whereas if $r = l$, then $a_1 \ldots a_l < c_1 \ldots c_l$. In the latter case, $a_1 \ldots a_s = c_1 \ldots c_s$ and $m < p$, so again $a_1 \ldots a_m < c_1 \ldots c_p$. If $l < t$, then we must have $b_1 \ldots b_l < c_1 \ldots c_l$, whence $a_1 \ldots a_l < c_1 \ldots c_l$.

40. **a)** If x and y are both greatest elements, then by definition, $x \preceq y$ and $y \preceq x$, whence $x = y$.
b) This is dual to part **(a)**. If x and y are both least elements, then by definition, $x \preceq y$ and $y \preceq x$, whence $x = y$.

42. **a)** If x and y are both least upper bounds, then by definition, $x \preceq y$ and $y \preceq x$, whence $x = y$.
b) This is dual to part **(a)**. If x and y are both greatest lower bounds, then by definition, $x \preceq y$ and $y \preceq x$, whence $x = y$.

44. In each case, we need to decide whether every pair of elements has a least upper bound and a greatest lower bound.
a) This is not a lattice, since the elements 6 and 9 have no upper bound (no element in our set is a multiple of both of them).
b) This is a lattice; in fact it is a linear order, since each element in the list divides the next one. The least upper bound of two numbers in the list is the larger, and the greatest lower bound is the smaller.
c) Again, this is a lattice because it is a linear order. The least upper bound of two numbers in the list is the smaller number (since here "greater" really means "less"!), and the greatest lower bound is the larger of the two numbers.
d) This is similar to Example 24, with the roles of subset and superset reversed. Here the g.l.b. of two subsets A and B is $A \cup B$, and their l.u.b. is $A \cap B$.

46. By the duality in the definitions, the greatest lower bound of two elements of S under R is their least upper bound under R^{-1}, and their least upper bound under R is their greatest lower bound under R^{-1}. Therefore, if (S, R) is a lattice (i.e., all the l.u.b.'s and g.l.b.'s exist), then so is (S, R^{-1}).

48. We need to verify the various defining properties of a lattice. First, we need to show that S is a poset under the given $\preceq$ relation. Clearly $(A, C) \preceq (A, C)$, since $A \le A$ and $C \subseteq C$; thus we have established reflexivity. For antisymmetry, suppose that $(A_1, C_1) \preceq (A_2, C_2)$ and $(A_2, C_2) \preceq (A_1, C_1)$. This means that $A_1 \le A_2$, $C_1 \subseteq C_2$, $A_2 \le A_1$, and $C_2 \subseteq C_1$. By the properties of $\le$ and $\subseteq$ it immediately follows that $A_1 = A_2$ and $C_1 = C_2$, so $(A_1, C_1) = (A_2, C_2)$. Transitivity is proved in a similar way, using the transitivity of $\le$ and $\subseteq$. Second, we need to show that greatest lower bounds and least upper bounds exist. Suppose that (A_1, C_1) and (A_2, C_2) are two elements of S; we claim that $(\min(A_1, A_2), C_1 \cap C_2)$ is their greatest lower bound. Clearly $\min(A_1, A_2) \le A_1$ and $\min(A_1, A_2) \le A_2$; and $C_1 \cap C_2 \subseteq C_1$ and $C_1 \cap C_2 \subseteq C_2$. Therefore $(\min(A_1, A_2), C_1 \cap C_2) \preceq (A_1, C_1)$ and $(\min(A_1, A_2), C_1 \cap C_2) \preceq (A_2, C_2)$, so this is a lower bound. On the other hand, if (A, C) is any lower bound, then $A \le A_1$, $A \le A_2$, $C \subseteq C_1$, and $C \subseteq C_2$. It follows from the properties of $\le$ and $\subseteq$ that $A \le \min(A_1, A_2)$ and $C \subseteq C_1 \cap C_2$. Therefore $(A, C) \preceq (\min(A_1, A_2), C_1 \cap C_2)$. This means that $(\min(A_1, A_2), C_1 \cap C_2)$ is the greatest lower bound. The proof that $(\max(A_1, A_2), C_1 \cup C_2)$ is the least upper bound is exactly dual to this argument.

50. This issue was already dealt with in our solution to Exercise 44, parts **(b)** and **(c)**. If $(S, \le)$ is a total (linear) order, then the least upper bound of two elements is the larger one, and their greatest lower bound is the smaller.

52. By Exercise 50, we can try to choose our examples from among total orders, such as subsets of $\mathbf{Z}$ under $\le$.
a) $(\mathbf{Z}, \le)$ **b)** $(\mathbf{Z}^+, \le)$ **c)** $(\mathbf{Z}^-, \le)$, where $\mathbf{Z}^-$ is the set of negative integers **d)** $(\{1\}, \le)$

54. In each case, the issue is whether every nonempty subset contains a least element.

a) The is well-ordered, since the minimum element in any nonempty subset is its smallest element.

b) This is not well-ordered. For example, the set $\{\frac{1}{n} \mid n \in \mathbf{N}\}$ contains no minimum element.

c) Note that $S = \{\frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \ldots\}$. This is well-ordered, since the minimum element in any nonempty subset is its smallest element.

d) This is well-ordered, since it has the same structure as the positive integers under $\leq$, because $x \geq y$ if and only if $-x \leq -y$. Thus the minimum element in any nonempty subset is its largest element.

56. Let x_0 and x_1 be two elements in the dense poset, with $x_0 \prec x_1$ (guaranteed by the conditions stated). By density, there is an element x_2 between x_0 and x_1, i.e., with $x_0 \prec x_2 \prec x_1$. Again by density, there is an element x_3 between x_0 and x_2, i.e., with $x_0 \prec x_3 \prec x_2$. We continue in this manner and have produced an infinite decreasing sequence: $\cdots \prec x_4 \prec x_3 \prec x_2 \prec x_1$. Thus the poset is not well-founded.

58. It is not well-founded because of the infinite decreasing sequence $\cdots \prec aaab \prec aab \prec ab \prec b$. It is not dense, because there is no element between a and aa in this order.

60. This is dual to Lemma 1. We can simply copy the proof, changing every "minimal" to "maximal" and reversing each inequality.

62. Since a larger number can never divide a smaller one, the "is less than or equal to" relation on any set is a compatible total order for the divisibility relation. This gives $1 \prec_t 2 \prec_t 3 \prec_t 6 \prec_t 8 \prec_t 12 \prec_t 24 \prec_t 36$.

64. Clearly g must go in the middle, with any of the six permutations of $\{a, b, c\}$ before g and any of the six permutations of $\{d, e, f\}$ following g. Thus there are 36 compatible total orderings for this poset, such as $a \prec b \prec c \prec g \prec d \prec e \prec f$ and $b \prec a \prec c \prec g \prec f \prec e \prec d$.

66. There are many compatible total orders here. We just need to work from the bottom up. One answer is to take Foundation $\prec$ Framing $\prec$ Roof $\prec$ Exterior siding $\prec$ Wiring $\prec$ Plumbing $\prec$ Flooring $\prec$ Wall $-$ board $\prec$ Exterior painting $\prec$ Interior painting $\prec$ Carpeting $\prec$ Interior fixtures $\prec$ Exterior fixtures $\prec$ Completion.

SUPPLEMENTARY EXERCISES FOR CHAPTER 9

2. In each case we will construct a simplest such relation.

a) $\{(a,a), (b,b), (c,c), (a,b), (b,a), (b,c), (c,b), (d,d)\}$ **b)** $\emptyset$ **c)** $\{(a,b), (b,c)\}$

d) $\{(a,a), (b,b), (c,c), (a,b), (b,a), (c,a), (c,b), (d,d)\}$ **e)** $\{(a,b), (b,a), (c,c), (c,a)\}$

4. Suppose that $R_1 \subseteq R_2$ and that R_2 is antisymmetric. We must show that R_1 is also antisymmetric. Let $(a,b) \in R_1$ and $(b,a) \in R_1$. Since these two pairs are also both in R_2, we know that $a = b$, as desired.

6. Since $(a,a) \in R_1$ and $(a,a) \in R_2$ for all $a \in A$, it follows that $(a,a) \notin R_1 \oplus R_2$ for all $a \in A$.

8. Under this hypothesis, $\overline{R}$ must also be symmetric, for if $(a,b) \in \overline{R}$, then $(a,b) \notin R$, whence (b,a) cannot be in R, either (by the symmetry of R); in other words, (b,a) is also in $\overline{R}$.

10. First suppose that R is reflexive and circular. We need to show that R is symmetric and transitive. Let $(a,b) \in R$. Since also $(b,b) \in R$, it follows by circularity that $(b,a) \in R$; this proves symmetry. Now if $(a,b) \in R$ and $(b,c) \in R$, then by circularity $(c,a) \in R$ and so by symmetry $(a,c) \in R$; thus R is transitive. Conversely, transitivity and symmetry immediately imply circularity, so every equivalence relation is reflexive and circular.

12. A primary key in the first relation need not be a primary key in the join. Let the first relation contain the pairs $(\text{John}, \text{boy})$ and $(\text{Mary}, \text{girl})$; and let the second relation contain the pairs $(\text{boy}, \text{vain})$, $(\text{girl}, \text{athletic})$, and $(\text{girl}, \text{smart})$. Clearly *Name* is a primary key for the first relation. If we take the join on the *Sex* column, then we obtain the relation containing the pairs $(\text{John}, \text{boy}, \text{vain})$, $(\text{Mary}, \text{girl}, \text{athletic})$, and $(\text{Mary}, \text{girl}, \text{smart})$; in this relation *Name* is not a primary key.

14. **a)** Two mathematicians are related under R^2 if and only if each has written a joint paper with some mathematician c.

b) Two mathematicians are related under R^* if there is a finite sequence of mathematicians $a = c_0$, c_1, c_2, $\ldots$, c_{m-1}, $c_m = b$, with $m \geq 1$, such that for each i from 1 to m, mathematician c_i has written a joint paper with mathematician c_{i-1}.

c) The Erdős number of a is the length of a shortest path in R from a to Erdős, if such a path exists. (Some mathematicians have no Erdős number.)

16. We assume that the notion of calling is a potential one—subroutine $\mathbf{P}$ is related to subroutine $\mathbf{Q}$ if it might be possible for $\mathbf{P}$ to call $\mathbf{Q}$ during its execution (in other words, there is a call to $\mathbf{Q}$ as one of the steps in the subroutine $\mathbf{P}$). Otherwise this exercise would not be well-defined, since *actual* calls are unpredictable—they depend on what actually happens as the programs execute.

a) Let $\mathbf{P}$ and $\mathbf{Q}$ be subroutines. Then $\mathbf{P}$ is related to $\mathbf{Q}$ under the transitive closure of R if and only if at some time during an active invocation of $\mathbf{P}$ it might be possible for $\mathbf{Q}$ to be called.

b) Routines such as this are usually called recursive—it might be possible for $\mathbf{P}$ to be called again while it is still active.

c) The reflexive closure of the transitive closure of any relation is just the transitive closure (see part **(a)**) with all the loops adjoined.

18. We can prove this symbolically, since the symmetric closure of a relation is the union of the relation and its inverse. Thus we have $(R \cup S) \cup (R \cup S)^{-1} = R \cup S \cup R^{-1} \cup S^{-1} = (R \cup R^{-1}) \cup (S \cup S^{-1})$.

20. **a)** This is an equivalence relation by Exercise 9 in Section 9.5, letting $f(x)$ be the sign of the zodiac under which x was born.

b) This is an equivalence relation by Exercise 9 in Section 9.5, letting $f(x)$ be the year in which x was born.

c) This is not an equivalence relation (it is not transitive).

22. This relation is reflexive, since $x - x = 0 \in \mathbf{Q}$. To see that it is symmetric, suppose that $x - y \in \mathbf{Q}$. Then $y - x = -(x - y)$ is again a rational number. For transitivity, if $x - y \in \mathbf{Q}$ and $y - z \in \mathbf{Q}$, then their sum, namely $x - z$, is also rational (the rational numbers are closed under addition). The equivalence class of 1 and of $1/2$ are both just the set of rational numbers. The equivalence class of π is the set of real numbers that differ from π by a rational number; in other words it is $\{\, \pi + r \mid r \in \mathbf{Q} \,\}$.

24. Let S be the transitive closure of the symmetric closure of the reflexive closure of R. Then by Exercise 23 in Section 9.4, S is symmetric. Since it is also clearly transitive and reflexive, S is an equivalence relation. Furthermore, every element added to R to produce S was forced to be added in order to insure reflexivity, symmetry, or transitivity; therefore S is the smallest equivalence relation containing R.

26. This follows from the fact (Exercise 54 in Section 9.5) that two partitions are related under the refinement relation if and only if their corresponding equivalence relations are related under the $\subseteq$ relation, together with the fact that $\subseteq$ is a partial order on every collection of sets.

28. A subset of a chain is again a chain, so we list only the maximal chains.
a) $\{a, b, c\}$ and $\{a, b, d\}$ **b)** $\{a, b, e\}$, $\{a, b, d\}$, and $\{a, c, d\}$
c) In this case there are 9 maximal chains, each consisting of one element from the top row, the element in the middle, and one element in the bottom row.

30. The vertices are arranged in three columns. Each pair of vertices in the same column are clearly comparable. Therefore the largest antichain can have at most three elements. One such antichain is $\{a, b, c\}$.

32. This result is known as Dilworth's theorem. For a proof, see, for instance, page 58 of *Graph Theory* by Béla Bollobás (Springer-Verlag, 1979).

34. Let x be a minimal element in S. Then the hypothesis $\forall y(y \prec x \to P(y))$ is vacuously true, so the conclusion $P(x)$ is true, which is what we wanted to show.

36. Reflexivity is the statement that f is $O(f)$. This is trivial, by taking $C = 1$ and $k = 1$ in the definition of the big-O relation. Transitivity was proved in Exercise 17 of Section 3.2.

38. It was proved in Exercise 37 that $R \cap R^{-1}$ is an equivalence relation whenever R is a quasi-ordering on a set A. Therefore it makes sense to speak of the equivalence classes of $R \cap R^{-1}$, and the relation S is well-defined from its syntax. To show that S is a partial order, we must show that it is reflexive, anti-symmetric, and transitive. For the first of these, we need to show that (C, C) belongs to S, which means that there are elements $c \in C$ and $d \in C$ such that (c, d) belongs to R. By the definition of equivalence class, C is not empty, so let c be any element of C, and let $d = c$. Then (c, c) belongs to R by the reflexivity of R. Next, for antisymmetry, suppose that (C, D) and (D, C) both belong to S; we must show that $C = D$. We have that (c, d) belongs to R for some $c \in C$ and $d \in D$; and we have that (d', c') belongs to R for some $d' \in D$ and $c' \in C$. If we show that (c, d) also belongs to R^{-1}, then we will know that c and d are in the same equivalence class of $R \cap R'$, and therefore that $C = D$. To do this, we need to show that (d, c) belongs to R. Since d and d' are in the same equivalence class, we know that (d, d') belongs to R; we already mentioned that (d', c') belongs to R; and since c' and c are in the same equivalence class, we know that (c', c) belongs to R. Applying the transitivity of R three times, we conclude that (d, c) belongs to R, as desired.

Finally, to show the transitivity of S, we must show that if (C, D) belongs to S and (D, E) belongs to S, then (C, E) belongs to S. The hypothesis tells us that (c, d) belongs to R for some $c \in C$ and $d \in D$, and that (d', e) belongs to R for some $d' \in D$ and $e \in E$. As in the previous paragraph, we know that (d, d') belongs to R. Therefore by the transitivity of R (thrice), (c, e) belongs to R, and our proof is complete.

40. This follows in essentially one step from part **(c)** of Exercise 39. Suppose that $x \vee y = y$. Then by the first absorption law, $x = x \wedge (x \vee y) = x \wedge y$. Conversely, if $x \wedge y = x$, then by the second absorption law (with the roles of x and y reversed), $y = y \vee (x \wedge y) = y \vee x$. (We are using the commutative law as well, of course.)

42. By Exercise 51 in Section 9.6, every finite lattice has a least element and a greatest element. These elements are the 0 and 1, respectively, discussed in the preamble to this exercise.

44. We learned in Example 24 of Section 9.6 that the meet and join in this lattice are $\cap$ and $\cup$. We know from Section 2.2 (see Table 1) that these operations are distributive over each other. There is nothing more to prove.

46. Here is one example. The reader should draw the Hasse diagram to see it more vividly. The elements in the lattice are 0, 1, a, b, c, d, and e. The relations are that 0 precedes all other elements; all other elements precede 1; b, d, and e precede c; and b precedes a. Then both d and e are complements of a, but b has no complement (since $b \vee x \neq 1$ unless $x = 1$).

48. This can be proved by playing around with the symbolism. Suppose that a and b are both complements of x. This means that $x \vee a = 1$, $x \wedge a = 0$, $x \vee b = 1$, and $x \wedge b = 0$. Now using the various identities in Exercises 39 and 41 and the preamble to Exercise 43, we have $a = a \wedge 1 = a \wedge (x \vee b) = (a \wedge x) \vee (a \wedge b) = 0 \vee (a \wedge b) = a \wedge b$. By the same argument, we can also show that $b = a \wedge b$. By transitivity of equality, it follows that $a = b$.

50. Actually all finite games have a winning strategy for one player or the other; one can see this by writing down the game tree and analyzing it from the bottom up, as shown in Section 11.2. What we can show in this case is that the player who goes first has a winning strategy. We give a proof by contradiction.

By the remark above, if the first player does not have a winning strategy, then the second player does. In particular, the second player has a winning response and strategy if the first player chooses b as her first move. Suppose that c is the first move of that winning strategy of the second player. But because $c \preceq b$, if the first player makes the move c at her first turn, then play can proceed exactly as if the first player had chosen b and then the second player had chosen c (because element b would be removed anyway when c is chosen). Thus the first player can win by adopting the strategy that the second player would have adopted. This is a contradiction, because it is impossible for both players to have a winning strategy. Therefore we can conclude that our assumption that the first player does not have a winning strategy is wrong, and therefore the first player does have a winning strategy.

CHAPTER 10
Graphs

SECTION 10.1 Graphs and Graph Models

2. **a)** A simple graph would be the model here, since there are no parallel edges or loops, and the edges are undirected.

b) A multigraph would, in theory, be needed here, since there may be more than one interstate highway between the same pair of cities.

c) A pseudograph is needed here, to allow for loops.

4. This is a multigraph; the edges are undirected, and there are no loops, but there are parallel edges.

6. This is a multigraph; the edges are undirected, and there are no loops, but there are parallel edges.

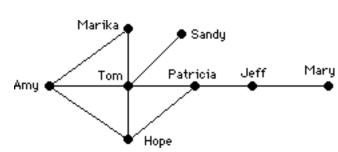
8. This is a directed multigraph; the edges are directed, and there are parallel edges.

10. The graph in Exercise 3 is simple. The multigraph in Exercise 4 can be made simple by removing one of the edges between a and b, and two of the edges between b and d. The pseudograph in Exercise 5 can be made simple by removing the three loops and one edge in each of the three pairs of parallel edges. The multigraph in Exercise 6 can be made simple by removing one of the edges between a and c, and one of the edges between b and d. The other three are not undirected graphs. (Of course removing any supersets of the answers given here are equally valid answers; in particular, we could remove *all* the edges in each case.)

12. If $u\,R\,v$, then there is an edge joining vertices u and v, and since the graph is undirected, this is also an edge joining vertices v and u. This means that $v\,R\,u$. Thus the relation is symmetric. The relation is reflexive because the loops guarantee that $u\,R\,u$ for each vertex u.

14. Since there are edges from Hawk to Crow, Owl, and Raccoon, the graph is telling us that the hawk competes with these three animals.

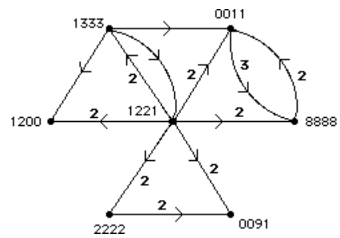
16. Each person is represented by a vertex, with an edge between two vertices if and only if the people are acquainted.



18. Fred influences Brian, since there is an edge from Fred to Brian. Yvonne and Deborah influence Fred, since there are edges from these vertices to Fred.

20. Team four beat the vertices to which there are edges from Team four, namely only Team three. The other teams—Team one, Team two, Team five, and Team six—all beat Team four, since there are edges from them to Team four.

22. This is a directed multigraph with one edge from a to b for each call made by a to b. Rather than draw the parallel edges with parallel lines, we have indicated what is intended by writing a numeral on the edge to indicate how many calls were made, if it was more than one.



24. This is similar to the use of directed graphs to model telephone calls.

a) We can have a vertex for each mailbox or e-mail address in the network, with a directed edge between two vertices if a message is sent from the tail of the edge to the head.

b) As in part **(a)** we use a directed edge for each message sent during the week.

26. Vertices with thousands or millions of edges going out from them could be the senders of such mass mailings. The collection of heads of these edges would be the mailing lists themselves.

28. We make the subway stations the vertices, with an edge from station u to station v if there is a train going from u to v without stopping. It is quite possible that some segments are one-way, so we should use directed edges. (If there are no one-way segments, then we could use undirected edges.) There would be no need for multiple edges, unless we had two kinds of edges, maybe with different colors, to represent local and express trains. In that case, there could be parallel edges of different colors between the same vertices, because both a local and an express train might travel the same segment. There would be no point in having loops, because no passenger would want to travel from a station back to the same station without stopping.

30. A bipartite graph (this terminology is introduced in the next section) works well here. There are two types of vertices—one type representing the critics and one type representing the movies. There is an edge between vertex c (a critic vertex) and vertex m (a movie vertex) if and only if the critic represented by c has positively recommended the movie represented by m. There are no edges between critic vertices and there are no edges between movie vertices.

32. The model says that the statements for which there are edges to S_6 must be executed before S_6, namely the statements S_1, S_2, S_3, and S_4.

34. The vertices in the directed graph represent cities. Whenever there is a nonstop flight from city A to city B, we put a directed edge into our directed graph from vertex A to vertex B, and furthermore we label that edge with the flight time. Let us see how to incorporate this into the mathematical definition. Let us call such a thing a directed graph with weighted edges. It is defined to be a triple (V, E, W), where (V, E) is a directed graph (i.e., V is a set of vertices and E is a set of ordered pairs of elements of V) and W is a function from E to the set of nonnegative real numbers. Here we are simply thinking of $W(e)$ as the weight of edge e, which in this case is the flight time.

36. We can let the vertices represent people; an edge from u to v would indicate that u can send a message to v. We would need a directed multigraph in which the edges have labels, where the label on each edge indicates the form of communication (cell phone audio, text messaging, and so on).

SECTION 10.2 Graph Terminology and Special Types of Graphs

2. In this pseudograph there are 5 vertices and 13 edges. The degree of vertex a is 6, since in addition to the 4 nonloops incident to a, there is a loop contributing 2 to the degree. The degrees of the other vertices are $\deg(b) = 6$, $\deg(c) = 6$, $\deg(d) = 5$, and $\deg(e) = 3$. There are no pendant or isolated vertices in this pseudograph.

4. For the graph in Exercise 1, the sum is $2+4+1+0+2+3 = 12 = 2\cdot 6$; there are 6 edges. For the pseudograph in Exercise 2, the sum is $6+6+6+5+3 = 26 = 2\cdot 13$; there are 13 edges. For the pseudograph in Exercise 3, the sum is $3+2+4+0+6+0+4+2+3 = 24 = 2\cdot 12$; there are 12 edges.

6. Model this problem by letting the vertices of a graph be the people at the party, with an edge between two people if they shake hands. Then the degree of each vertex is the number of people the person that vertex represents shakes hands with. By Theorem 1 the sum of the degrees is even (it is $2e$).

8. In this directed multigraph there are 4 vertices and 8 edges. The degrees are $\deg^-(a) = 2$, $\deg^+(a) = 2$, $\deg^-(b) = 3$, $\deg^+(b) = 4$, $\deg^-(c) = 2$, $\deg^+(c) = 1$, $\deg^-(d) = 1$, and $\deg^+(d) = 1$.

10. For Exercise 7 the sum of the in-degrees is $3+1+2+1 = 7$, and the sum of the out-degrees is $1+2+1+3 = 7$; there are 7 edges. For Exercise 8 the sum of the in-degrees is $2+3+2+1 = 8$, and the sum of the out-degrees is $2+4+1+1 = 8$; there are 8 edges. For Exercise 9 the sum of the in-degrees is $6+1+2+4+0 = 13$, and the sum of the out-degrees is $1+5+5+2+0 = 13$; there are 13 edges.

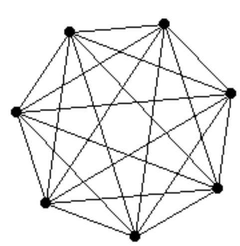
12. Since there is an edge from a person to each of his or her acquaintances, the degree of v is the number of people v knows. An isolated vertex would be a person who knows no one, and a pendant vertex would be a person who knows just one other person (it is doubtful that there are many, if any, isolated or pendant vertices). If the average degree is 1000, then the average person knows 1000 other people.

14. Since there is an edge from a person to each of the other actors with whom that person has appeared in a movie, the degree of v is the number of other actors with whom that person has appeared. The neighborhood of v is the *set* of actors with whom v as appeared. An isolated vertex would be a person who has appeared only in movies in which he or she was the only actor, and a pendant vertex would be a person who has appeared with only one other actor in any movie (it is doubtful that there are many, if any, isolated or pendant vertices).

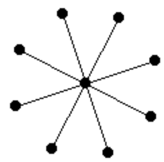
16. Since there is an edge from a page to each page that it links to, the outdegree of a vertex is the number of links on that page, and the in-degree of a vertex is the number of other pages that have a link to it.

18. This is essentially the same as Exercise 40 in Section 6.2, where the graph models the “know each other” relation on the people at the party. See the solution given for that exercise. The number of people a person knows is the degree of the corresponding vertex in the graph.

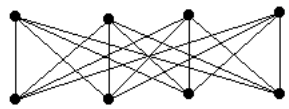
20. **a)** This graph has 7 vertices, with an edge joining each pair of distinct vertices.



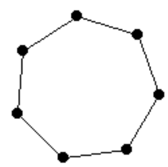
b) This graph is the complete bipartite graph on parts of size 1 and 8; we have put the part of size 1 in the middle.



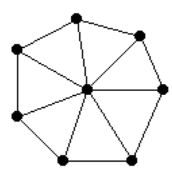
c) This is the complete bipartite graph with 4 vertices in each part.



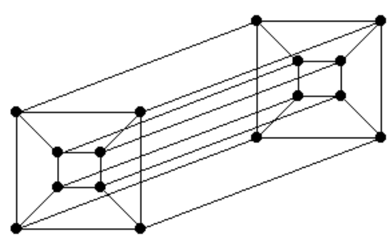
d) This is the 7-cycle.



e) The 7-wheel is the 7-cycle with an extra vertex joined to the other 7 vertices. Warning: Some texts call this W_8, to have the consistent notation that the subscript in the name of a graph should be the number of vertices in that graph.



f) We take two copies of Q_3 and join corresponding vertices.



22. This graph is bipartite, with bipartition $\{a, c\}$ and $\{b, d, e\}$. In fact this is the complete bipartite graph $K_{2,3}$. If this graph were missing the edge between a and d, then it would still be bipartite on the same sets, but not a complete bipartite graph.

24. This is the complete bipartite graph $K_{2,4}$. The vertices in the part of size 2 are c and f, and the vertices in the part of size 4 are a, b, d, and e.

26. a) By the definition given in the text, K_1 does not have enough vertices to be bipartite (the sets in a partition have to be nonempty). Clearly K_2 is bipartite. There is a triangle in K_n for $n > 2$, so those complete graphs are not bipartite. (See Exercise 23.)

b) First we need $n \geq 3$ for C_n to be defined. If n is even, then C_n is bipartite, since we can take one part to be every other vertex. If n is odd, then C_n is not bipartite.

c) Every wheel contains triangles, so no W_n is bipartite.

d) Q_n is bipartite for all $n \geq 1$, since we can divide the vertices into these two classes: those bit strings with an odd number of 1's, and those bit strings with an even number of 1's.

28. **a)** Following the lead in Example 14, we construct a bipartite graph in which the vertex set consists of two subsets—one for the employees and one for the jobs. Let $V_1 = \{\text{Zamora}, \text{Agraharam}, \text{Smith}, \text{Chou}, \text{Macintyre}\}$, and let $V_2 = \{\text{planning}, \text{publicity}, \text{sales}, \text{marketing}, \text{development}, \text{industry relations}\}$. Then the vertex set for our graph is $V = V_1 \cup V_2$. Given the list of capabilities in the exercise, we must include precisely the following edges in our graph: $\{\text{Zamora}, \text{planning}\}$, $\{\text{Zamora}, \text{sales}\}$, $\{\text{Zamora}, \text{marketing}\}$, $\{\text{Zamora}, \text{industry relations}\}$, $\{\text{Agraharam}, \text{planning}\}$, $\{\text{Agraharam}, \text{development}\}$, $\{\text{Smith}, \text{publicity}\}$, $\{\text{Smith}, \text{sales}\}$, $\{\text{Smith}, \text{industry relations}\}$, $\{\text{Chou}, \text{planning}\}$, $\{\text{Chou}, \text{sales}\}$, $\{\text{Chou}, \text{industry relations}\}$, $\{\text{Macintyre}, \text{planning}\}$, $\{\text{Macintyre}, \text{publicity}\}$, $\{\text{Macintyre}, \text{sales}\}$, $\{\text{Macintyre}, \text{industry relations}\}$.

b) Many assignments are possible. If we take it as an implicit assumption that there will be no more than one employee assigned to the same job, then we want a maximum matching for this graph. So we look for five edges in this graph that share no endpoints. A little trial and error gives us, for example, $\{\text{Zamora}, \text{planning}\}$, $\{\text{Agraharam}, \text{development}\}$, $\{\text{Smith}, \text{publicity}\}$, $\{\text{Chou}, \text{sales}\}$, $\{\text{Macintyre}, \text{industry relations}\}$. We assign the employees to the jobs given in this matching.

c) This is a complete matching from the set of employees to the set of jobs, but not the other way around. It is a maximum matching; because there were only five employees, no matching could have more than five edges.

30. **a)** The partite sets are the set of women ($\{\text{Anna}, \text{Barbara}, \text{Carol}, \text{Diane}, \text{Elizabeth}\}$) and the set of men ($\{\text{Jason}, \text{Kevin}, \text{Larry}, \text{Matt}, \text{Nick}, \text{Oscar}\}$). We will use first letters for convenience. The given information tells us to have edges AJ, AL, AM, BK, BL, CJ, CN, CO, DJ, DL, DN, DO, EJ, and EM in our graph. We do not put an edge between a woman and a man she is not willing to marry.

b) By trial and error we easily find a matching (it's not unique), such as AL, BK, CJ, DN, and EM.

c) This is a complete matching from the women to the men (as well as from the men to the women). A complete matching is always a maximum matching.

32. Let $d = \max_{A \subseteq V_1} \operatorname{def}(A)$, and fix A to be a subset of V_1 that achieves this maximum. Thus $d = |A| - |N(A)|$. First we show that no matching in G can touch more than $|V_1| - d$ vertices of V_1 (or, equivalently, that no matching in G can have more than $|V_1| - d$ edges). At most $|N(A)|$ edges of such a matching can have endpoints in A, and at most $|V_1| - |A|$ can have endpoints in $V_1 - A$, so the total number of such edges is at most $|N(A)| + |V_1| - |A| = |V_1| - d$. It remains to show that we can find a matching in G touching (at least) $|V_1| - d$ vertices of V_1 (i.e., a matching in G with $|V_1| - d$ edges). Following the hint, construct a larger graph G' by adding d new vertices to V_2 and joining all of them to all the vertices of V_1. Then the condition in Hall's theorem holds in G', so G' has a matching that touches all the vertices of V_1. At most d of these edges do not lie in G, and so the edges of this matching that do lie in G form a matching in G with at least $|V_1| - d$ edges.

34. Since all the vertices in the subgraph are adjacent in K_n, they are adjacent in the subgraph, i.e., the subgraph is complete.

36. We just have to count the number of edges at each vertex, and then arrange these counts in nonincreasing order. For Exercise 21, we have $4, 1, 1, 1, 1$. For Exercise 22, we have $3, 3, 2, 2, 2$. For Exercise 23, we have $4, 3, 3, 2, 2, 2$. For Exercise 24, we have $4, 4, 2, 2, 2, 2$. For Exercise 25, we have $3, 3, 3, 3, 2, 2$.

38. Assume that $m \geq n$. Then each of the n vertices in one part has degree m, and each of the m vertices in other part has degree n. Thus the degree sequence is $m, m, \ldots, m, n, n, \ldots, n$, where the sequence contains n copies of m and m copies of n. We put the m's first because we assumed that $m \geq n$. If $n \geq m$, then of course we would put the m copies of n first. If $m = n$, this would mean a total of $2n$ copies of n.

40. The 4-wheel (see Figure 5) with one edge along the rim deleted is such a graph. It has $(4+3+3+2+2)/2 = 7$ edges.

42. **a)** Since the number of odd-degree vertices has to be even, no graph exists with these degrees. Another reason no such graph exists is that the vertex of degree 0 would have to be isolated but the vertex of degree 5 would have to be adjacent to every other vertex, and these two statements are contradictory.

b) Since the number of odd-degree vertices has to be even, no graph exists with these degrees. Another reason no such graph exists is that the degree of a vertex in a simple graph is at most 1 less than the number of vertices.

c) A 6-cycle is such a graph. (See picture below.)

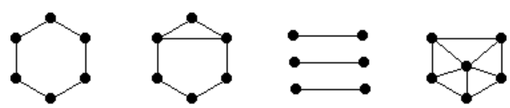
d) Since the number of odd-degree vertices has to be even, no graph exists with these degrees.

e) A 6-cycle with one of its diagonals added is such a graph. (See picture below.)

f) A graph consisting of three edges with no common vertices is such a graph. (See picture below.)

g) The 5-wheel is such a graph. (See picture below.)

h) Each of the vertices of degree 5 is adjacent to all the other vertices. Thus there can be no vertex of degree 1. So no such graph exists.



(c) (e) (f) (g)

44. Since isolated vertices play no essential role, we can assume that $d_n > 0$. The sequence is graphic, so there is some simple graph G such that the degrees of the vertices are d_1, d_2, $\ldots$, d_n. Without loss of generality, we can label the vertices of our graph so that $d(v_i) = d_i$. Among all such graphs, choose G to be one in which v_1 is adjacent to as many of v_2, v_3, $\ldots$, v_{d_1+1} as possible. (The worst case might be that v_1 is not adjacent to any of these vertices.) If v_1 is adjacent to all of them, then we are done. We will show that if there is a vertex among v_2, v_3, $\ldots$, v_{d_1+1} that v_1 is not adjacent to, then we can find another graph with $d(v_i) = d_i$ and having v_1 adjacent to one more of the vertices v_2, v_3, $\ldots$, v_{d_1+1} than is true for G. This is a contradiction to the choice of G, and hence we will have shown that G satisfies the desired condition.

Under this assumption, then, let u be a vertex among v_2, v_3, $\ldots$, v_{d_1+1} that v_1 is not adjacent to, and let w be a vertex not among v_2, v_3, $\ldots$, v_{d_1+1} that v_1 is adjacent to; such a vertex w has to exist because $d(v_1) = d_1$. Because the degree sequence is listed in nonincreasing order, we have $d(u) \geq d(w)$. Consider all the vertices that are adjacent to u. It cannot be the case that w is adjacent to each of them, because then w would have a higher degree than u (because w is adjacent to v_1 as well, but u is not). Therefore there is some vertex x such that edge ux is present but edge xw is not present. Note also that edge v_1w is present but edge v_1u is not present. Now construct the graph G' to be the same as G except that edges ux and v_1w are removed and edges xw and v_1u are added. The degrees of all vertices are unchanged, but this graph has v_1 adjacent to more of the vertices among v_2, v_3, $\ldots$, v_{d_1+1} than is the case in G. That gives the desired contradiction, and our proof is complete.

46. Given a sequence d_1, d_2, $\ldots$, d_n, if $n = 2$, then the sequence is graphic if and only if $d_1 = d_2 = 1$ (the graph consists of one edge)—this is one base case. Otherwise, if $n < d_1 + 1$, then the sequence is not graphic—this is the other base case. Otherwise (this is the recursive step), form a new sequence by deleting d_1, subtracting 1 from each of d_2, d_3, $\ldots$, d_{d_1+1}, deleting all 0's, and rearranging the terms into nonincreasing order. The original sequence is graphic if and only if the resulting sequence (with $n-1$ terms) is graphic.

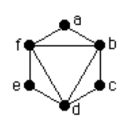
48. We list the subgraphs: the subgraph consisting of K_2 itself, the subgraph consisting of two vertices and no edges, and two subgraphs with 1 vertex each. Therefore the answer is 4.

50. We need to count this in an organized manner. First note that W_3 is the same as K_4, and it will be easier if we think of it as K_4. We will count the subgraphs in terms of the number of vertices they contain. There are clearly just 4 subgraphs consisting of just one vertex. If a subgraph is to have two vertices, then there are $C(4,2)=6$ ways to choose the vertices, and then 2 ways in each case to decide whether or not to include the edge joining them. This gives us $6\cdot 2=12$ subgraphs with two vertices. If a subgraph is to have three vertices, then there are $C(4,3)=4$ ways to choose the vertices, and then $2^3=8$ ways in each case to decide whether or not to include each of the edges joining pairs of them. This gives us $4\cdot 8=32$ subgraphs with three vertices. Finally, there are the subgraphs containing all four vertices. Here there are $2^6=64$ ways to decide which edges to include. Thus our answer is $4+12+32+64=112$.

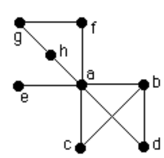
52. **a)** We want to show that $2e\geq vm$. We know from Theorem 1 that $2e$ is the sum of the degrees of the vertices. This certainly cannot be less than the sum of m for each vertex, since each degree is no less than m.
b) We want to show that $2e\leq vM$. We know from Theorem 1 that $2e$ is the sum of the degrees of the vertices. This certainly cannot exceed the sum of M for each vertex, since each degree is no greater than M.

54. Since the vertices in one part have degree m, and vertices in the other part have degree n, we conclude that $K_{m,n}$ is regular if and only if $m=n$.

56. We draw the answer by superimposing the graphs (keeping the positions of the vertices the same).



58. The union is shown here. The only common vertex is a, so we have reoriented the drawing so that the pieces will not overlap.



60. The given information tells us that $G\cup\overline{G}$ has 28 edges. However, $G\cup\overline{G}$ is the complete graph on the number of vertices n that G has. Since this graph has $n(n-1)/2$ edges, we want to solve $n(n-1)/2=28$. Thus $n=8$.

62. Following the ideas given in the solution to Exercise 63, we see that the degree sequence is obtained by subtracting each of these numbers from 4 (the number of vertices) and reversing the order. We obtain $2,2,1,1,0$.

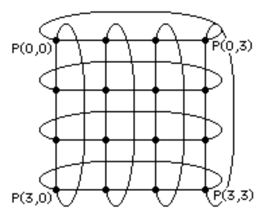
64. Suppose the parts are of sizes k and $v-k$. Then the maximum number of edges the graph may have is $k(v-k)$ (an edge between each pair of vertices in different parts). By algebra or calculus, we know that the function $f(k)=k(v-k)$ achieves its maximum when $k=v/2$, giving $f(k)=v^2/4$. Thus there are at most $v^2/4$ edges.

66. We start by coloring any vertex red. Then we color all the vertices adjacent to this vertex blue. Then we color all the vertices adjacent to blue vertices red, then color all the vertices adjacent to red vertices blue, and so on. If we ever are in the position of trying to color a vertex with the color opposite to the color it already has, then we stop and know that the graph is not bipartite. If the process terminates (successfully) before all the vertices have been colored, then we color some uncolored vertex red (it will necessarily not be adjacent to any vertices we have already colored) and begin the process again. Eventually we will have either colored all the vertices (producing the bipartition) or stopped and decided that the graph is not bipartite.

68. Obviously $(G^c)^c$ and G have the same vertex set, so we need only show that they have the same directed edges. But this is clear, since an edge (u,v) is in $(G^c)^c$ if and only if the edge (v,u) is in G^c if and only if the edge (u,v) is in G.

70. Let $|V_1| = n_1$ and $|V_2| = n_2$. Then the number of endpoints of edges in V_1 is $n \cdot n_1$, and the number of endpoints of edges in V_2 is $n \cdot n_2$. Since every edge must have one endpoint in each part, these two expressions must be equal, and it follows (because $n \neq 0$) that $n_1 = n_2$, as desired.

72. In addition to the connections shown in Figure 13, we need to make connections between $P(i,3)$ and $P(i,0)$ for each i, and between $P(3,j)$ and $P(0,j)$ for each j. The complete network is shown here. We can imagine this drawn on a torus.



SECTION 10.3 Representing Graphs and Graph Isomorphism

2. This is similar to Exercise 1. The list is as follows.

Vertex	Adjacent vertices
a	b, d
b	a, d, e
c	d, e
d	a, b, c
e	b, c

4. This is similar to Exercise 3. The list is as follows.

Initial vertex	Terminal vertices
a	b, d
b	a, c, d, e
c	b, c
d	a, e
e	c, e

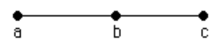
6. This is similar to Exercise 5. The vertices are assumed to be listed in alphabetical order.

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

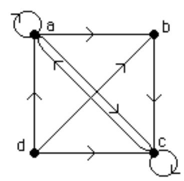
8. This is similar to Exercise 7.

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

10. This graph has three vertices and is undirected, since the matrix is symmetric.



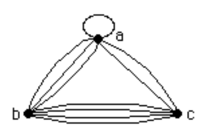
12. This graph is directed, since the matrix is not symmetric.



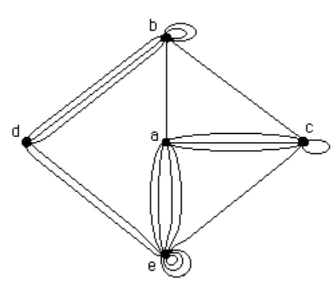
14. This is similar to Exercise 13.

$$\begin{bmatrix} 0 & 3 & 0 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 \\ 1 & 0 & 3 & 0 \end{bmatrix}$$

16. Because of the numbers larger than 1, we need multiple edges in this graph.



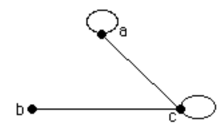
18. This is similar to Exercise 16.



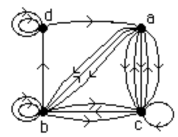
20. This is similar to Exercise 19.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

22. a) This matrix is symmetric, so we can take the graph to be undirected. No parallel edges are present, since no entries exceed 1.



24. This is the adjacency matrix of a directed multigraph, because the matrix is not symmetric and it contains entries greater than 1.



26. Each column represents an edge; the two 1's in the column are in the rows for the endpoints of the edge.

Exercise 1 $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ Exercise 2 $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$

28. For an undirected graph, the sum of the entries in the i^{th} row is the same as the corresponding column sum, namely the number of edges incident to the vertex i, which is the same as the degree of i minus the number of loops at i (since each loop contributes 2 toward the degree count).

For a directed graph, the answer is dual to the answer for Exercise 29. The sum of the entries in the i^{th} row is the number of edges that have i as their initial vertex, i.e., the out-degree of i.

30. The sum of the entries in the i^{th} row of the incidence matrix is the number of edges incident to vertex i, since there is one column with a 1 in row i for each such edge.

32. a) This is just the matrix that has 0's on the main diagonal and 1's elsewhere, namely

$$\begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 0 \end{bmatrix}.$$

b) We label the vertices so that the cycle goes $v_1, v_2, \ldots, v_n, v_1$. Then the matrix has 1's on the diagonals just above and below the main diagonal and in positions $(1, n)$ and $(n, 1)$, and 0's elsewhere:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

c) This matrix is the same as the answer in part **(b)**, except that we add one row and column for the vertex in the middle of the wheel; in our matrix it is the last row and column:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & 1 & \dots & 0 & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & 0 & \dots & 1 & 0 & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 & 0 \end{bmatrix}$$

d) Since the first m vertices are adjacent to none of the first m vertices but all of the last n, and vice versa, this matrix splits up into four pieces:

$$\begin{bmatrix} 0 & \dots & 0 & 1 & \dots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & \dots & 1 \\ 1 & \dots & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \dots & 1 & 0 & \dots & 0 \end{bmatrix}$$

e) It is not convenient to show these matrices explicitly. Instead, we will give a recursive definition. Let $\mathbf{Q}_n$ be the adjacency matrix for the graph Q_n. Then

$$\mathbf{Q}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and

$$\mathbf{Q}_{n+1} = \begin{bmatrix} \mathbf{Q}_n & \mathbf{I}_n \\ \mathbf{I}_n & \mathbf{Q}_n \end{bmatrix},$$

where $\mathbf{I}_n$ is the identity matrix (since the corresponding vertices of the two n-cubes are joined by edges in the $(n+1)$-cube).

34. These graphs are isomorphic, since each is a path with five vertices. One isomorphism is $f(u_1) = v_1$, $f(u_2) = v_2$, $f(u_3) = v_4$, $f(u_4) = v_5$, and $f(u_5) = v_3$.

36. These graphs are not isomorphic. The second has a vertex of degree 4, whereas the first does not.

38. These two graphs are isomorphic. Each consists of a K_4 with a fifth vertex adjacent to two of the vertices in the K_4. Many isomorphisms are possible. One is $f(u_1) = v_1$, $f(u_2) = v_3$, $f(u_3) = v_2$, $f(u_4) = v_5$, and $f(u_5) = v_4$.

40. These graphs are not isomorphic—the degrees of the vertices are not the same (the graph on the right has a vertex of degree 4, which the graph on the left lacks).

42. These graphs are not isomorphic. In the first graph the vertices of degree 4 are adjacent. This is not true of the second graph.

44. The easiest way to show that these graphs are not isomorphic is to look at their complements. The complement of the graph on the left consists of two 4-cycles. The complement of the graph on the right is an 8-cycle. Since the complements are not isomorphic, the graphs are also not isomorphic.

46. This is immediate from the definition, since an edge is in $\overline{G}$ if and only if it is not in G, if and only if the corresponding edge is not in H, if and only if the corresponding edge is in $\overline{H}$.

48. An isolated vertex has no incident edges, so the row consists of all 0's.

50. The complementary graph consists of edges $\{a, c\}$, $\{c, d\}$, and $\{d, b\}$; it is clearly isomorphic to the original graph (send d to a, a to c, b to d, and c to b).

52. If G is self-complementary, then the number of edges of G must equal the number of edges of $\overline{G}$. But the sum of these two numbers is $n(n-1)/2$, where n is the number of vertices of G, since the union of the two graphs is K_n. Therefore the number of edges of G must be $n(n-1)/4$. Since this number must be an integer, a look at the four cases shows that n may be congruent to either 0 or 1, but not congruent to either 2 or 3, modulo 4.

54. An excellent resource for questions of the form "how many nonisomorphic graphs are there with ...?" is Ronald C. Read and Robin J. Wilson, *An Atlas of Graphs* (Clarendon Press, 1998).

a) There are just two graphs with 2 vertices—the one with no edges, and the one with one edge.

b) A graph with three vertices can contain 0, 1, 2, or 3 edges. There is only one graph for each number of edges, up to isomorphism. Therefore the answer is 4.

c) Here we look at graphs with 4 vertices. There is 1 graph with no edges, and 1 (up to isomorphism) with a single edge. If there are two edges, then these edges may or may not be adjacent, giving us 2 possibilities. If there are three edges, then the edges may form a triangle, a star, or a path, giving us 3 possibilities. Since graphs with four, five, or six edges are just complements of graphs with two, one, or no edges (respectively), the number of isomorphism classes must be the same as for these earlier cases. Thus our answer is $1+1+2+3+2+1+1=11$.

56. There are 9 such graphs. Let us first look at the graphs that have a cycle in them. There is only 1 with a 4-cycle. There are 2 with a triangle, since the fourth edge can either be incident to the triangle or not. If there are no cycles, then the edges may all be in one connected component (see Section 10.4), in which case there are 3 possibilities (a path of length four, a path of length three with an edge incident to one of the middle vertices on the path, and a star). Otherwise, there are two components, which are necessarily either two paths of length two, a path of length three plus a single edge, or a star with three edges plus a single edge (3 possibilities in this case as well).

58. a) These graphs are both K_3, so they are isomorphic.

b) These are both simple graphs with 4 vertices and 5 edges. Up to isomorphism there is only one such graph (its complement is a single edge), so the graphs have to be isomorphic.

60. We need only modify the definition of isomorphism of simple graphs slightly. The directed graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a one-to-one and onto function $f: V_1 \to V_2$ such that for all pairs of vertices a and b in V_1, $(a, b) \in E_1$ if and only if $(f(a), f(b)) \in E_2$.

62. These two graphs are not isomorphic. In the first there is no edge from the unique vertex of in-degree 0 (u_1) to the unique vertex of out-degree 0 (u_2), whereas in the second graph there is such an edge, namely v_3v_4.

64. We claim that the digraphs are isomorphic. To discover an isomorphism, we first note that vertices u_1, u_2, and u_3 in the first digraph are independent (i.e., have no edges joining them), as are u_4, u_5, and u_6. Therefore these two groups of vertices will have to correspond to similar groups in the second digraph, namely v_1, v_3, and v_5, and v_2, v_4, and v_6, in some order. Furthermore, u_3 is the only vertex among one of these groups of u's to be the only one in the group with out-degree 2, so it must correspond to v_6, the vertex with the similar property in the other digraph; and in the same manner, u_4 must correspond to v_5. Now it is an easy matter, by looking at where the edges lead, to see that the isomorphism (if there is one) must also pair up u_1 with v_2; u_2 with v_4; u_5 with v_1; and u_6 with v_3. Finally, we easily verify that this indeed gives an isomorphism—each directed edge in the first digraph is present precisely when the corresponding directed edge is present in the second digraph.

66. To show that the property that a graph is bipartite is an isomorphic invariant, we need to show that if G is bipartite and G is isomorphic to H, say via the function f, then H is bipartite. Let V_1 and V_2 be the partite sets for G. Then we claim that $f(V_1)$—the images under f of the vertices in V_1—and $f(V_2)$—the images under f of the vertices in V_2—form a bipartition for H. Indeed, since f must preserve the property of not being adjacent, since no two vertices in V_1 are adjacent, no two vertices in $f(V_1)$ are adjacent, and similarly for V_2.

68. **a)** There are 10 nonisomorphic directed graphs with 2 vertices. To see this, first consider graphs that have no edges from one vertex to the other. There are 3 such graphs, depending on whether they have no, one, or two loops. Similarly there are 3 in which there is an edge from each vertex to the other. Finally, there are 4 graphs that have exactly one edge between the vertices, because now the vertices are distinguished, and there can be or fail to be a loop at each vertex.

b) A detailed discussion of the number of directed graphs with 3 vertices would be rather long, so we will just give the answer, namely 104. There are some useful pictures relevant to this problem (and part **(c)** as well) in the appendix to *Graph Theory* by Frank Harary (Addison-Wesley, 1969).

c) The answer is 3069.

70. The answers depend on exactly how the storage is done, of course, but we will give naive answers that are at least correct as approximations.

a) We need one adjacency list for each vertex, and the list needs some sort of name or header; this requires n storage locations. In addition, each edge will appear twice, once in the list of each of its endpoints; this will require $2m$ storage locations. Therefore we need $n+2m$ locations in all.

b) The adjacency matrix is a $n \times n$ matrix, so it requires n^2 bits of storage.

c) The incidence matrix is a $n \times m$ matrix, so it requires nm bits of storage.

72. Assume the adjacency matrices of the two graphs are given. This will enable us to check whether a given pair of vertices are adjacent in constant time. For each pair of vertices u and v in V_1, check that u and v are adjacent in G_1 if and only if $f(u)$ and $f(v)$ are adjacent in G_2. This takes $O(1)$ comparisons for each pair, and there are $O(n^2)$ pairs for a graph with n vertices.

SECTION 10.4 Connectivity

2. **a)** This is a path of length 4, but it is not a circuit, since it ends at a vertex other than the one at which it began. It is simple, since no edges are repeated.

b) This is a path of length 4, which is a circuit. It is not simple, since it uses an edge more than once.

c) This is not a path, since there is no edge from d to b.

d) This is not a path, since there is no edge from b to d.

4. This graph is connected—it is easy to see that there is a path from every vertex to every other vertex.

6. The graph in Exercise 3 has three components: the piece that looks like a $\wedge$, the piece that looks like a $\vee$, and the isolated vertex. The graph in Exercise 4 is connected, with just one component. The graph in Exercise 5 has two components, each a triangle.

8. A connected component of a collaboration graph represent a maximal set of people with the property that for any two of them, we can find a string of joint works that takes us from one to the other. The word "maximal" here implies that nobody else can be added to this set of people without destroying this property.

10. An actor is in the same connected component as Kevin Bacon if there is a path from that person to Bacon. This means that the actor was in a movie with someone who was in a movie with someone who ... who was in a movie with Kevin Bacon. This includes Kevin Bacon, all actors who appeared in a movie with Kevin Bacon, all actors who appeared in movies with those people, and so on.

12. **a)** Notice that there is no path from f to a, so the graph is not strongly connected. However, the underlying undirected graph is clearly connected, so this graph is weakly connected.

b) Notice that the sequence a, b, c, d, e, f, a provides a path from every vertex to every other vertex, so this graph is strongly connected.

c) The underlying undirected graph is clearly not connected (one component consists of the triangle), so this graph is neither strongly nor weakly connected.

14. **a)** The cycle *baeb* guarantees that these three vertices are in one strongly connected component. Since there is no path from c to any other vertex, and there is no path from any other vertex to d, these two vertices are in strong components by themselves. Therefore the strongly connected components are $\{a, b, e\}$, $\{c\}$, and $\{d\}$.

b) The cycle *cdec* guarantees that these three vertices are in one strongly connected component. The vertices a, b, and f are in strong components by themselves, since there are no paths both to and from each of these to every other vertex. Therefore the strongly connected components are $\{a\}$, $\{b\}$ $\{c, d, e\}$, and $\{f\}$.

c) The cycle *abcdfghia* guarantees that these eight vertices are in one strongly connected component. Since there is no path from e to any other vertex, this vertex is in a strong component by itself. Therefore the strongly connected components are $\{a, b, c, d, f, g, h, i\}$ and $\{e\}$.

16. The given conditions imply that there is a path from u to v, a path from v to u, a path from v to w, and a path from w to v. Concatenating the first and third of these paths gives a path from u to w, and concatenating the fourth and second of these paths gives a path from w to u. Therefore u and w are mutually reachable.

18. Let $a, b, c, \ldots, z$ be the directed path. Since z and a are in the same strongly connected component, there is a directed path from z to a. This path appended to the given path gives us a circuit. We can reach any vertex on the original path from any other vertex on that path by going around this circuit.

20. The graph G has a simple closed path containing exactly the vertices of degree 3, namely $u_1u_2u_6u_5u_1$. The graph H has no simple closed path containing exactly the vertices of degree 3. Therefore the two graphs are not isomorphic.

22. We notice that there are two vertices in each graph that are not in cycles of size 4. So let us try to construct an isomorphism that matches them, say $u_1 \leftrightarrow v_2$ and $u_8 \leftrightarrow v_6$. Now u_1 is adjacent to u_2 and u_3, and v_2 is adjacent to v_1 and v_3, so we try $u_2 \leftrightarrow v_1$ and $u_3 \leftrightarrow v_3$. Then since u_4 is the other vertex adjacent to u_3 and v_4 is the other vertex adjacent to v_3 (and we already matched u_3 and v_3), we must have $u_4 \leftrightarrow v_4$. Proceeding along similar lines, we then complete the bijection with $u_5 \leftrightarrow v_8$, $u_6 \leftrightarrow v_7$, and $u_7 \leftrightarrow v_5$. Having thus been led to the only possible isomorphism, we check that the 12 edges of G exactly correspond to the 12 edges of H, and we have proved that the two graphs are isomorphic.

24. **a)** Adjacent vertices are in different parts, so every path between them must have odd length. Therefore there are no paths of length 2.

b) A path of length 3 is specified by choosing a vertex in one part for the second vertex in the path and a vertex in the other part for the third vertex in the path (the first and fourth vertices are the given adjacent vertices). Therefore there are $3 \cdot 3 = 9$ paths.

c) As in part **(a)**, the answer is 0.

d) This is similar to part **(b)**; therefore the answer is $3^4 = 81$.

26. Probably the best way to do this is to write down the adjacency matrix for this graph and then compute its powers. The matrix is

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

a) To find the number of paths of length 2, we need to look at $\mathbf{A}^2$, which is

$$\begin{bmatrix} 3 & 1 & 2 & 1 & 2 & 2 \\ 1 & 4 & 1 & 3 & 2 & 2 \\ 2 & 1 & 3 & 0 & 3 & 1 \\ 1 & 3 & 0 & 3 & 1 & 2 \\ 2 & 2 & 3 & 1 & 4 & 1 \\ 2 & 2 & 1 & 2 & 1 & 3 \end{bmatrix}.$$

Since the $(3,4)^{\text{th}}$ entry is 0, so there are no paths of length 2.

b) The $(3,4)^{\text{th}}$ entry of $\mathbf{A}^3$ turns out to be 8, so there are 8 paths of length 3.

c) The $(3,4)^{\text{th}}$ entry of $\mathbf{A}^4$ turns out to be 10, so there are 10 paths of length 4.

d) The $(3,4)^{\text{th}}$ entry of $\mathbf{A}^5$ turns out to be 73, so there are 73 paths of length 5.

e) The $(3,4)^{\text{th}}$ entry of $\mathbf{A}^6$ turns out to be 160, so there are 160 paths of length 6.

f) The $(3,4)^{\text{th}}$ entry of $\mathbf{A}^7$ turns out to be 739, so there are 739 paths of length 7.

28. We show this by induction on n. For $n = 1$ there is nothing to prove. Now assume the inductive hypothesis, and let G be a connected graph with $n+1$ vertices and fewer than n edges, where $n \geq 1$. Since the sum of the degrees of the vertices of G is equal to 2 times the number of edges, we know that the sum of the degrees is less than $2n$, which is less than $2(n+1)$. Therefore some vertex has degree less than 2. Since G is connected, this vertex is not isolated, so it must have degree 1. Remove this vertex and its edge. Clearly the result is still connected, and it has n vertices and fewer than $n-1$ edges, contradicting the inductive hypothesis. Therefore the statement holds for G, and the proof is complete.

30. Let v be a vertex of odd degree, and let H be the component of G containing v. Then H is a graph itself, so it has an even number of vertices of odd degree. In particular, there is another vertex w in H with odd degree. By definition of connectivity, there is a path from v to w.

32. Vertices c and d are the cut vertices. The removal of either one creates a graph with two components. The removal of any other vertex does not disconnect the graph.

34. The graph in Exercise 31 has no cut edges; any edge can be removed, and the result is still connected. For the graph in Exercise 32, $\{c,d\}$ is the only cut edge. There are several cut edges for the graph in Exercise 33: $\{a,b\}$, $\{b,c\}$, $\{c,d\}$, $\{c,e\}$, $\{e,i\}$, and $\{h,i\}$.

36. First we show that if c is a cut vertex, then there exist vertices u and v such that every path between them passes through c. Since the removal of c increases the number of components, there must be two vertices in G that are in different components after the removal of c. Then every path between these two vertices has to pass through c. Conversely, if u and v are as specified, then they must be in different components of the graph with c removed. Therefore the removal of c resulted in at least two components, so c is a cut vertex.

38. First suppose that $e = \{u, v\}$ is a cut edge. Every circuit containing e must contain a path from u to v in addition to just the edge e. Since there are no such paths if e is removed from the graph, every such path must contain e. Thus e appears twice in the circuit, so the circuit is not simple. Conversely, suppose that e is not a cut edge. Then in the graph with e deleted u and v are still in the same component. Therefore there is a simple path P from u to v in this deleted graph. The circuit consisting of P followed by e is a simple circuit containing e.

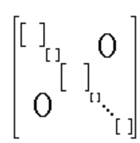
40. In the directed graph in Exercise 7, there is a path from b to each of the other three vertices, so $\{b\}$ is a vertex basis (and a smallest one). It is easy to see that $\{c\}$ and $\{d\}$ are also vertex bases, but a is not in any vertex basis. For the directed graph in Exercise 8, there is a path from b to each of a and c; on the other hand, d must clearly be in every vertex basis. Thus $\{b, d\}$ is a smallest vertex basis. So are $\{a, d\}$ and $\{c, d\}$. Every vertex basis for the directed graph in Exercise 9 must contain vertex e, since it has no incoming edges. On the other hand, from any other vertex we can reach all the other vertices, so e together with any one of the other four vertices will form a vertex basis.

42. By definition of graph, both G_1 and G_2 are nonempty. If they have no common vertex, then there clearly can be no paths from $v_1 \in G_1$ to $v_2 \in G_2$. In that case G would not be connected, contradicting the hypothesis.

44. First we obtain the inequality given in the hint. We claim that the maximum value of $\sum n_i^2$, subject to the constraint that $\sum n_i = n$, is obtained when one of the n_i's is as large as possible, namely $n - k + 1$, and the remaining n_i's (there are $k - 1$ of them) are all equal to 1. To justify this claim, suppose instead that two of the n_i's were a and b, with $a \geq b \geq 2$. If we replace a by $a + 1$ and b by $b - 1$, then the constraint is still satisfied, and the sum of the squares has changed by $(a+1)^2 + (b-1)^2 - a^2 - b^2 = 2(a - b) + 2 \geq 2$. Therefore the maximum cannot be attained unless the n_i's are as we claimed. Since there are only a finite number of possibilities for the distribution of the n_i's, the arrangement we give must in fact yield the maximum. Therefore $\sum n_i^2 \leq (n - k + 1)^2 + (k - 1) \cdot 1^2 = n^2 - (k - 1)(2n - k)$, as desired.

Now by Exercise 43, the number of edges of the given graph does not exceed $\sum C(n_i, 2) = \sum (n_i^2 + n_i)/2 = \big((\sum n_i^2) + n\big)/2$. Applying the inequality obtained above, we see that this does not exceed $(n^2 - (k-1)(2n - k) + n)/2$, which after a little algebra is seen to equal $(n - k)(n - k + 1)/2$. The upshot of all this is that the most edges are obtained if there is one component as large as possible, with all the other components consisting of isolated vertices.

46. Under these conditions, the matrix has a block structure, with all the 1's confined to small squares (of various sizes) along the main diagonal. The reason for this is that there are no edges between different components. See the picture for a schematic view. The only 1's occur inside the small submatrices (but not all the entries in these squares are 1's, of course).



48. **a)** If any vertex is removed from C_n, the graph that remains is a connected graph, namely a path with $n - 1$ vertices.

b) If the central vertex is removed, the resulting graph is a cycle, which is connected. If a vertex on the cycle of W_n is removed, the resulting graph is connected because every remaining vertex on the cycle is joined to the central vertex.

c) Let v be a vertex in one part and w a vertex in the other part, after some vertex has been removed (these exists because m and n are both greater than 1). Then v and w are joined by an edge, and every other vertex is joined by an edge to either v or w, giving us a connected graph.

d) We can use mathematical induction, based on the recursive definition of the n-cubes (see Example 8 in Section 10.2). The basis step is Q_2, which is the same as C_4, and we argued in part **(a)** that it has no cut vertex. Assume the inductive hypothesis. Let G be Q_{k+1} with a vertex removed. Then G consists of a copy of Q_k, which is certainly connected, a copy of Q_k with a vertex removed, which is connected by the inductive hypothesis, and at least one edge joining those two subgraphs; therefore G is connected.

50. **a)** Removing vertex b leaves two components, so $\kappa(G) = 1$. Removing one edge does not disconnect the graph, but removing edges ab and eb do disconnect the graph, so $\lambda(G) = 2$. The minimum degree is clearly 2. Thus only $\kappa(G) < \lambda(G)$ is strict.

b) Removing vertex c leaves two components, so $\kappa(G) = 1$. It is not hard to see that removing two edges does not disconnect the graph, but removing the three edges incident to vertex a, for example, does. Therefore $\lambda(G) = 3$. Since the minimum degree is also 3, only $\kappa(G) < \lambda(G)$ is a strict inequality.

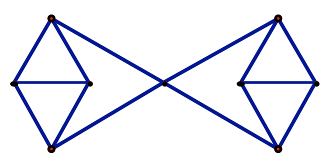
c) It is easy to see that removing only one vertex or one edge does not disconnect this graph, but removing vertices a and k, or removing edges ab and kl, does. Therefore $\kappa(G) = \lambda(G) = 2$. Since the minimum degree is 3, only the inequality $\lambda(G) < \min_{v\in V} \deg(v)$ is strict.

d) With a little effort we see that $\kappa(G) = \lambda(G) = \min_{v\in V} \deg(v) = 4$, so none of the inequalities is strict.

52. **a)** According to the discussion following Example 7, $\kappa(K_n) = n-1$. Conversely, if G is a graph with n vertices other than K_n, let u and v be two nonadjacent vertices of G. Then removing the $n-2$ vertices other than u and v disconnects G, so $\kappa(G) < n-1$.

b) Since $\kappa(K_n) \le \lambda(K_n) \le \min_{v\in K_n} \deg(v)$ (see the discussion following Example 9) and the outside quantities are both $n-1$, it follows that $\lambda(K_n) = n-1$. Conversely, if G is not K_n, then its minimum degree is less than $n-1$, so it edge connectivity is also less than $n-1$.

54. Here is one example.



56. The length of a shortest path is the smallest l such that there is at least one path of length l from v to w. Therefore we can find the length by computing successively $\mathbf{A}^1$, $\mathbf{A}^2$, $\mathbf{A}^3$, $\ldots$, until we find the first l such that the $(i,j)^{\text{th}}$ entry of $\mathbf{A}^l$ is not 0, where v is the i^{th} vertex and w is the j^{th}.

58. First we write down the adjacency matrix for this graph, namely

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Then we compute $\mathbf{A}^2$ and $\mathbf{A}^3$, and look at the $(1,3)^{\text{th}}$ entry of each. We find that these entries are 0 and 1, respectively. By the reasoning given in Exercise 57, we conclude that a shortest path has length 3.

60. Suppose that f is an isomorphism from graph G to graph H. If G has a simple circuit of length k, say $u_1, u_2, \ldots, u_k, u_1$, then we claim that $f(u_1), f(u_2), \ldots, f(u_k), f(u_1)$ is a simple circuit in H. Certainly this is a circuit, since each edge u_iu_{i+1} (and u_ku_1) in G corresponds to an edge $f(u_i)f(u_{i+1})$ (and $f(u_k)f(u_1)$) in H. Furthermore, since no edge was repeated in this circuit in G, no edge will be repeated when we use f to move over to H.

62. The adjacency matrix of G is as follows:

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

We compute $\mathbf{A}^2$ and $\mathbf{A}^3$, obtaining

$$\mathbf{A}^2 = \begin{bmatrix} 2 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 4 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 3 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{A}^3 = \begin{bmatrix} 2 & 3 & 5 & 2 & 1 & 2 & 1 \\ 3 & 2 & 5 & 2 & 1 & 2 & 1 \\ 5 & 5 & 4 & 6 & 1 & 6 & 1 \\ 2 & 2 & 6 & 2 & 3 & 5 & 1 \\ 1 & 1 & 1 & 3 & 0 & 1 & 1 \\ 2 & 2 & 6 & 5 & 1 & 2 & 3 \\ 1 & 1 & 1 & 1 & 1 & 3 & 0 \end{bmatrix}.$$

Already every off-diagonal entry in $\mathbf{A}^3$ is nonzero, so we know that there is a path of length 3 between every pair of distinct vertices in this graph. Therefore the graph G is connected.

On the other hand, the adjacency matrix of H is as follows:

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

We compute $\mathbf{A}^2$ through $\mathbf{A}^5$, obtaining the following matrices:

$$\mathbf{A}^2 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{bmatrix} \qquad \mathbf{A}^3 = \begin{bmatrix} 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 3 & 3 \\ 0 & 0 & 0 & 3 & 2 & 3 \\ 0 & 0 & 0 & 3 & 3 & 2 \end{bmatrix}$$

$$\mathbf{A}^4 = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 5 & 5 \\ 0 & 0 & 0 & 5 & 6 & 5 \\ 0 & 0 & 0 & 5 & 5 & 6 \end{bmatrix} \qquad \mathbf{A}^5 = \begin{bmatrix} 0 & 4 & 4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 10 & 11 & 11 \\ 0 & 0 & 0 & 11 & 10 & 11 \\ 0 & 0 & 0 & 11 & 11 & 10 \end{bmatrix}$$

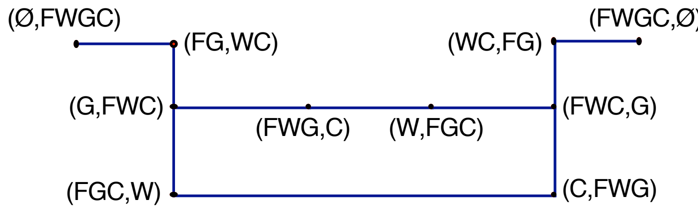
If we compute the sum $\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \mathbf{A}^4 + \mathbf{A}^5$ we obtain

$$\begin{bmatrix} 6 & 7 & 7 & 0 & 0 & 0 \\ 7 & 3 & 3 & 0 & 0 & 0 \\ 7 & 3 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 20 & 21 & 21 \\ 0 & 0 & 0 & 21 & 20 & 21 \\ 0 & 0 & 0 & 21 & 21 & 20 \end{bmatrix}.$$

There is a 0 in the $(1,4)$ position, telling us that there is no path of length at most 5 from vertex a to vertex d. Since the graph only has six vertices, this tells us that there is no path at all from a to d. Thus the fact that there was a 0 as an off-diagonal entry in the sum told us that the graph was not connected.

64. **a)** To proceed systematically, we list the states in order of decreasing population on the left shore. The allowable states are then $(FWGC, \emptyset)$, (FWG, C), (FWC, G), (FGC, W), (FG, WC), (WC, FG) (C, FWG), (G, FWC), (W, FGC), and $(\emptyset, FWGC)$. Notice that, for example, (GC, FW) and (WGC, F) are not allowed by the rules.

b) The graph is as shown here. Notice that the boat can carry only the farmer and one other object, so the transitions are rather restricted.



c) The path in the graph corresponds to the moves in the solution.

d) There are two simple paths from $(FWGC, \emptyset)$ to $(\emptyset, FWGC)$ that can be easily seen in the graph. One is $(FWGC, \emptyset)$, (WC, FG), (FWC, G), (W, FGC), (FWG, C), (G, FWC), (FG, WC), $(\emptyset, FWGC)$. The other is $(FWGC, \emptyset)$, (WC, FG), (FWC, G), (C, FWG), (FGC, W), (G, FWC), (FG, WC), $(\emptyset, FWGC)$.

e) Both solutions cost \$4.

66. If we use the ordered pair (a, b) to indicate that the three-gallon jug has a gallons in it and the five-gallon jug has b gallons in it, then we start with $(0, 0)$ and can do the following things: fill a jug that is empty or partially empty (so that, for example, we can go from $(0, 3)$ to $(3, 3)$); empty a jug; or transfer some or all of the contents of a jug to the other jug , as long as we either completely empty the donor jug or completely fill the receiving jug. A simple solution to the puzzle uses this directed path: $(0, 0) \to (3, 0) \to (0, 3) \to (3, 3) \to (1, 5)$.

SECTION 10.5 Euler and Hamilton Paths

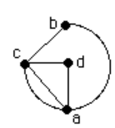
2. All the vertex degrees are even, so there is an Euler circuit. We can find one by trial and error, or by using Algorithm 1. One such circuit is $a, b, c, f, i, h, g, d, e, h, f, e, b, d, a$.

4. This graph has no Euler circuit, since the degree of vertex c (for one) is odd. There is an Euler path between the two vertices of odd degree. One such path is $f, a, b, c, d, e, f, b, d, a, e, c$.

6. This graph has no Euler circuit, since the degree of vertex b (for one) is odd. There is an Euler path between the two vertices of odd degree. One such path is $b, c, d, e, f, d, g, i, d, a, h, i, a, b, i, c$.

8. All the vertex degrees are even, so there is an Euler circuit. We can find one by trial and error, or by using Algorithm 1. One such circuit is $a, b, c, d, e, j, c, h, i, d, b, g, h, m, n, o, j, i, n, l, m, f, g, l, k, f, a$.

10. The graph model for this exercise is as shown here.



Vertices a and b are the banks of the river, and vertices c and d are the islands. Each vertex has even degree, so the graph has an Euler circuit, such as a, c, b, a, d, c, a. Therefore a walk of the type described is possible.

12. The algorithm is essentially the same as Algorithm 1. If there are no vertices of odd degree, then we simply use Algorithm 1, of course. If there are exactly two vertices of odd degree, then we begin constructing the initial path at one such vertex, and it will necessarily end at the other when it cannot be extended any further. Thereafter we follow Algorithm 1 exactly, splicing new circuits into the path we have constructed so far until no unused edges remain.

14. See the comments in the solution to Exercise 13. This graph has exactly two vertices of odd degree; therefore it has an Euler path and can be so traced.

16. First suppose that the directed multigraph has an Euler circuit. Since this circuit provides a path from every vertex to every other vertex, the graph must be strongly connected (and hence also weakly connected). Also, we can count the in-degrees and out-degrees of the vertices by following this circuit; as the circuit passes through a vertex, it adds one to the count of both the in-degree (as it comes in) and the out-degree (as it leaves). Therefore the two degrees are equal for each vertex.

Conversely, suppose that the graph meets the conditions stated. Then we can proceed as in the proof of Theorem 1 and construct an Euler circuit.

18. For Exercises 18–23 we use the results of Exercises 16 and 17. This directed graph satisfies the condition of Exercise 17 but not that of Exercise 16. Therefore there is no Euler circuit. The Euler path must go from a to d. One such path is $a, b, d, b, c, d, c, a, d$.

20. The conditions of Exercise 16 are met, so there is an Euler circuit, which is perforce also an Euler path. One such path is $a, d, b, d, e, b, e, c, b, a$.

22. This directed graph satisfies the condition of Exercise 17 but not that of Exercise 16. Therefore there is no Euler circuit. The Euler path must go from c to b. One such path is $c, e, b, d, c, b, f, d, e, f, e, a, f, a, b, c, b$. (There is no Euler circuit, however, since the conditions of Exercise 16 are not met.)

24. The algorithm is identical to Algorithm 1.

26. **a)** The degrees of the vertices ($n-1$) are even if and only if n is odd. Therefore there is an Euler circuit if and only if n is odd (and greater than 1, of course).

b) For all $n \geq 3$, clearly C_n has an Euler circuit, namely itself.

c) Since the degrees of the vertices around the rim are all odd, no wheel has an Euler circuit.

d) The degrees of the vertices are all n. Therefore there is an Euler circuit if and only if n is even (and greater than 0, of course).

28. **a)** Since the degrees of the vertices are all m and n, this graph has an Euler circuit if and only if both of the positive integers m and n are even.

b) All the graphs listed in part **(a)** have an Euler circuit, which is also an Euler path. In addition, the graphs $K_{2,n}$ for odd n (and $K_{m,2}$ for odd m) have exactly 2 vertices of odd degree, so they have an Euler path but not an Euler circuit. Also, $K_{1,1}$ obviously has an Euler path. All other complete bipartite graphs have too many vertices of odd degree.

30. This graph can have no Hamilton circuit because of the cut edge $\{c, f\}$. Every simple circuit must be confined to one of the two components obtained by deleting this edge.

32. As in Exercise 30, the cut edge ($\{e, f\}$ in this case) prevents a Hamilton circuit.

34. This graph has no Hamilton circuit. If it did, then certainly the circuit would have to contain edges $\{d,a\}$ and $\{a,b\}$, since these are the only edges incident to vertex a. By the same reasoning, the circuit would have to contain the other six edges around the outside of the figure. These eight edges already complete a circuit, and this circuit omits the nine vertices on the inside. Therefore there is no Hamilton circuit.

36. It is easy to find a Hamilton circuit here, such as a, d, g, h, i, f, c, e, b, and back to a.

38. This graph has the Hamilton path a,b,c,d,e.

40. This graph has no Hamilton path. There are three vertices of degree 1; each of them would have to be an end vertex of every Hamilton path. Since a path has only 2 ends, this is impossible.

42. It is easy to find the Hamilton path d, c, a, b, e here.

44. **a)** Obviously K_n has a Hamilton circuit for all $n \geq 3$ but not for $n \leq 2$.
b) Obviously C_n has a Hamilton circuit for all $n \geq 3$.
c) A Hamilton circuit for C_n can easily be extended to one for W_n by replacing one edge along the rim of the wheel by two edges, one going to the center and the other leading from the center. Therefore W_n has a Hamilton circuit for all $n \geq 3$.
d) This is Exercise 49; see the solution given for it.

46. We do the easy part first, showing that the graph obtained by deleting a vertex from the Petersen graph has a Hamilton circuit. By symmetry, it makes no difference which vertex we delete, so assume that it is vertex j. Then a Hamilton circuit in what remains is a,e,d,i,g,b,c,h,f,a. Now we show that the entire graph has no Hamilton circuit. Assume that a Hamilton circuit exists. Not all the edges around the outside can be used, so without loss of generality assume that $\{c,d\}$ is not used. Then $\{e,d\}$, $\{d,i\}$, $\{h,c\}$, and $\{b,c\}$ must all be used. If $\{a,f\}$ is not used, then $\{e,a\}$, $\{a,b\}$, $\{f,i\}$, and $\{f,h\}$ must be used, forming a premature circuit. Therefore $\{a,f\}$ is used. Without loss of generality we may assume that $\{e,a\}$ is also used, and $\{a,b\}$ is not used. Then $\{b,g\}$ is also used, and $\{e,j\}$ is not. But this requires $\{g,j\}$ and $\{h,j\}$ to be used, forming a premature circuit b,c,h,j,g,b. Hence no Hamilton circuit can exist in this graph.

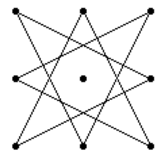
48. We want to look only at odd n, since if n is even, then being at least $(n-1)/2$ is the same as being at least $n/2$, in which case Dirac's theorem would apply. One way to avoid having a Hamilton circuit is to have a cut vertex—a vertex whose removal disconnects the graph. The simplest example would be the "bow-tie" graph with five vertices (a, b, c, d, and e), where cut vertex c is adjacent to each of the other vertices, and the only other edges are ab and de. Every vertex has degree at least $(5-1)/2 = 2$, but there is no Hamilton circuit.

50. Let us begin at vertex a and walk toward vertex b. Then the circuit begins a,b,c. At this point we must choose among three edges to continue the circuit. If we choose edge $\{c,f\}$, then we will have disconnected the graph that remains, so we must not choose this edge. Suppose instead that the circuit continues with edge $\{c,d\}$. Then the entire circuit is forced to be a,b,c,d,e,c,f,a.

52. This proof is rather hard. See page 63 of *Graph Theory with Applications* by J. A. Bondy and U. S. R. Murty (American Elsevier, 1976).

54. An Euler path will cover every link, so it can be used to test the links. A Hamilton path will cover all the devices, so it can be used to test the devices.

56. We draw one vertex for each of the 9 squares on the board. We then draw an edge from a vertex to each vertex that can be reached by moving 2 units horizontally and 1 unit vertically or vice versa. The result is as shown.



58. **a)** In a Hamilton path we need to visit each vertex once, moving along the edges. A knight's tour is precisely such a path, since we visit each square once, making legal moves.

b) This is the same as part **(a)**, except that a re-entrant tour must return to its starting point, just as a Hamilton circuit must return to its starting point.

60. In a 3×3 board, the middle vertex is isolated (see solution to Exercise 56). In other words, there is no knight move to or from the middle square. Thus there can clearly be no knight's tour. There is a tour of the rest of the squares, however, as the picture above shows.

62. Each square of the board can be thought of as a pair of integers (x, y). Let A be the set of squares for which $x + y$ is odd, and let B be the set of squares for which $x + y$ is even. This partitions the vertex set of the graph representing the legal moves of a knight on the board into two parts. Now every move of the knight changes $x + y$ by an odd number—either $1 + 2 = 3$, $2 - 1 = 1$, $1 - 2 = -1$, or $-1 - 2 = -3$. Therefore every edge in this graph joins a vertex in A to a vertex in B. Thus the graph is bipartite.

64. A little trial and error, loosely following the hint, produced the following solution. The numbers show the order in which the squares are to be traversed.

1	28	13	26	3	38	41	16
64	25	2	39	52	15	4	37
29	12	27	14	57	40	17	42
24	63	56	53	60	51	36	5
11	30	49	62	55	58	43	18
48	23	54	59	50	61	6	35
31	10	21	46	33	8	19	44
22	47	32	9	20	45	34	7

66. We assume that the graph is given to us in terms of adjacency lists for all the vertices. We also maintain a queue (or stack) of vertices that have been visited, eliminating vertices when they are incident to no more unused edges. Each vertex in this list also has a pointer to a spot in the circuit constructed so far at which this vertex appears. We keep the circuit as a circularly linked list. Finding the initial circuit can be done by starting at some vertex, and as we reach each new vertex that still has unused edges emanating from it (which we can know by consulting its adjacency list) we add the new edge to the circuit and delete it from the relevant adjacency lists. All this takes $O(m)$ time. For the **while** loop, finding a vertex at which to begin the subcircuit can be done in $O(1)$ time by consulting the queue, and then finding the subcircuit takes $O(m)$ time. Splicing the subcircuit into the circuit takes $O(1)$ time. Furthermore, finding *all* the subcircuits takes at most $O(m)$ time in total, because each edge is used only once in the entire process. Thus the total time is $O(m)$.

SECTION 10.6 Shortest-Path Problems

2. In the solution to Exercise 5 we find a shortest path. Its length is 7.

4. In the solution to Exercise 5 we find a shortest path. Its length is 16.

6. The solution to this problem is given in the solution to Exercise 7, where the paths themselves are found.

8. In theory, we can use Dijkstra's algorithm. In practice with graphs of this size and shape, we can tell by observation what the conceivable answers will be and find the one that produces the minimum total length by inspection.
a) The direct path is the shortest.
b) The path via Chicago only is the shortest.
c) The path via Atlanta and Chicago is the shortest.
d) The path via Atlanta, Chicago and Denver is the shortest.

10. The comments for Exercise 8 apply.
a) The direct flight is the cheapest.
b) The path via New York is the cheapest.
c) The path via New York and Chicago is the cheapest.
d) The path via New York is the cheapest.

12. The comments for Exercise 8 apply.
a) The path through Chicago is the fastest.
b) The path via Chicago is the fastest.
c) The path via Denver (or the path via Los Angeles) is the fastest.
d) The path via Dallas (or the path via Chicago) is the fastest.

14. Here we simply assign the weight of 1 to each edge.

16. We need to keep track of the vertex from which a shortest path known so far comes, as well as the length of that path. Thus we add an array P to the algorithm, where $P(v)$ is the previous vertex in the best known path to v. We modify Algorithm 1 so that when L is updated by the statement $L(v) := L(u) + w(u,v)$, we also set $P(v) := u$. Once the **while** loop has terminated, we can obtain a shortest path from a to z *in reverse* by starting with z and following the pointers in P. Thus the path in reverse is z, $P(z)$, $P(P(z))$, $\ldots$, $P(P(\cdots P(z)\cdots)) = a$.

18. The shortest path need not be unique. For example, we could have a graph with vertices a, b, c, and d, with edges $\{a,b\}$ of weight 3, $\{b,c\}$ of weight 7, $\{a,d\}$ of weight 4, and $\{d,c\}$ of weight 6. There are two shortest paths from a to c.

20. We give an ad hoc analysis. Recall that a simple path cannot use any edge more than once. Furthermore, since the path must use an odd number of edges incident to a and an odd number of edges incident to z, the path must omit at least two edges, one at each end. The best we could hope for, then, in trying for a path of maximum length, is that the path leaves out the shortest such edges—$\{a,c\}$ and $\{e,z\}$. If the path leaves out these two edges, then it must also leave out one more edge incident to c, since the path must use an even number of the three remaining edges incident to c. The best we could hope for is that the path omits the two aforementioned edges and edge $\{b,c\}$. Since $2+1<4$, this is better than the other possibility, namely omitting edge $\{a,b\}$ instead of edge $\{a,c\}$. Finally, we find a simple path omitting only these three edges, namely a,b,d,c,e,d,z, with length 35, and thus we conclude that it is a longest simple path from a to z.

A similar argument shows that the longest simple path from c to z is c, a, b, d, c, e, d, z

22. It follows by induction on i that after the i^{th} pass through the triply nested **for** loop in the pseudocode, $d(v_j, v_k)$ gives, for each j and k, the shortest distance between v_j and v_k using only intermediate vertices v_m for $m \leq i$. Therefore after the final path, we have obtained the shortest distance.

24. Consider the graph with vertices a, b, and z, where the weight of $\{a, z\}$ is 2, the weight of $\{a, b\}$ is 3, and the weight of $\{b, z\}$ is -2. Then Dijkstra's algorithm will decide that $L(z) = 2$ and stop, whereas the path a, b, z is shorter (has length 1).

26. The following table shows the twelve different Hamilton circuits and their weights:

Circuit	Weight
a-b-c-d-e-a	$3 + 10 + 6 + 1 + 7 = 27$
a-b-c-e-d-a	$3 + 10 + 5 + 1 + 4 = 23$
a-b-d-c-e-a	$3 + 9 + 6 + 5 + 7 = 30$
a-b-d-e-c-a	$3 + 9 + 1 + 5 + 8 = 26$
a-b-e-c-d-a	$3 + 2 + 5 + 6 + 4 = 20$
a-b-e-d-c-a	$3 + 2 + 1 + 6 + 8 = 20$
a-c-b-d-e-a	$8 + 10 + 9 + 1 + 7 = 35$
a-c-b-e-d-a	$8 + 10 + 2 + 1 + 4 = 25$
a-c-d-b-e-a	$8 + 6 + 9 + 2 + 7 = 32$
a-c-e-b-d-a	$8 + 5 + 2 + 9 + 4 = 28$
a-d-b-c-e-a	$4 + 9 + 10 + 5 + 7 = 35$
a-d-c-b-e-a	$4 + 6 + 10 + 2 + 7 = 29$

Thus we see that the circuits a-b-e-c-d-a and a-b-e-d-c-a (or the same circuits starting at some other point but traversing the vertices in the same or exactly opposite order) are the ones with minimum total weight.

28. The following table shows the twelve different Hamilton circuits and their weights, where we abbreviate the cities with the beginning letter of their name, except that New Orleans is O:

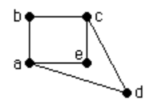
Circuit	Weight
S-B-N-O-P-S	$409 + 109 + 229 + 309 + 119 = 1175$
S-B-N-P-O-S	$409 + 109 + 319 + 309 + 429 = 1575$
S-B-O-N-P-S	$409 + 239 + 229 + 319 + 119 = 1315$
S-B-O-P-N-S	$409 + 239 + 309 + 319 + 389 = 1665$
S-B-P-N-O-S	$409 + 379 + 319 + 229 + 429 = 1765$
S-B-P-O-N-S	$409 + 379 + 309 + 229 + 389 = 1715$
S-N-B-O-P-S	$389 + 109 + 239 + 309 + 119 = 1165$
S-N-B-P-O-S	$389 + 109 + 379 + 309 + 429 = 1615$
S-N-O-B-P-S	$389 + 229 + 239 + 379 + 119 = 1355$
S-N-P-B-O-S	$389 + 319 + 379 + 239 + 429 = 1755$
S-O-B-N-P-S	$429 + 239 + 109 + 319 + 119 = 1215$
S-O-N-B-P-S	$429 + 229 + 109 + 379 + 119 = 1265$

As a check of our arithmetic, we can compute the total weight (price) of all the trips (it comes to 17580) and check that it is equal to 6 times the sum of the weights (which here is 2930), since each edge appears in six paths (and sure enough, $17580 = 6 \cdot 2930$). We see that the circuit S-N-B-O-P-S (or the same circuit starting at some other point but traversing the vertices in the same or exactly opposite order) is the one with minimum total weight, 1165.

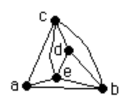
30. We follow the hint. Let G be our original weighted graph, and construct a new graph G' as follows. The vertices and edges of G' are the same as the vertices and edges of G. For each pair of vertices u and v in G, use an algorithm such as Dijkstra's algorithm to find a shortest path (i.e., one of minimum total weight) between u and v. Record this path in a table, and assign to the edge $\{u, v\}$ in G' the weight of this path. It is now clear that finding the circuit of minimum total weight in G' that visits each vertex exactly once is equivalent to finding the circuit of minimum total weight in G that visits each vertex at least once.

SECTION 10.7 Planar Graphs

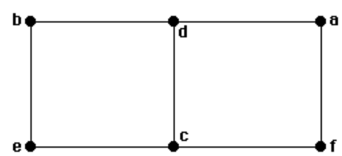
2. For convenience we label the vertices a, b, c, d, e, starting with the vertex in the lower left corner and proceeding clockwise around the outside of the figure as drawn in the exercise. If we move vertex d down, then the crossings can be avoided.



4. For convenience we label the vertices a, b, c, d, e, starting with the vertex in the lower left corner and proceeding clockwise around the outside of the figure as drawn in the exercise. If we move vertex b far to the right, and squeeze vertices d and e in a little, then we can avoid crossings.



6. This graph is easily untangled and drawn in the following planar representation.



8. If one has access to software such as *The Geometer's Sketchpad*, then this problem can be solved by drawing the graph and moving the points around, trying to find a planar drawing. If we are unable to find one, then we look for a reason why—either a subgraph homeomorphic to K_5 or one homeomorphic to $K_{3,3}$ (always try the latter first). In this case we find that there is in fact an actual copy of $K_{3,3}$, with vertices a, c, and e in one set and b, d, and f in the other.

10. The argument is similar to the argument when v_3 is inside region R_2. In the case at hand the edges between v_3 and v_4 and between v_3 and v_5 separate R_1 into two subregions, R_{11} (bounded by v_1, v_4, v_3, and v_5) and R_{12} (bounded by v_2, v_4, v_3, and v_5). Now again there is no way to place vertex v_6 without forcing a crossing. If v_6 is in R_2, then there is no way to draw the edge $\{v_3, v_6\}$ without crossing another edge. If v_6 is in R_{11}, then the edge between v_2 and v_6 cannot be drawn; whereas if v_6 is in R_{12}, then the edge between v_1 and v_6 cannot be drawn.

12. Euler's formula says that $v - e + r = 2$. We are given $v = 8$, and from the fact that the sum of the degrees equals twice the number of edges, we deduce that $e = (3 \cdot 8)/2 = 12$. Therefore $r = 2 - v + e = 2 - 8 + 12 = 6$.

14. Euler's formula says that $v - e + r = 2$. We are given $e = 30$ and $r = 20$. Therefore $v = 2 - r + e = 2 - 20 + 30 = 12$.

16. A bipartite simple graph has no simple circuits of length three. Therefore the inequality follows from Corollary 3.

18. If we add $k-1$ edges, we can make the graph connected, create no new regions, and still avoid edge crossings. (We just add an edge from one vertex in one component, incident to the unbounded region, to one vertex in each of the other components.) For this new graph, Euler's formula tells us that $v-(e+k-1)+r=2$. This simplifies algebraically to $r=e-v+k+1$.

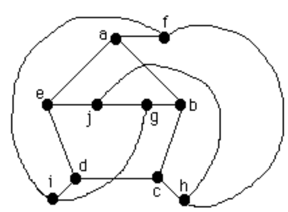
20. This graph is not homeomorphic to $K_{3,3}$, since by rerouting the edge between a and h we see that it is planar.

22. Replace each vertex of degree two and its incident edges by a single edge. Then the result is $K_{3,3}$: the parts are $\{a,e,i\}$ and $\{c,g,k\}$. Therefore this graph is homeomorphic to $K_{3,3}$.

24. This graph is nonplanar. If we delete the five curved edges outside the big pentagon, then the graph is homeomorphic to K_5. We can see this by replacing each vertex of degree 2 and its two edges by one edge.

26. If we follow the proof in Example 3, we see how to construct a planar representation of all of $K_{3,3}$ except for one edge. In particular, if we place vertex v_6 inside region R_{22} of Figure 7(b), then we can draw edges from v_6 to v_2 and v_3 with no crossings, and to v_1 with only one crossing. Furthermore, since $K_{3,3}$ is not planar, its crossing number cannot be 0. Hence its crossing number is 1.

28. First note that the Petersen graph with one edge removed is not planar; indeed, by Example 9, the Petersen graph with three mutually adjacent edges removed is not planar. Therefore the crossing number must be greater than 1. (If it were only 1, then removing the edge that crossed would give a planar drawing of the Petersen graph minus one edge.) The following figure shows a drawing with only two crossings. (This drawing was obtained by a little trial and error.) Therefore the crossing number must be 2. (In this figure, the vertices are labeled as in Figure 14(a).)

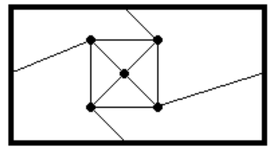


30. Since by Exercise 26 we know how to embed all but one edge of $K_{3,3}$ in one plane with no crossings, we can embed all of $K_{3,3}$ in two planes with no crossings simply by drawing the last edge in the second plane.

32. By Corollary 1 to Euler's formula, we know that in one plane we can draw without crossing at most $3v-6$ edges from a graph with v vertices. Therefore if a graph has v vertices and e edges, then it will require at least $e/(3v-6)$ planes in order to draw all the edges without crossing. Since the thickness is a whole number, it must be greater than or equal to the smallest integer at least this large, i.e., $\lceil e/(3v-6)\rceil$.

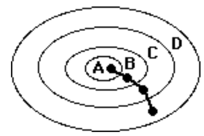
34. This is essentially the same as Exercise 32, using Corollary 3 in place of Corollary 1.

36. As in the solution to Exercise 37, we represent the torus by a rectangle. The figure below shows how K_5 is embedded without crossings. (The reader might try to embed K_6 or K_7 on a torus.)



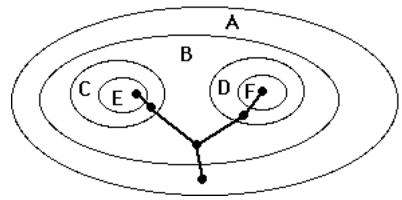
SECTION 10.8 Graph Coloring

2. We construct the dual as in Exercise 1.



As in Exercise 1, the number of colors needed to color this map is the same as the number of colors needed to color the dual graph. Clearly two colors are necessary and sufficient: one for vertices (regions) A and C, and the other for B and D.

4. We construct the dual as in Exercise 1.



As in Exercise 1, the number of colors needed to color this map is the same as the number of colors needed to color the dual graph. Clearly two colors are necessary and sufficient: one for vertices (regions) A, C, and D, and the other for B, E, and F.

6. Since there is a triangle, at least 3 colors are needed. To show that 3 colors suffice, notice that we can color the vertices around the outside alternately using red and blue, and color vertex g green.

8. Since there is a triangle, at least 3 colors are needed. The coloring in which b and c are blue, a and f are red, and d and e are green shows that 3 colors suffice.

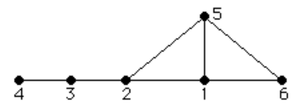
10. Since vertices b, c, h, and i form a K_4, at least 4 colors are required. A coloring using only 4 colors (and we can get this by trial and error, without much difficulty) is to let a and c be red; b, d, and f, blue; g and i, green; and e and h, yellow.

12. In Exercise 5 the chromatic number is 3, but if we remove vertex a, then the chromatic number will fall to 2. In Exercise 6 the chromatic number is 3, but if we remove vertex g, then the chromatic number will fall to 2. In Exercise 7 the chromatic number is 3, but if we remove vertex b, then the chromatic number will fall to 2. In Exercise 8 the chromatic number was shown to be 3. Even if we remove a vertex, at least one of the two triangles *ace* and *bdf* must remain, since they share no vertices. Therefore the smaller graph will still have chromatic number 3. In Exercise 9 the chromatic number is 2. Obviously it is not possible to reduce it to 1 by removing one vertex, since at least one edge will remain. In Exercise 10 the chromatic number was shown to be 4, and a coloring was provided. If we remove vertex h and recolor vertex e red, then we can eliminate color yellow from that solution. Therefore we will have reduced the chromatic number to 3. Finally, the graph in Exercise 11 will still have a triangle, no matter what vertex is removed, so we cannot lower its chromatic number below 3 by removing a vertex.

14. Since the map is planar, we know that four colors suffice. That four colors are necessary can be seen by looking at Kentucky. It is surrounded by Tennessee, Missouri, Illinois, Indiana, Ohio, West Virginia, and Virginia; furthermore the states in this list form a C_7, each one adjacent to the next. Therefore at least three colors are needed to color these seven states (see Exercise 16), and then a fourth is necessary for Kentucky.

16. Let the circuit be v_1, v_2, $\ldots$, v_n, v_1, where n is odd. Suppose that two colors (red and blue) sufficed to color the graph containing this circuit. Without loss of generality let the color of v_1 be red. Then v_2 must be blue, v_3 must be red, and so on, until finally v_n must be red (since n is odd). But this is a contradiction, since v_n is adjacent to v_1. Therefore at least three colors are needed.

18. We draw the graph in which two vertices (representing locations) are adjacent if the locations are within 150 miles of each other.



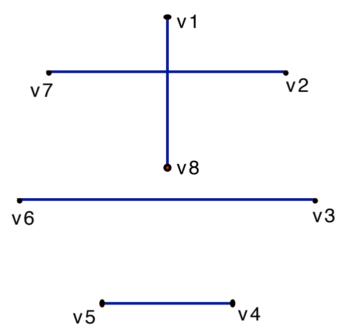
Clearly three colors are necessary and sufficient to color this graph, say red for vertices 4, 2, and 6; blue for 3 and 5; and yellow for 1. Thus three channels are necessary and sufficient.

20. We let the vertices of a graph be the animals, and we draw an edge between two vertices if the animals they represent cannot be in the same habitat because of their eating habits. A coloring of this graph gives an assignment of habitats (the colors are the habitats).

22. We model the circuit board with a graph: The n vertices correspond to the n devices, with an edge between each pair of devices connected by a wire. Then coloring the edges corresponds to coloring the wires, and the given requirement about the colors of the wires is exactly the requirement for an edge coloring. Therefore the number of colors needed for the wires is the edge chromatic number of the graph.

24. If there is a vertex with degree d, then there are d edges incident with a common vertex. Thus in any edge coloring each of those edges must get a different color, so we need at least d colors.

26. This is really a problem about scheduling a round-robin tournament. Let the vertices of K_n be $v_1, v_2, \ldots, v_n$. These are the players in the tournament. We join two vertices with an edge of color i if those two players meet in round i of the tournament. First suppose that n is even. Place v_n in the center of a circle, with the remaining vertices evenly spaced on the circle, as shown here for $n = 8$. The first round of the tournament uses edges $v_n v_1$, $v_2 v_{n-1}$, $v_3 v_{n-2}$, $\ldots$, $v_{n/2} v_{(n/2)+1}$; these edges, shown in the diagram, get color 1.



For the second round, rotate this picture by an angle of $360/(n-1)$ degrees clockwise. Thus in round 2, the matchings are $v_n v_2$, $v_1 v_3$, $v_4 v_{n-1}$, $v_5 v_{n-2}$, $\ldots$, and so on. Continue in this manner for $n-1$ rounds in all. It is not hard to see that every edge of K_n appears in exactly one of these matchings. (Indeed, the edges other than the radial edge join vertices whose indexes differ by 1, 2, $\ldots$, $(n-2)/2$ modulo $n-1$.) Therefore the edge chromatic number of K_n when n is even is $n-1$. (We cannot do better than this because we can have at most $n/2$ edges of each color and need $(n-1)n/2$ edges in all.)

For n odd (other than the trivial case $n = 1$), we can have at most $(n-1)/2$ edges of each color, and so we will need at least n colors. We can accomplish this in the same manner by creating a fictitious $(n+1)^{\text{st}}$ player and using the procedure for n even. (Playing against player $n+1$ means having a bye during that round of the tournament.) Thus the edge chromatic number of K_n when n is odd is n.

28. Since each of the n vertices in this subgraph must have a different color, the chromatic number must be at least n.

30. Our pseudocode is as follows. The comments should explain how it implements the algorithm.

```
procedure coloring(G : simple graph)
{assume that the vertices are labeled 1, 2, ..., n so that
   deg(1) ≥ deg(2) ≥ ··· ≥ deg(n) }
for i := 1 to n
        c(i) := 0 {originally no vertices are colored}
count := 0 {no vertices colored yet}
color := 1 {try the first color}
while count < n {there are still vertices to be colored}
        for i := 1 to n {try to color vertex i with color color}
                if c(i) = 0 {vertex i is not yet colored} then
                        c(i) := color {assume we can do it until we find out otherwise}
                        for j := 1 to n
                                if {i, j} is an edge and c(j) = color
                                        then c(i) := 0 {we found out otherwise}
                        if c(i) = color
                                then count := count + 1 {the new coloring of i worked}
        color := color + 1 {we have to go on to the next color}
{the coloring is complete}
```

32. We know that the chromatic number of an odd cycle is 3 (see Example 4). If we remove one edge, then we get a path, which clearly can be colored with two colors. This shows that the cycle is chromatically 3-critical.

34. Although the chromatic number of W_4 is 3, if we remove one edge then the graph still contains a triangle, so its chromatic number remains 3. Therefore W_4 is not chromatically 3-critical.

36. First let us prove some general results. In a complete graph, each vertex is adjacent to every other vertex, so each vertex must get its own set of k different colors. Therefore if there are n vertices, kn colors are clearly necessary and sufficient. Thus $\chi_k(K_n) = kn$. In a bipartite graph, every vertex in one part can get the same set of k colors, and every vertex in the other part can get the same set of k colors (a disjoint set from the colors assigned to the vertices in the first part). Therefore $2k$ colors are sufficient, and clearly $2k$ colors are required if there is at least one edge. Let us now look at the specific graphs.

a) For this complete graph situation we have $k = 2$ and $n = 3$, so $2 \cdot 3 = 6$ colors are necessary and sufficient.

b) As in part **(a)**, the answer is kn, which here is $2 \cdot 4 = 8$.

c) Call the vertex in the middle of the wheel m, and call the vertices around the rim, in order, a, b, c, and d. Since m, a, and b form a triangle, we need at least 6 colors. Assign colors 1 and 2 to m, 3 and 4 to a, and 5 and 6 to b. Then we can also assign 3 and 4 to c, and 5 and 6 to d, completing a 2-tuple coloring with 6 colors. Therefore $\chi_2(W_4) = 6$.

d) First we show that 4 colors are not sufficient. If we had only colors 1 through 4, then as we went around the cycle we would have to assign, say, 1 and 2 to the first vertex, 3 and 4 to the second, 1 and 2 to the third, and 3 and 4 to the fourth. This gives us no colors for the final vertex. To see that 5 colors are sufficient, we simply give the coloring: In order around the cycle the colors are $\{1,2\}$, $\{3,4\}$, $\{1,5\}$, $\{2,4\}$, and $\{3,5\}$. Therefore $\chi_2(C_5) = 5$.

e) By our general result on bipartite graphs, the answer is $2k = 2 \cdot 2 = 4$.

f) By our general result on complete graphs, the answer is $kn = 3 \cdot 5 = 15$.

g) We claim that the answer is 8. To see that eight colors suffice, we can color the vertices as follows in order around the cycle: $\{1,2,3\}$, $\{4,5,6\}$, $\{1,2,7\}$, $\{3,6,8\}$, and $\{4,5,7\}$. Showing that seven colors are not sufficient is harder. Assume that a coloring with seven colors exists. Without loss of generality, color the first vertex $\{1,2,3\}$ and color the second vertex $\{4,5,6\}$. If the third vertex is colored $\{1,2,3\}$, then the fourth and fifth vertices would need to use six colors different from 1, 2, and 3, for a total of nine colors. Therefore without loss of generality, assume that the third vertex is colored $\{1, 2, 7\}$. But now the other two vertices cannot have colors 1 or 2, and they must have six different colors, so eight colors would be required in all. This is a contradiction, so there is in fact no coloring with just seven colors.

h) By our general result on bipartite graphs, the answer is $2k = 2 \cdot 3 = 6$.

38. As we observed in the solution to Exercise 36, the answer is $2k$ if G has at least one edge (and it is clearly k if G has no edges, since every vertex can get the same colors).

40. We use induction on the number of vertices of the graph. Every graph with six or fewer vertices can be colored with six or fewer colors, since each vertex can get a different color. That takes care of the basis case(s). So we assume that all graphs with k vertices can be 6-colored and consider a graph G with $k+1$ vertices. By Corollary 2 in Section 10.7, G has a vertex v with degree at most 5. Remove v to form the graph G'. Since G' has only k vertices, we 6-color it by the inductive hypothesis. Now we can 6-color G by assigning to v a color not used by any of its five or fewer neighbors. This completes the inductive step, and the theorem is proved.

42. Clearly any convex polygon can be guarded by one guard, because every vertex sees all points on or inside the polygon. This takes care of triangles and convex quadrilaterals ($n = 3$ and some of $n = 4$). It is also clear that for a nonconvex quadrilateral, a guard placed at the vertex with the reflex angle can see all points on or inside the polygon. This completes the proof that $g(3) = g(4) = 1$.

44. By Lemma 1 in Section 5.2 every hexagon has an interior diagonal, which will divide the hexagon into two polygons, each with fewer than six sides (either two quadrilaterals or one triangle and one pentagon). By Exercises 42 and 43, one guard suffices for each, so $g(6) \leq 2$. By Exercise 45, we also know that $g(6) \geq 2$. Therefore $g(6) = 2$.

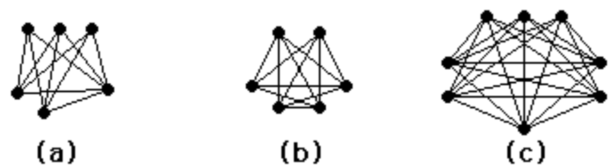
46. By Theorem 1 in Section 5.2, we can triangulate the polygon. We claim that it is possible to color the vertices of the triangulated polygon using three colors so that no two adjacent vertices have the same color. We prove this by induction. The basis step ($n = 3$) is trivial. Assume the inductive hypothesis that every triangulated polygon with k vertices can be 3-colored, and consider a triangulated polygon with $k+1$ vertices. By Exercise 23 in Section 5.2, one of the triangles in the triangulation has two sides that were sides of the original polygon. If we remove those two sides and their common vertex, the result is a triangulated polygon with k vertices. By the inductive hypothesis, we can 3-color its vertices. Now put the removed edges and vertex back. The vertex is adjacent to only two other vertices, so we can extend the coloring to it by assigning it the color not used by those vertices. This completes the proof of our claim. Now some color must be used no more than $n/3$ times; if not, then every color would be used more than $n/3$ times, and that would account for more than $3 \cdot n/3 = n$ vertices. (This argument is in the spirit of the pigeonhole principle.) Say that red is the color used least in our coloring. Then there are at most $n/3$ vertices colored red, and since this is an integer, there are at most $\lfloor n/3 \rfloor$ vertices colored red. Put guards at all these vertices. Since each triangle must have its vertices colored with three different colors, there is a guard who can see all points on or in the interior of each triangle in the triangulation. But this is all the points on or in the interior of the polygon, and our proof is complete. Combining this with Exercise 45, we have proved that $g(n) = \lfloor n/3 \rfloor$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 10

2. A graph must be nonempty, so the subgraph can have 1, 2, or 3 vertices. If it has 1 vertex, then it has no edges, so there is clearly just one possibility, K_1. If the subgraph has 2 vertices, then it can have no edges or the one edge joining these two vertices; this gives 2 subgraphs. Finally, if all three vertices are in the subgraph, then the graph can contain no edges, one edge (and we get isomorphic graphs, no matter which edge is used), two edges (ditto), or all three edges. This gives 4 different subgraphs with 3 vertices. Therefore the answer is $1+2+4=7$.

4. Each vertex in the first graph has degree 4. This statement is not true for the second graph. Therefore the graphs cannot be isomorphic. (In fact, the number of edges is different.)

6. We draw these graphs by putting the points in each part close together in clumps, and joining all vertices in different clumps.



8. **a)** The statement is true, and we can prove it using the pigeonhole principle. Suppose that the graph has n vertices. The degrees have to be numbers from 0 to $n-1$, inclusive, a total of n possibilities. Now if there is a vertex of degree $n-1$, then it is adjacent to every other vertex, and hence there can be no vertex of degree 0. Thus not all n of the possible degrees can be used. Therefore by the pigeonhole principle, some degree must occur twice.

b) The statement is false for multigraphs. As a simple example, let the multigraph have three vertices a, b, and c. Let there be one edge between a and b, and two edges between b and c. Then it is easy to see that the degrees of the vertices are 1, 3, and 2.

10. **a)** Every vertex adjacent to v has one or more edges joining it to v, so there are at least as many edges (which is what $\deg(v)$ counts) as neighbors (which is what $|N(v)|$ counts). Note that loops are not a problem here, because each loop at v contributes 2 to $\deg(v)$ and all the loops combined contribute only 1 to $|N(v)|$.

b) If G is a simple graph, then there are no loops and no parallel edges (multiple edges connecting the same pair of vertices). This means that for each v there is a one-to-one correspondence between the edges incident to v (which is what $\deg(v)$ counts) and the vertices adjacent to v (which is what $|N(v)|$ counts): Edge vw corresponds to vertex w.

12. Set up a bipartite graph model for the SDR problem. The vertices in V_1 are S_1, S_2, ..., S_n, and the vertices in V_2 are the elements of S. There is an edge between S_i and each element of S_i. An SDR is then a complete matching from V_1 to V_2. The condition $\left|\bigcup_{i\in I} S_i\right| \geq |I|$ is exactly the condition in Hall's marriage theorem.

14. Let $I=\{1,2,4,7\}$. Then $\left|\bigcup_{i\in I} S_i\right| = |\{a,b,c\}| = 3$, but $|I|=4$, violating the necessary (and sufficient) condition given in Exercise 12.

16. **a)** Since every pair of neighbors of any given vertex are adjacent, the desired probability is 1. Another way to see this, using the formula from Exercise 15, is that the number of triangles in K_7 is $C(7,3)=35$, the number of paths of length 2 in K_7 is $P(7,3)=210$, and $6\cdot 35/210=1$.

b) There are no triangles in $K_{1,8}$, so the probability is 0.

c) There are no triangles in $K_{4,4}$, so the probability is 0.

d) There are no triangles in C_7, so the probability is 0.

e) We use the result from Exercise 15, more generally computing the clustering coefficient of W_n. There are n triangles in W_n. Paths of length 2 can go around the cycle ($n \cdot 2$ of this type), can start with an edge of the cycle and then go to the center ($n \cdot 2$ of this type), start at a vertex on the cycle, go to the center, and come out along another spoke ($n \cdot (n-1)$ of this type), or start at the center ($n \cdot 2$ of this type). This gives a total of $n^2 + 5n$ paths of length 2. Therefore the clustering coefficient is $6n/(n^2+5n) = 6/(n+5)$. For $n = 7$ the numerical value is $1/2$.

f) There are no triangles in Q_4, so the probability is 0.

18. **a)** One would expect this to be rather large, since all the actors appearing together in a movie form very large complete subgraphs. One of the first studies of this phenomenon, reported in Duncan J. Watts and Steven H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature* **393** (1998) 440–442, using a somewhat different definition of clustering coefficient, found a value of 0.79. Another study (M. E. J. Newman, "The structure and function of complex networks," *SIAM Review* **45** (2003) 167–256) found the clustering coefficient of the Hollywood graph to be 0.20.

b) It reasonable to expect that the likelihood that two people who are Facebook friends of the same person are also Facebook friends is reasonably large. That is, it is reasonable to expect that this likelihood is not close to zero. In fact, one study found that it is approximately 0.16—about one out of six pairs of your Facebook friends are also Facebook friends.

c) The probability that two people who have each written a paper with a third person have written a paper with each other should not be close to zero. Two people who have written papers with the same third person may even have been co-authors with this third person on the same paper. If not, they may work on the same research problems and know each other (maybe they are at the same institution), because they have a common co-author, and also may be doing active research at the same time, all making it more likely than it would be otherwise that they have been co-authors. According to the Erdős Number Project website (`www.oakland.edu/enp`), for the entire mathematics collaboration graph, this value is 0.14. Restricting this to graph theory researchers would probably increase the value.

d) One would need some specialized knowledge of biology to have an informed opinion about this graph. Research shows that the protein interaction graph for a human cell has a large number of nodes, each representing a different protein, and the likelihood that two proteins that each interact with a third protein interact themselves is quite small. However, the clustering coefficient for the subgraph representing a particular functional module in the cell is generally larger. One paper on the Web shows values ranging from 0.01 to 0.43, depending on the data used.

e) One might expect this to be low, because routers that are linked to a common third router would not need to be linked to each other for efficient communication. According to M. E. J. Newman, *Networks, An Introduction* (Oxford University Press, 2010), the clustering coefficient of the Internet (at the autonomous system level) has been found to be about 0.01. In this book the author mentions that clustering coefficients for technology and biological networks are often small, as opposed to social networks, where these coefficients are often reasonably large. In particular, the latter are around 0.1 or larger and the former are around 0.01 or smaller.

20. Some staring at the graph convinces us that there are no K_6's. There is one K_5, namely the clique $ceghi$. There are two K_4's not contained in this K_5, which therefore are cliques: $abce$, and $cdeg$. All the K_3's not contained in any of the cliques listed so far are also cliques. We find only aef and efg. All the edges are in at least one of the cliques listed so far (and there are no isolated vertices), so we are done.

22. Since e is adjacent to every other vertex, the (unique) minimum dominating set is $\{e\}$.

24. It is easy to check that the set $\{c,e,j,l\}$ is dominating. We must show that no set with only three vertices is dominating. Suppose that there were such a set. First suppose that the vertex f is to be included. Then at least two more vertices are needed to take care of vertices a and i, unless vertex e is chosen. If vertex e is not chosen, therefore, the dominating set must have more than three vertices, since no pair of vertices covering a and i can cover d, for instance. On the other hand, if e is chosen, then since no single vertex covers c and l, again at least four vertices are required. Thus we may assume that f (and by symmetry g as well) is not in the dominating set with only three elements. This means that we need to find three vertices from the 10-cycle a,b,c,d,h,l,k,j,i,e,a that cover all ten of these vertices. This is impossible, since each vertex covers only three, and $3\cdot 3<10$. Therefore we conclude that there is no dominating set with only three vertices.

26. If G is the graph representing the $n\times n$ chessboard, then a minimum dominating set for G corresponds exactly to a set of squares on which we may place the minimum number of queens to control the board.

28. This isomorphism need not hold. For the simplest counterexample, let G_1, G_2, and H_1 each be the graph consisting of the single vertex v, and let H_2 be the graph consisting of the single vertex w. Then of course G_1 and H_1 are isomorphic, as are G_2 and H_2. But $G_1\cup G_2$ is a graph with one vertex, and $H_1\cup H_2$ is a graph with two vertices.

30. Since a 1 in the adjacency matrix indicates the presence of an edge and a 0 the absence of an edge, to obtain the adjacency matrix for $\overline{G}$ we change each 1 in the adjacency matrix for G to a 0, and we change each 0 not on the main diagonal to a 1 (we do not want to introduce loops).

32. **a)** If no degree is greater than 2, then the graph must consist either of the 5-cycle or a path with no vertices repeated. Therefore there are just two graphs.

b) Certainly every graph besides K_5 that contains K_4 as a subgraph will have chromatic number 4. There are 3 such graphs, since the vertex not in "the" K_4 can be adjacent to one, two or three of the other four vertices. A little further trial and error will convince one that there are no other graphs meeting these conditions, so the answer is 3.

c) Since every proper subgraph of K_5 is planar, there is only one such graph, namely K_5.

34. This follows from the transitivity of the "is isomorphic to" relation and Exercise 65 in Section 10.3. If G is self-converse, then G is isomorphic to G^c. Since H is isomorphic to G, H^c is also isomorphic to G^c. Stringing together these isomorphisms, we see that H is isomorphic to H^c, as desired.

36. This graph is not orientable because of the cut edge $\{c,d\}$, exactly as in Exercise 35.

38. Since we need the city to be strongly connected, we need to find an orientation of the undirected graph representing the city's streets, where the edges represent streets and the vertices represent intersections.

40. There are $C(n,2)=n(n-1)/2$ edges in a tournament. We must decide how to orient each one, and there are 2 ways to do this for each edge. Therefore the answer is $2^{n(n-1)/2}$. Note that we have not answered the question of how many nonisomorphic tournaments there are—that is much harder.

42. We proceed by induction on n, the number of vertices in the tournament. The base case is $n=2$, and the single edge is the Hamilton path. Now let G be a tournament with $n+1$ vertices. Delete one vertex, say v, and find (by the inductive hypothesis) a Hamilton path $v_1,v_2,\ldots,v_n$ in the tournament that remains. Now if (v_n,v) is an edge of G, then we have the Hamilton path $v_1,v_2,\ldots,v_n,v$; similarly if (v,v_1) is an edge of G, then we have the Hamilton path $v,v_1,v_2,\ldots,v_n$. Otherwise, there must exist a smallest i such that (v_i,v) and (v,v_{i+1}) are edges of G. We can then splice v into the previous path to obtain the Hamilton path $v_1,v_2,\ldots,v_i,v,v_{i+1},\ldots,v_n$.

44. Because $\kappa(G)$ is less than or equal to the minimum degree of the vertices, we know that the minimum degree here is at least k. This means that the sum of the degrees is at least kn, so the number of edges, by the handshaking theorem, is at least $kn/2$. Since this value must be an integer, it is at least $\lceil kn/2 \rceil$.

46. The usual notation for the minimum degree of the vertices of a graph G is $\delta(G)$.

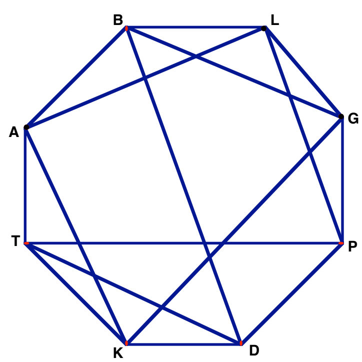
a) $\kappa(C_n) = \lambda(C_n) = \delta(C_n) = 2$

b) $\kappa(K_n) = \lambda(K_n) = \delta(K_n) = n - 1$

c) $\kappa(K_{r,r}) = \lambda(K_{r,r}) = \delta(K_{r,r}) = r$ (See Exercise 53 in Section 10.4.)

48. We follow the hint, arbitrarily pairing the vertices of odd degree and adding an extra edge joining the vertices in each pair. The resulting multigraph has all vertices of even degree, and so it has an Euler circuit. If we delete the new edges, then this circuit is split into k paths. Since no two of the added edges were adjacent, each path is nonempty. The edges and vertices in each of these paths constitute a subgraph, and these subgraphs constitute the desired collection.

50. Dirac's theorem guarantees that this friendship graph, in which each vertex has degree 4, will have a Hamilton circuit.



52. **a)** The diameter is clearly 1, since the maximum distance between two vertices is 1. The radius is also 1, with any vertex serving as the center.

b) The diameter is clearly 2, since vertices in the same part are not adjacent, but no pair of vertices are at a distance greater than 2. Similarly, the radius is 2, with any vertex serving as the center.

c) Vertices at diagonally opposite corners of the cube are a distance 3 from each other, and this is the worst case, so the diameter is 3. By symmetry we can take any vertex as the center, so it is clear that the radius is also 3.

d) Vertices at opposite corners of the hexagon are a distance 3 from each other, and this is the worst case, so the diameter is 3. By symmetry we can take any vertex as the center, so it is clear that the radius is also 3. (Despite the appearances in this exercise, it is not always the case that the radius equals the diameter; for example, $K_{1,n}$ has radius 1 and diameter 2.)

54. Suppose that we follow the given circuit through the multigraph, but instead of using edges more than once, we put in a new parallel edge whenever needed. The result is an Euler circuit through a larger multigraph. If we added new parallel edges in only $m-1$ or fewer places in this process, then we have modified at most $2(m-1)$ vertex degrees. This means that there are at least $2m - 2(m-1) = 2$ vertices of odd degree remaining, which is impossible in a multigraph with an Euler circuit. Therefore we must have added new edges in at least m places, which means the circuit must have used at least m edges more than once.

56. We assume that only simple paths are of interest here. There may be no such path, so no such algorithm is possible. If we want an algorithm that looks for such a path and either finds one or determines that none exists, we can proceed as follows. First we use Dijkstra's algorithm (or some other algorithm) to find a shortest path from a to z (the given vertices). Then for each edge e in that path (one at a time), we delete e from the graph and find a shortest path between a and z in the graph that remains, or determine that no such path exists (again using, say, Dijkstra's algorithm). The second shortest path from a to z is a path of minimum length among all the paths so found, or does not exist if no such paths are found.

58. If we want a shortest path from a to z that passes through m, then clearly we need to find a shortest path from a to m and a shortest path from m to z, and then concatenate them. Each of these paths can be found using Dijkstra's algorithm.

60. **a)** No two vertices are not adjacent, so the independence number is 1.

b) If n is even, then we can take every other vertex as our independent set, so the independence number is $n/2$. If n is odd, then this does not quite work, but clearly we can take every other vertex except for one vertex. In this case the independence number is $(n-1)/2$. We can state this answer succinctly as $\lfloor n/2 \rfloor$.

c) Since Q_n is a bipartite graph with 2^{n-1} vertices in each part, the independence number is at least 2^{n-1} (take one of the parts as the independent set). We prove that there can be no more than this many independent vertices by induction on n. It is trivial for $n=1$. Assume the inductive hypothesis, and suppose that there are more than 2^n independent vertices in Q_{n+1}. Recall that Q_{n+1} contains two copies of Q_n in it (with each pair of corresponding points joined by an edge). By the pigeonhole principle, at least one of these Q_n's must contain more than $2^n/2 = 2^{n-1}$ independent vertices. This contradicts the inductive hypothesis. Thus Q_{n+1} has only 2^n independent vertices, as desired.

d) The independence number is clearly the larger of m and n; the independent set to take is the part with this number of vertices.

62. In order to prove this statement it is sufficient to find a coloring with $n-i+1$ colors. We color the graph as follows. Let S be an independent set with i vertices. Color each vertex of S with color $n-i+1$. Color each of the other $n-i$ vertices a different color.

64. **a)** Obviously adding edges can only help in making the graph connected, so this property is monotone increasing. It is not monotone decreasing, because by removing edges one can disconnect a connected graph.

b) This is dual to part **(a)**; the property is monotone decreasing. To see this, note that removing edges from a nonconnected graph cannot possibly make it connected, while adding edges certainly can.

c) This property is neither monotone increasing nor monotone decreasing. We need to provide examples to verify this. Consider the graph C_4, a square. It has an Euler circuit. However, if we add one edge or remove one edge, then the resulting graph will no longer have an Euler circuit.

d) This property is monotone increasing (since the extra edges do not interfere with the Hamilton circuit already there) but not monotone decreasing (e.g., start with a cycle).

e) This property is monotone decreasing. If a graph can be drawn in the plane, then clearly each of its subgraphs can also be drawn in the plane (just get out your eraser!). The property is not monotone increasing; for example, adding the missing edge to the complete graph on five vertices minus an edge changes the graph from being planar to being nonplanar.

f) This property is neither monotone increasing nor monotone decreasing. It is easy to find examples in which adding edges increases the chromatic number and removing them decreases it (e.g., start with C_5).

g) As in part **(f)**, adding edges can easily decrease the radius and removing them can easily increase it, so this property is neither monotone increasing nor monotone decreasing. For example, C_7 has radius three, but adding enough edges to make K_7 reduces the radius to 1, and removing enough edges to disconnect the graph renders the radius infinite.

h) As in part **(g)**, this is neither monotone increasing nor monotone decreasing.

66. Suppose that G is a graph on n vertices randomly generated using edge probability p, and G' is a graph on n vertices randomly generated using edge probability p', where $p < p'$. Recall that this means that for G we go through all pairs of vertices and independently put an edge between them with probability p; and similarly for G'. We must show that G is no more likely to have property P than G' is. To see this, we will imagine a different way of forming G. First we generate a random graph G' using edge probability p'; then we go through the edges that are present, and independently erase each of them with probability $1 - (p/p')$. Clearly, for an edge to end up in G, it must first get generated and then not get erased, which has probability $p' \cdot (p/p') = p$; therefore this is a valid way to generate G. Now whenever G has property P, then so does G', since P is monotone increasing. Thus the probability that G has property P is no greater than the probability that G' does; in fact it will usually be less, since once a G' having property P is generated, it is possible that it will lose the property as edges are erased.

CHAPTER 11
Trees

SECTION 11.1 Introduction to Trees

2. **a)** This is a tree since it is connected and has no simple circuits.
b) This is a tree since it is connected and has no simple circuits.
c) This is not a tree, since it is not connected.
d) This is a tree since it is connected and has no simple circuits.
e) This is not a tree, since it has a simple circuit.
f) This is a tree since it is connected and has no simple circuits.

4. **a)** Vertex a is the root, since it is drawn at the top.
b) The internal vertices are the vertices with children, namely a, b, d, e, g, h, i, and o.
c) The leaves are the vertices without children, namely c, f, j, k, l, m, n, p, q, r, and s.
d) The children of j are the vertices adjacent to j and below j. There are no such vertices, so there are no children.
e) The parent of h is the vertex adjacent to h and above h, namely d.
f) Vertex o has only one sibling, namely p, which is the other child of o's parent, i.
g) The ancestors of m are all the vertices on the unique simple path from m back to the root, namely g, b, and a.
h) The descendants of b are all the vertices that have b as an ancestor, namely e, f, g, j, k, l, and m.

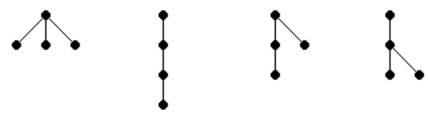
6. This is not a full m-ary tree for any m. It is an m-ary tree for all $m \geq 3$, since each vertex has at most 3 children, but since some vertices have 3 children, while others have 1 or 2, it is not full for any m.

8. We can easily determine the levels from the drawing. The root a is at level 0. The vertices in the row below a are at level 1, namely b, c, and d. The vertices below that, namely e through i (in alphabetical order), are at level 2. Similarly j through p are at level 3, and q, r, and s are at level 4.

10. We describe the answers, rather than actually drawing pictures.
a) The subtree rooted at a is the entire tree, since a is the root.
b) The subtree rooted at c consists of just the vertex c.
c) The subtree rooted at e consists of e, j, and k, and the edges ej and ek.

12. We find the answer by carefully enumerating these trees, i.e., drawing a full set of nonisomorphic trees. One way to organize this work so as to avoid leaving any trees out or counting the same tree (up to isomorphism) more than once is to list the trees by the length of their longest simple path (or longest simple path from the root in the case of rooted trees).
a) There are two trees with four vertices, namely $K_{1,3}$ and the simple path of length 3. See the first two trees below.

b) The longest path from the root can have length 1, 2 or 3. There is only one tree with longest path of length 1 (the other three vertices are at level 1), and only one with longest path of length 3. If the longest path has length 2, then the fourth vertex (after using three vertices to draw this path) can be "attached" to either the root or the vertex at level 1, giving us two nonisomorphic trees. Thus there are a total of four nonisomorphic rooted trees on 4 vertices, as shown below.



14. There are two things to prove. First suppose that T is a tree. By definition it is connected, so we need to show that the deletion of any of its edges produces a graph that is not connected. Let $\{x,y\}$ be an edge of T, and note that $x \neq y$. Now T with $\{x,y\}$ deleted has no path from x to y, since there was only one simple path from x to y in T, and the edge itself was it. (We use Theorem 1 here, as well as the fact that if there is a path from a vertex u to another vertex v, then there is a simple path from u to v by Theorem 1 in Section 10.4.) Therefore the graph with $\{x,y\}$ deleted is not connected.

Conversely, suppose that a simple connected graph T satisfies the condition that the removal of any edge will disconnect it. We must show that T is a tree. If not, then T has a simple circuit, say $x_1, x_2, \ldots, x_r, x_1$. If we delete edge $\{x_r, x_1\}$ from T, then the graph will remain connected, since wherever the deleted edge was used in forming paths between vertices we can instead use the rest of the circuit: $x_1, x_2, \ldots, x_r$ or its reverse, depending on which direction we need to go. This is a contradiction to the condition. Therefore our assumption was wrong, and T is a tree.

16. If both m and n are at least 2, then clearly there is a simple circuit of length 4 in $K_{m,n}$. On the other hand, $K_{m,1}$ is clearly a tree (as is $K_{1,n}$). Thus we conclude that $K_{m,n}$ is a tree if and only if $m = 1$ or $n = 1$.

18. By Theorem 4(ii), the answer is $mi + 1 = 5 \cdot 100 + 1 = 501$.

20. By Theorem 4(i), the answer is $[(m-1)n+1]/m = (2 \cdot 100 + 1)/3 = 67$.

22. The model here is a full 5-ary tree. We are told that there are 10,000 internal vertices (these represent the people who send out the letter). By Theorem 4(ii) we see that $n = mi + 1 = 5 \cdot 10000 + 1 = 50{,}001$. Everyone but the root receives the letter, so we conclude that 50,000 people receive the letter. There are $50001 - 10000 = 40{,}001$ leaves in the tree, so that is the number of people who receive the letter but do not send it out.

24. Such a tree does exist. By Theorem 4(iii), we note that such a tree must have $i = 75/(m-1)$ internal vertices. This has to be a whole number, so $m-1$ must divide 75. This is possible, for example, if $m = 6$, so let us try it. A complete 6-ary tree (see preamble to Exercise 27) of height 2 would have 36 leaves. We therefore need to add 40 leaves. This can be accomplished by changing 8 vertices at level 2 to internal vertices; each such change adds 5 leaves to the tree (6 new leaves at level 3, less the one leaf at level 5 that has been changed to an internal vertex). We will not show a picture of this tree, but just summarize its appearance. The root has 6 children, each of which has 6 children, giving 36 vertices at level 2. Of these, 28 are leaves, and each of the remaining 8 vertices at level 2 has 6 children, living at level 3, for a total of 48 leaves at level 3. The total number of leaves is therefore $28 + 48 = 76$, as desired.

26. By Theorem 4(iii), we note that such a tree must have $i = 80/(m-1)$ internal vertices. This has to be a whole number, so $m-1$ must divide 80. By enumerating the divisors of 80, we see that m can equal 2, 3, 5, 6, 9, 11, 17, 21, 41, or 81. Some of these are incompatible with the height requirements, however.

a) Since the height is 4, we cannot have $m = 2$, since that will give us at most $1+2+4+8+16 = 31$ vertices. Any of the larger values of m shown above, up to 21, allows us to form a tree with 81 leaves and height 4. In each case we could get m^4 leaves if we made all vertices at levels smaller than 4 internal; and we can get as few as $4(m-1)+1$ leaves by putting only one internal vertex at each such level. We can get 81 leaves in the former case by taking $m = 3$; on the other hand, if $m > 21$, then we would be forced to have more than 81 leaves. Therefore the bounds on m are $3 \le m \le 21$ (with m also restricted to being in the list above).

b) If T must be balanced, then the smallest possible number of leaves is obtained when level 3 has only one internal vertex and $m^3 - 1$ leaves, giving a total of $m^3 - 1 + m$ leaves in T. Again, the maximum number of leaves will be m^4. With these restriction, we see that $m = 5$ is already too big, since this would require at least $5^3 - 1 + 5 = 129$ leaves. Therefore the only possibility is $m = 3$.

28. This tree has 1 vertex at level 0, m vertices at level 1, m^2 vertices at level 2, ..., m^h vertices at level h. Therefore it has

$$1 + m + m^2 + \cdots + m^h = \frac{m^{h+1} - 1}{m - 1}$$

vertices in all. The vertices at level h are the only leaves, so it has m^h leaves.

30. (We assume $m \ge 2$.) First we delete all the vertices at level h; there is at least one such vertex, and they are all leaves. The result must be a complete m-ary tree of height $h-1$. By the result of Exercise 28, this tree has m^{h-1} leaves. In the original tree, then, there are more than this many leaves, since every internal vertex at level $h-1$ (which counts as a leaf in our reduced tree) spawns at least two leaves at level h.

32. The root of the tree represents the entire book. The vertices at level 1 represent the chapters—each chapter is a chapter of (read "child of") the book. The vertices at level 2 represent the sections (the parent of each such vertex is the chapter in which the section resides). Similarly the vertices at level 3 are the subsections.

34. **a)** The parent of a vertex is that vertex's boss.

b) The child of a vertex is an immediate subordinate of that vertex (one he or she directly supervises).

c) The sibling of a vertex is a coworker with the same boss.

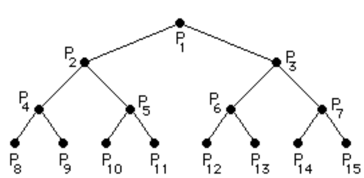
d) The ancestors of a vertex are that vertex's boss, his/her boss's boss, etc.

e) The descendants of a vertex are all the people that that vertex ultimately supervises (directly or indirectly).

f) The level of a vertex is the number of levels away from the top of the organization that vertex is.

g) The height of the tree is the depth of the structure.

36. **a)** We simply add one more row to the tree in Figure 12, obtaining the following tree.



b) During the first step we use the bottom row of the network to add $x_1 + x_2$, $x_3 + x_4$, $x_5 + x_6$, ..., $x_{15} + x_{16}$. During the second step we use the next row up to add the results of the computations from the first step, namely $(x_1 + x_2) + (x_3 + x_4)$, $(x_5 + x_6) + (x_7 + x_8)$, ..., $(x_{13} + x_{14}) + (x_{15} + x_{16})$. The third step uses the sums obtained in the second, and the two processors in the second row of the tree perform $(x_1 + x_2 + x_3 + x_4) + (x_5 + x_6 + x_7 + x_8)$ and $(x_9 + x_{10} + x_{11} + x_{12}) + (x_{13} + x_{14} + x_{15} + x_{16})$. Finally, during the fourth step the root processor adds these two quantities to obtain the desired sum.

38. For $n = 3$, there is only one tree to consider, the one that is a simple path of length 2. There are 3 choices for the label to put in the middle of the path, and once that choice is made, the labeled tree is determined up to isomorphism. Therefore there are 3 labeled trees with 3 vertices.

For $n = 4$, there are two structures the tree might have. If it is a simple path with length 3, then there are 12 different labelings; this follows from the fact that there are $P(4,4) = 4! = 24$ permutations of the integers from 1 to 4, but a permutation and its reverse lead to the same labeled tree. If the tree structure is $K_{1,3}$, then the only choice is which label to put on the vertex that is adjacent to the other three, so there are 4 such trees. Thus in all there are 16 labeled trees with 4 vertices.

In fact it is a theorem that the number of labeled trees with n vertices is n^{n-2} for all $n \geq 2$.

40. The eccentricity of vertex e is 3, and it is the only vertex with eccentricity this small. Therefore e is the only center.

42. Since the height of a tree is the maximum distance from the root to another vertex, this is clear from the definition of center.

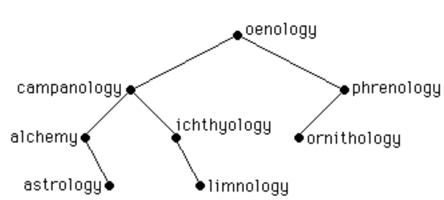
44. We choose a root and color it red. Then we color all the vertices at odd levels blue and all the vertices at even levels red.

46. The number of vertices in the tree T_n satisfies the recurrence relation $v_n = v_{n-1} + v_{n-2} + 1$ (the "+1" is for the root), with $v_1 = v_2 = 1$. Thus the sequence begins $1,\ 1,\ 3,\ 5,\ 9,\ 15,\ 25,\ \ldots$. It is easy to prove by induction that $v_n = 2f_n - 1$, where f_n is the n^{th} Fibonacci number. The number of leaves satisfies the recurrence relation $l_n = l_{n-1} + l_{n-2}$, with $l_1 = l_2 = 1$, so $l_n = f_n$. Since $i_n = v_n - l_n$, we have $i_n = f_n - 1$. Finally, it is clear that the height of the tree T_n is one more than the height of the tree T_{n-1} for $n \geq 3$, with the height of T_2 being 0. Therefore the height of T_n is $n - 2$ for all $n \geq 2$ (and of course the height of T_1 is 0).

48. Let T be a tree with n vertices, having height h. If there are any internal vertices in T at levels less than $h - 1$ that do not have two children, take a leaf at level h and move it to be such a missing child. This only lowers the average depth of a leaf in this tree, and since we are trying to prove a lower bound on the average depth, it suffices to prove the bound for the resulting tree. Repeat this process until there are no more internal vertices of this type. As a result, all the leaves are now at levels $h - 1$ and h. Now delete all vertices at level h. This changes the number of vertices by at most (one more than) a factor of two and so has no effect on a big-Omega estimate (it changes $\log n$ by at most 1). Now the tree is complete, and by Exercise 28 it has 2^{h-1} leaves, all at depth $h - 1$, where now $n = 2^h - 1$. The desired estimate follows.

SECTION 11.2 Applications of Trees

2. We make the first word the root. Since the second word follows the first in alphabetical order, we make it the right child of the root. Similarly the third word is the left child of the root. To place the next word, *ornithology*, we move right from the root, since it follows the root in alphabetical order, and then move left from *phrenology*, since it comes before that word. The rest of the tree is built in a similar manner.



4. To find *palmistry*, which is not in the tree, we must compare it to the root (*oenology*), then the right child of the root (*phrenology*), and then the left child of that vertex (*ornithology*). At this point it is known that the word is not in the tree, since *ornithology* has no right child. Three comparisons were used. The remaining parts are similar, and the answer is 3 in each case.

6. Decision tree theory tells us that at least $\lceil \log_3 4 \rceil = 2$ weighings are needed. In fact we can easily achieve this result. We first compare the first two coins. If one is lighter, it is the counterfeit. If they balance, then we compare the other two coins, and the lighter one of these is the counterfeit.

8. Decision tree theory applied naively says that at least $\lceil \log_3 8 \rceil = 2$ weighings are needed, but in fact at least 3 weighings are needed. To see this, consider what the first weighing might accomplish. We can put one, two, or three coins in each pan for the first weighing (no other arrangement will yield any information at all). If we put one or two coins in each pan, and if the scale balances, then we only know that the counterfeit is among the six or four remaining coins. If we put three coins in each pan, and if the scale does not balance, then essentially all we know is that the counterfeit coin is among the six coins involved in the weighing. In every case we have narrowed the search to more than three coins, so one more weighing cannot find the counterfeit (there being only three possible outcomes of one more weighing).

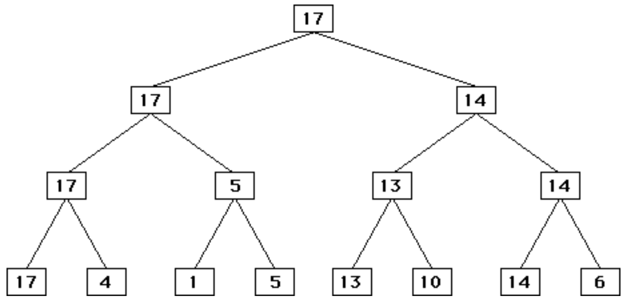
Next we must show how to solve the problem with three weighings. Put two coins in each pan. If the scale balances, then the search is reduced to the other four coins. If the scale does not balance, then the counterfeit is among the four coins on the scale. In either case, we then apply the solution to Exercise 7 to find the counterfeit with two more weighings.

10. There are nine possible outcomes here: either there is no counterfeit, or else we need to name a coin (4 choices) and a type (lighter or heavier). Decision tree theory holds out hope that perhaps only two weighings are needed, but we claim that we cannot get by with only two. Suppose the first weighing involves two coins per pan. If the pans balance, then we know that there is no counterfeit, and subsequent weighings add no information. Therefore we have only six possible decisions (three for each of the other two outcomes of the first weighing) to differentiate among the other eight possible outcomes, and this is impossible. Therefore assume without loss of generality that the first weighing pits coin A against coin B. If the scale balances, then we know that the counterfeit is among the other two coins, if there is one. Now we must separate coins C and D on the next weighing if this weighing is to be decisive, so this weighing is equivalent to pitting C against D. If the scale does not balance, then we have not solved the problem.

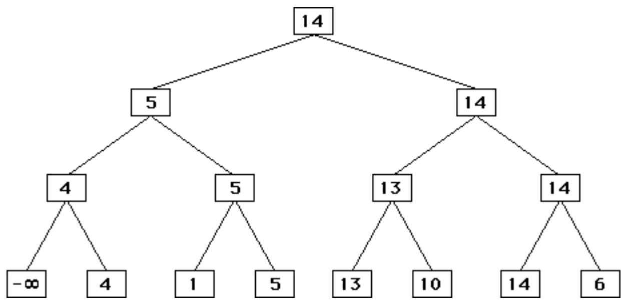
We give a solution using three weighings. Weigh coin A against coin B. If they do not balance, then without loss of generality assume that coin A is lighter (the opposite result is handled similarly). Then weigh coin A against coin C. If they balance, then we know that coin B is the counterfeit and is heavy. If they do not balance, then we know that A is the counterfeit and is light. The remaining case is that in which coins A and B balance. At this point we compare C and D. If they balance, then we conclude that there is no counterfeit. If they do not balance, then one more weighing of, say, the lighter of these against A, solves the problem just as in the case in which A and B did not balance.

12. By Theorem 1 in this section, at least $\lceil \log 5! \rceil$ comparisons are needed. Since $\log_2 120 \approx 6.9$, at least seven comparisons are required. We can accomplish the sorting with seven comparisons as follows. Call the elements a, b, c, d, and e. First compare a and b; and compare c and d. Without loss of generality, let us assume that $a < b$ and $c < d$. (If not, then relabel the elements after these comparisons.) Next we compare b and d (this is our third comparison), and again relabel all four of these elements if necessary to have $b < d$. So at this point we have $a < b < d$ and $c < d$ after three comparisons. We insert e into its proper position among a, b, and d with two more comparisons using binary search, i.e., by comparing e first to b and then to either a or d. Thus we have made five comparisons and obtained a linear ordering among a, b, d, and e, as well as knowing one more piece of information about the location of c, namely either that it is less than the largest among a, b, d, and e, or that it is less than the second largest. (Drawing a diagram helps here.) In any case, it then suffices to insert c into its correct position among the three smallest members of a, b, d, and e, which requires two more comparisons (binary search), bringing the total to the desired seven.

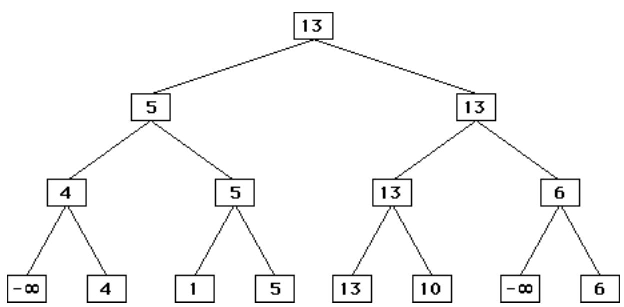
14. The first step builds the following tree.



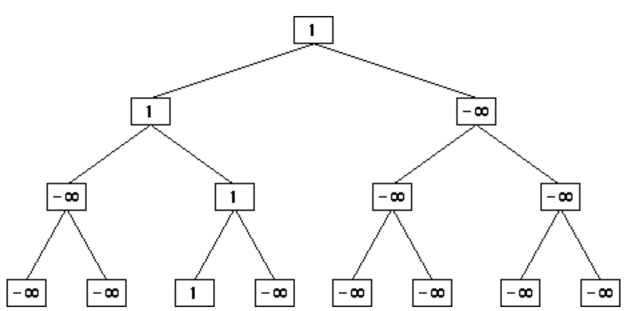
This identifies 17 as the largest element, so we replace the leaf 17 by $-\infty$ in the tree and recalculate the winner in the path from the leaf where 17 used to be up to the root. The result is as shown here.



Now we see that 14 is the second largest element, so we repeat the process: replace the leaf 14 by $-\infty$ and recalculate. This gives us the following tree.



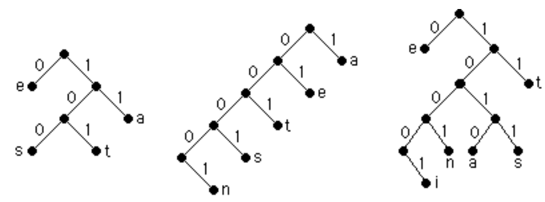
Thus we see that 13 is the third largest element, so we repeat the process: replace the leaf 13 by $-\infty$ and recalculate. The process continues in this manner. The final tree will look like this, as we determine that 1 is the eighth largest element.



16. Each comparison eliminates one contender, and $n-1$ contenders have to be eliminated, so there are $n-1$ comparisons to determine the largest element.

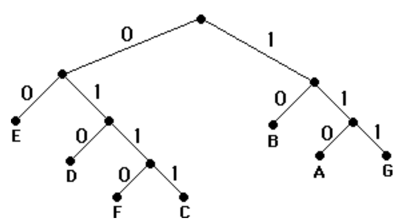
18. Following the hint we insert enough $-\infty$ values to make n a power of 2. This at most doubles n and so will not affect our final answer in big-Theta notation. By Exercise 16 we can build the initial tree using $n-1$ comparisons. By Exercise 17 for each round after the first it takes $k = \log n$ comparisons to identify the next largest element. There are $n-1$ additional rounds, so the total amount of work in these rounds is $(n-1)\log n$. Thus the total number of comparisons is $n-1+(n-1)\log n$, which is $\Theta(n \log n)$.

20. The constructions are straightforward.



22. **a)** The first three bits decode as t. The next bit decodes as e. The next four bits decode as s. The last three bits decode as t. Thus the word is *test*. The remaining parts are similar, so we give just the answers.
b) *beer* **c)** *sex* **d)** *tax*

24. We follow Algorithm 2. Since F and C are the symbols of least weight, they are combined into a subtree, which we will call T_1 for discussion purposes, of weight $0.07+0.05=0.12$, with the larger weight symbol, F, on the left. Now the two trees of smallest weight are the single symbols A and G, and so we get a tree T_2 with left subtree A and right subtree G, of weight 0.18. The next step is to combine D and T_1 into a subtree T_3 of weight 0.27. Then B and T_2 form T_4 of weight 0.43; and E and T_3 form T_5 of weight 0.57.The final step is to combine T_5 and T_4. The result is as shown.



We see by looking at the tree that A is encoded by 110, B by 10, C by 0111, D by 010, E by 00, F by 0110, and G by 111. To compute the average number of bits required to encode a character, we multiply the number of bits for each letter by the weight of that latter and add. Since A takes 3 bits and has weight 0.10, it contributes 0.30 to the sum. Similarly B contributes $2 \cdot 0.25 = 0.50$. In all we get $3 \cdot 0.10 + 2 \cdot 0.25 + 4 \cdot 0.05 + 3 \cdot 0.15 + 2 \cdot 0.30 + 4 \cdot 0.07 + 3 \cdot 0.08 = 2.57$. Thus on the average, 2.57 bits are needed per character. Note that this is an appropriately weighted average, weighted by the frequencies with which the letters occur.

26. **a)** First we combine e and d into a tree T_1 with weight 0.2. Then using the rule we choose T_1 and, say, c to combine into a tree T_2 with weight 0.4. Then again using the rule we must combine T_2 and b into T_3 with weight 0.6, and finally T_3 and a. This gives codes a:1, b:01, c:001, d:0001, e:0000. For the other method we first combine d and e to form a tree T_1 with weight 0.2. Next we combine b and c (the trees with the smallest number of vertices) into a tree T_2 with weight 0.4. Next we are forced to combine a with T_1 to form T_3 with weight 0.6, and then T_3 and T_2. This gives the codes a:00, b:10, c:11, d:010, e:011.

b) The average for the first method is $1\cdot 0.4+2\cdot 0.2+3\cdot 0.2+4\cdot 0.1+4\cdot 0.1=2.2$, and the average for the second method is $2\cdot 0.4+2\cdot 0.2+2\cdot 0.2+3\cdot 0.1+3\cdot 0.1=2.2$. We knew ahead of time, of course, that these would turn out to be equal, since the Huffman algorithm minimizes the expected number of bits. For variance we use the formula $V(X)=E(X^2)-E(X)^2$. For the first method, the expectation of the square of the number of bits is $1^2\cdot 0.4+2^2\cdot 0.2+3^2\cdot 0.2+4^2\cdot 0.1+4^2\cdot 0.1=6.2$, and for the second method it is $2^2\cdot 0.4+2^2\cdot 0.2+2^2\cdot 0.2+3^2\cdot 0.1+3^2\cdot 0.1=5.0$. Therefore the variance for the first method is $6.2-2.2^2=1.36$, and for the second method it is $5.0-2.2^2=0.16$. The second method has a smaller variance in this example.

28. The pseudocode is identical to Algorithm 2 with the following changes. First, the value of m needs to be specified, presumably as part of the input. Before the **while** loop starts, we choose the $k=((N-1)\ \mathbf{mod}\ (m-1))+1$ vertices with smallest weights and replace them by a single tree with a new root, whose children from left to right are these k vertices in order by weight (from greatest to smallest), with labels 0 through $k-1$ on the edges to these children, and with weight the sum of the weights of these k vertices. Within the loop, rather than replacing the two trees of smallest weight, we find the m trees of smallest weight, delete them from the forest and form a new tree with a new root, whose children from left to right are the roots of these m trees in order by weight (from greatest to smallest), with labels 0 through $m-1$ on the edges to these children, and with weight the sum of the weights of these m former trees.

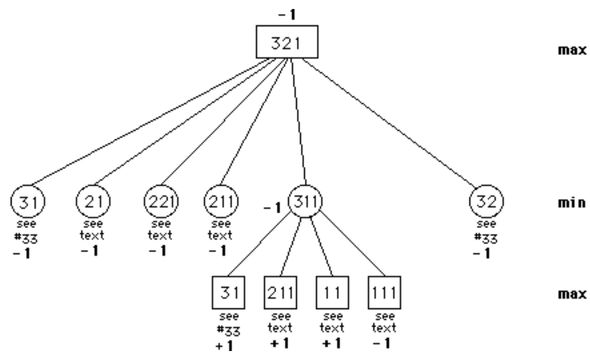
30. **a)** It is easy to construct this tree using the Huffman coding algorithm, as in previous exercises. We get A:0, B:10, C:11.

b) The frequencies of the new symbols are AA:0.6400, AB:0.1520, AC:0.0080, BA:0.1520, BB:0.0361, BC:0.0019, CA:0.0080, CB:0.0019, CC:0.0001. We form the tree by the algorithm and obtain this code: AA:0, AB:11, AC:10111, BA:100, BB:1010, BC:1011011, CA:101100, CB:10110100, CC:10110101.

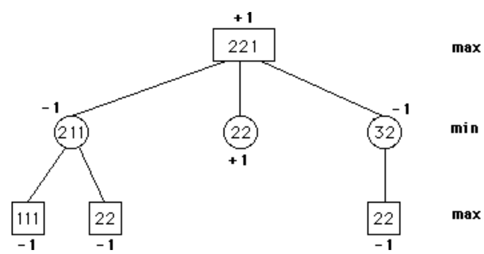
c) The average number of bits for part **(a)** is $1\cdot 0.80+2\cdot 0.19+2\cdot 0.01=1.2000$ per symbol. The average number of bits for part **(b)** is $1\cdot 0.6400+2\cdot 0.1520+5\cdot 0.0080+3\cdot 0.1520+4\cdot 0.0361+7\cdot 0.0019+6\cdot 0.0080+8\cdot 0.0019+8\cdot 0.0001=1.6617$ for sending two symbols, which is therefore 0.83085 bits per symbol. The second method is more efficient.

32. We prove this by induction on the number of symbols. If there are just two symbols, then there is nothing to prove, so assume the inductive hypothesis that Huffman codes are optimal for k symbols, and consider a situation in which there are $k+1$ symbols. First note that since the tree is full, the leaves at the bottom-most level come in pairs. Let a and b be two symbols of smallest frequencies, p_a and p_b. If in some binary prefix code they are not paired together at the bottom-most level, then we can obtain a code that is at least as efficient by interchanging the symbols on some of the leaves to make a and b siblings at the bottom-most level (since moving a more frequently occurring symbol closer to the root can only help). Therefore we can assume that a and b are siblings in every most-efficient tree. Now suppose we consider them to be one new symbol c, occurring with frequency equal to the sum of the frequencies of a and b, and apply the inductive hypothesis to obtain via the Huffman algorithm an optimal binary prefix code H_k on k symbols. Note that this is equivalent to applying the Huffman algorithm to the $k+1$ symbols, and obtaining a code we will call H_{k+1}. We must show that H_{k+1} is optimal for the $k+1$ symbols. Note that the average numbers of bits required to encode a symbol in H_k and in H_{k+1} are the same except for the symbols a, b, and c, and the difference is p_a+p_b (since one extra bit is needed for a and b, as opposed to c, and all other code words are the same). If H_{k+1} is not optimal, let H'_{k+1} be a better code (with smaller average number of bits per symbol). By the observation above we can assume that a and b are siblings at the bottom-most level in H'_{k+1}. Then the code H'_k for k symbols obtained by replacing a and b with their parent (and deleting the last bit) has average number of bits equal to the average for H'_{k+1} minus $p_a + p_b$, and that contradicts the inductive hypothesis that H_k was optimal.

34. The first player has six choices, as shown below. In five of these cases, the analysis from there on down has already been done, either in Figure 9 of the text or in the solution to Exercise 33, so we do not show the subtree in full but only indicate the value. Note that if the cited reference was to a square vertex rather than a circle vertex, then the outcome is reversed. From the fifth vertex at the second level there are four choices, as shown, and again they have all been analyzed previously. The upshot is that since all the vertices on the second level are wins for the second player (value -1), the value of the root is also -1, and the second player can always win this game.



36. The game tree is too large to draw in its entirety, so we simplify the analysis by noting that a player will never want to move to a situation with two piles, one of which has one stone, nor to a single pile with more than one stone. If we omit these suicide moves, the game tree looks like this.



Note that a vertex with no children except suicide moves is a win for whoever is not moving at that point. The first player wins this game by moving to the position 22.

38. **a)** First player wins by moving in the center at this point.This blocks second player's threat and creates two threats, only one of which can the second player block.

b) This game will end in a draw with optimal play. The first player must first block the second player's threat, and then as long as the second player makes his third and fourth moves in the first and third columns, the first player cannot win.

c) The first player can win by moving in the right-most square of the middle row. This creates two threats, only one of which can the second player block.

d) As long as neither player does anything stupid (fail to block a threat), this game must end in a draw, since the next three moves are forced and then no file can contain three of the same symbol.

40. If the smaller pile contains just one stone, then the first player wins by removing all the stones in the other pile. Otherwise the smaller pile contains at least two stones and the larger pile contains more stones than that, so the first player can remove enough stones from the larger pile to make two piles with the same number of stones, where this number is at least 2. By the result of Exercise 39, the resulting game is a win for the second player when played optimally, and our first player is now the second player in the resulting game.

42. We need to record how many moves are possible from various positions. If the game currently has piles with stones in them, we can take from one to all of the stones in any pile. That means the number of possible moves is the sum of the pile sizes. However, by symmetry, moves from piles of the same size are equivalent, so the actual number of moves is the sum of the distinct pile sizes. The one exception is that a position with just one pile has one fewer move, since we cannot take all the stones.

a) From 54 the possible moves are to 53, 52, 51, 44, 43, 42, 41, 5, and 4, so there are nine children. A similar analysis shows that the number of children of these children are 8, 7, 6, 4, 7, 6, 5, 4, and 3, respectively, so the number of grandchildren is the sum of these nine numbers, namely 50.

b) There are three children with just two piles left, and these lead to 18 grandchildren. There are six children with three piles left, and these lead to 37 grandchildren. So in all there are nine children and 55 grandchildren.

c) A similar analysis shows that there are 10 children and 70 grandchildren.

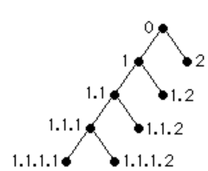
d) A similar analysis shows that there are 10 children and 82 grandchildren.

44. This recursive procedure finds the value of a game. It needs to keep track of which player is currently moving, so the value of the variable *player* will be either "First" or "Second." The variable P is a position of the game (for example, the numbers of stones in the piles for nim).

procedure $\mathit{value}(P, \mathit{player})$
if P is a leaf **then return** payoff to first player
else if $\mathit{player} = \text{First}$ **then**
  {compute maximum of values of children}
  $v := -\infty$
  for each legal move m for First
    {compute value of game at resulting position}
    $Q :=$ (P followed by move m)
    $v' := \mathit{value}(Q, \text{Second})$
    if $v' > v$ **then** $v := v'$
  return v
else { $\mathit{player} = \text{Second}$ }
  {compute minimum of values of children}
  $v := \infty$
  for each legal move m for Second
    {compute value of game at resulting position}
    $Q :=$ (P followed by move m)
    $v' := \mathit{value}(Q, \text{First})$
    if $v' < v$ **then** $v := v'$
  return v

SECTION 11.3 Tree Traversal

2. See the comments for the solution to Exercise 1. The order is $0 < 1 < 1.1 < 1.1.1 < 1.1.1.1 < 1.1.1.2 < 1.1.2 < 1.2 < 2$.



4. **a)** The vertex is at level 5; it is clear that an address (other than 0) of length l gives a vertex at level l.

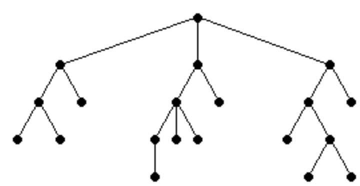
b) We obtain the address of the parent by deleting the last number in the address of the vertex. Therefore the parent is 3.4.5.2.

c) Since v is the fourth child, it has at least three siblings.

d) We know that v's parent must have at least 1 sibling, its grandparent must have at least 4, its great-grandparent at least 3, and its great-great-grandparent at least 2. Adding to this count the fact that v has 5 ancestors and 3 siblings (and not forgetting to count v itself), we obtain a total of 19 vertices in the tree.

e) The other addresses are 0 together with all prefixes of v and the all the addresses that can be obtained from v or prefixes of v by making the last number smaller. Thus we have 0, 1, 2, 3, 3.1, 3.2, 3.3, 3.4, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.5.1, 3.4.5.2, 3.4.5.2.1, 3.4.5.2.2, and 3.4.5.2.3.

6. **a)** The following tree has these addresses for its leaves. We construct it by starting from the beginning of the list and drawing the parts of the tree that are made necessary by the given leaves. First of course there must be a root. Then since the first leaf is labeled 1.1.1, there must be a first child of the root, a first child of this child, and a first child of this latter child, which is then a leaf. Next there must be the second child of the root's first grandchild (1.1.2), and then a second child of the first child of the root (1.2). We continue in this manner until the entire tree is drawn.



b) If there is such a tree, then the address 2.4.1 must occur since the address 2.4.2 does (the parent of 2.4.2.1). The vertex with that address must either be a leaf or have a descendant that is a leaf. The address of any such leaf must begin 2.4.1. Since no such address is in the list, we conclude that the answer to the question is no.

c) No such tree is possible, since the vertex with address 1.2.2 is not a leaf (it has a child 1.2.2.1 in the list).

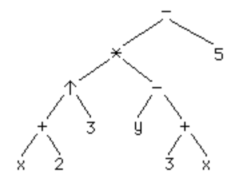
8. See the comments in the solution to Exercise 7 for the procedure. The only difference here is that some vertices have more than two children: after listing such a vertex, we list the vertices of its subtrees, in preorder, from left to right. The answer is $a, b, d, e, i, j, m, n, o, c, f, g, h, k, l, p$.

10. The left subtree of the root comes first, namely the tree rooted at b. There again the left subtree comes first, so the list begins with d. After that comes b, the root of this subtree, and then the right subtree of b, namely (in order) f, e, and g. Then comes the root of the entire tree and finally its right child. Thus the answer is d, b, f, e, g, a, c.

12. This is similar to Exercise 11. The answer is $k, e, l, m, b, f, r, n, s, g, a, c, o, h, d, i, p, j, q$.

14. The procedure is the same as in Exercise 13, except that some vertices have more than two children here: before listing such a vertex, we list the vertices of its subtrees, in postorder, from left to right. The answer is $d, i, m, n, o, j, e, b, f, g, k, p, l, h, c, a$.

16. **a)** We build the tree from the top down while analyzing the expression by identifying the outermost operation at each stage. The outermost operation in this expression is the final subtraction. Therefore the tree has $-$ at its root, with the two operands as the subtrees at the root. The right operand is clearly 5, so the right child of the root is 5. The left operand is the result of a multiplication, so the left subtree has $*$ as its root. We continue recursively in this way until the entire tree is constructed.

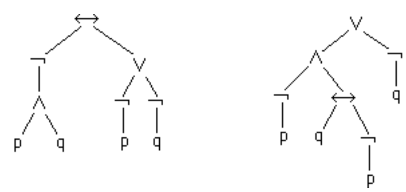


b) We can read off the answer from the picture we have just drawn simply by listing the vertices of the tree in preorder: First list the root, then the left subtree in preorder, then the right subtree in preorder. Therefore the answer is $- * \uparrow + x\,2\,3 - y + 3\,x\,5$.

c) We can read off the answer from the picture we have just drawn simply by listing the vertices of the tree in postorder: $x\,2 + 3 \uparrow y\,3\,x + - * 5\,-$.

d) The infix expression is just the given expression, fully parenthesized: $((((x+2)\uparrow 3) * (y-(3+x))) - 5)$. This corresponds to traversing the tree in inorder, putting in a left parenthesis whenever we go down to a left child and putting in a right parenthesis whenever we come up from a right child.

18. **a)** This exercise is similar to the previous few exercises. The only difference is that some portions of the tree represent the unary operation of negation ($\neg$). In the first tree, for example, the left subtree represents the expression $\neg(p \wedge q)$, so the root is the negation symbol, and the only child of this root is the tree for the expression $p \wedge q$.



Since this exercise is similar to previous exercises, we will not go into the details of obtaining the different expressions. The only difference is that negation ($\neg$) is a unary operator; we show it preceding its operand in infix notation, even though it would follow it in an inorder traversal of the expression tree.

b) $\leftrightarrow \neg \wedge p\,q \vee \neg p \neg q$ and $\vee \wedge \neg p \leftrightarrow q \neg p \neg q$

c) $p\,q \wedge \neg p \neg q \neg \vee \leftrightarrow$ and $p \neg q\,p \neg \leftrightarrow \wedge q \neg \vee$

d) $((\neg(p \wedge q)) \leftrightarrow ((\neg p) \vee (\neg q)))$ and $(((\neg p) \wedge (q \leftrightarrow (\neg p))) \vee (\neg q))$

20. This requires fairly careful counting. Let us work from the outside in. There are four symbols that can be the outermost operation: the first $\neg$, the $\wedge$, the $\leftrightarrow$, and the $\vee$. Let us first consider the cases in which the first $\neg$ is the outermost operation, necessarily applied, then, to the rest of the expression. Then there are three possible choices for the outermost operation of the rest: the $\wedge$, the $\leftrightarrow$, and the $\vee$. Let us assume first that it is the $\wedge$. Then there are two choices for the outermost operation of the rest of the expression: the $\leftrightarrow$ and the $\vee$. If it is the $\leftrightarrow$, then there are two ways to parenthesize the rest—depending on whether the second $\neg$ applies to the disjunction or only to the p. Backing up, we next consider the case in which the $\vee$ is outermost operation among the last seven symbols, rather than the $\leftrightarrow$. In this case there are no further choices. We then back up again and assume that the $\leftrightarrow$, rather than the $\wedge$, is the second outermost operation. In this case there are two possibilities for completing the parenthesization (involving the second $\neg$). If the $\vee$ is the second outermost operation, then again there are two possibilities, depending on whether the $\wedge$ or the $\leftrightarrow$ is applied first. Thus in the case in which the outermost operation is the first $\neg$, we have counted 7 ways to parenthesize the expression:

$$(\neg(p \wedge (q \leftrightarrow (\neg(p \vee (\neg q))))))$$

$$(\neg(p \wedge (q \leftrightarrow ((\neg p) \vee (\neg q)))))$$

$$(\neg(p \wedge ((q \leftrightarrow (\neg p)) \vee (\neg q))))$$

$$(\neg((p \wedge q) \leftrightarrow (\neg(p \vee (\neg q)))))$$

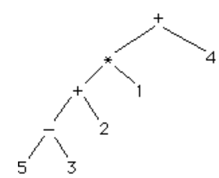
$$(\neg((p \wedge q) \leftrightarrow ((\neg p) \vee (\neg q))))$$

$$(\neg((p \wedge (q \leftrightarrow (\neg p))) \vee (\neg q)))$$

$$(\neg(((p \wedge q) \leftrightarrow (\neg p)) \vee (\neg q)))$$

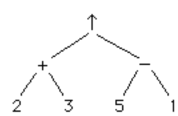
The other three cases are similar, giving us 3 possibilities if the $\wedge$ is the outermost operation, 4 if the $\leftrightarrow$ is, and 5 if the $\vee$ is. Therefore the answer is $7+3+4+5=19$.

22. We work from the beginning of the expression. In part **(a)** the root of the tree is necessarily the first $+$. We then use up as much of the rest of the expression as needed to construct the left subtree of the root. The root of this left subtree is the $*$, and its left subtree is as much of the rest of the expression as is needed. We continue in this way, making our way to the subtree consisting of root $-$ and children 5 and 3. Then the 2 must be the right child of the second $+$, the 1 must be the right child of the $*$, and the 4 must be the right child of the root. The result is shown here.

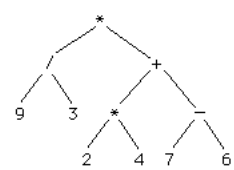


(a)

In infix form we have $((((5-3)+2)*1)+4)$. The other two trees are constructed in a similar manner.



(b)



(c)

The infix expressions are therefore $((2+3)\uparrow(5-1))$ and $((9/3)*((2*4)+(7-6)))$, respectively.

24. We exhibit the answers by showing with parentheses the operation that is applied next, working from left to right (it always involves the first occurrence of an operator symbol).

a) $5\,(2\,1\,-)-3\,1\,4++*=(5\,1\,-)\,3\,1\,4++*=4\,3\,(1\,4+)+*=4\,(3\,5+)*=(4\,8*)=32$

b) $(9\,3\,/)\,5+7\,2-*=(3\,5+)\,7\,2-*=8\,(7\,2\,-)*=(8\,5*)=40$

c) $(3\,2*)\,2\uparrow5\,3-8\,4\,/*-\;=\;(6\,2\uparrow)\,5\,3-8\,4\,/*-\;=\;36\,(5\,3\,-)\,8\,4\,/*-\;=\;36\;\;2\,(8\,4\,/)*-\;=\;36\,(2\,2*)-\;=\;(36\;\;4\,-)=32$

26. We prove this by induction on the length of the list. If the list has just one element, then the statement is trivially true. For the inductive step, consider the beginning of the list. There we find a sequence of vertices, starting with the root and ending with the first leaf (we can recognize the first leaf as the first vertex with no children), each vertex in the sequence being the first child of its predecessor in the list. Now remove this leaf, and decrease the child count of its parent by 1. The result is the preorder and child counts of a tree with one fewer vertex. By the inductive hypothesis we can uniquely determine this smaller tree. Then we can uniquely determine where the deleted vertex goes, since it is the first child of its parent (whom we know).

28. It is routine to see that the list is in alphabetical order in each case. In the first tree, vertex b has two children, whereas in the second, vertex b has three children, so the statement in Exercise 26 is not contradicted.

30. **a)** This is not well-formed by the result in Exercise 31.

b) This is not well-formed by the result in Exercise 31.

c) This is not well-formed by the result in Exercise 31.

d) This is well-formed. Each of the two subexpressions $\circ xx$ is well-formed. Therefore the subexpression $+\circ xx\circ xx$ is well-formed; call it A. Thus the entire expression is $\times Ax$, so it is well-formed.

32. The definition is word-for-word the same as that given for prefix expressions, except that "postfix" is substituted for "prefix" throughout, and $*XY$ is replaced by $XY*$.

34. We replace the inductive step (ii) in the definition with the statement that if X_1, X_2, $\ldots$, X_n are well-formed formulae and $*$ is an n-ary operator, then $*X_1X_2\ldots X_n$ is a well-formed formula.

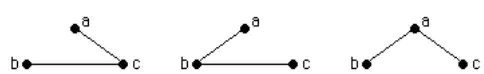
SECTION 11.4 Spanning Trees

2. Since the edge $\{a,b\}$ is part of a simple circuit, we can remove it. Then since the edge $\{b,c\}$ is part of a simple circuit that still remains, we can remove it. At this point there are no more simple circuits, so we have a spanning tree. There are many other possible answers, corresponding to different choices of edges to remove.

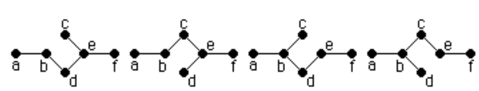
4. We can remove these edges to produce a spanning tree (see comments for Exercise 2): $\{a,i\}$, $\{b,i\}$, $\{b,j\}$, $\{c,d\}$, $\{c,j\}$, $\{d,e\}$, $\{e,j\}$, $\{f,i\}$, $\{f,j\}$, and $\{g,i\}$.

6. There are many, many possible answers. One set of choices is to remove edges $\{a,e\}$, $\{a,h\}$, $\{b,g\}$, $\{c,f\}$, $\{c,j\}$, $\{d,k\}$, $\{e,i\}$, $\{g,l\}$, $\{h,l\}$, and $\{i,k\}$.

8. We can remove any one of the three edges to produce a spanning tree. The trees are therefore the ones shown below.



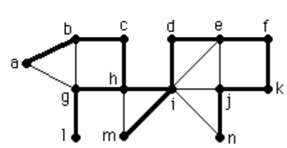
10. We can remove any one of the four edges in the middle square to produce a spanning tree, as shown.



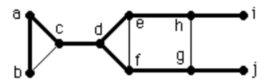
12. This is really the same problem as Exercises 11a, 12a, and 13a in Section 11.1, since a spanning tree of K_n is just a tree with n vertices. The answers are restated here for convenience.

a) 1 **b)** 2 **c)** 3

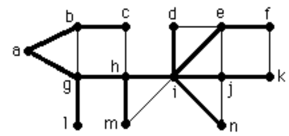
14. The tree is shown in heavy lines. It is produced by starting at a and continuing as far as possible without backtracking, choosing the first unused vertex (in alphabetical order) at each point. When the path reaches vertex l, we need to backtrack. Backtracking to h, we can then form the path all the way to n without further backtracking. Finally we backtrack to vertex i to pick up vertex m.



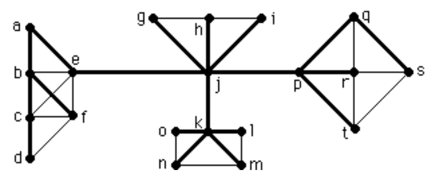
16. If we start at vertex a and use alphabetical order, then the breadth-first search spanning tree is unique. Consider the graph in Exercise 13. We first fan out from vertex a, picking up the edges $\{a, b\}$ and $\{a, c\}$. There are no new vertices from b, so we fan out from c, to get edge $\{c, d\}$. Then we fan out from d to get edges $\{d, e\}$ and $\{d, f\}$. This process continues until we have the entire tree shown in heavy lines below.



The tree for the graph in Exercise 14 is shown in heavy lines. It is produced by the same fanning-out procedure as described above.



The spanning tree for the graph in Exercise 15 is shown in heavy lines.

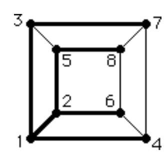


18. **a)** We start at the vertex in the middle of the wheel and visit all its neighbors—the vertices on the rim. This forms the spanning tree $K_{1,6}$ (see Exercise 19 for the general situation).

b) We start at any vertex and visit all its neighbors. Thus the resulting spanning tree is therefore $K_{1,4}$.

c) See Exercise 21 for the general result. We get a "double star": a $K_{1,3}$ and a $K_{1,2}$ with their centers joined by an edge.

d) By the symmetry of the cube, the result will always be the same (up to isomorphism), regardless of the order we impose on the vertices. We start at a vertex and fan out to its three neighbors. From one of them we fan out to two more, and pick up one more vertex from another neighbor. The final vertex is at a distance 3 from the root. In this figure we have labeled the vertices in the order visited.



20. Since every vertex is connected to every other vertex, the breadth-first search will construct the tree $K_{1,n-1}$, with every vertex adjacent to the starting vertex. The depth-first search will produce a simple path of length $n-1$ for the same reason.

22. The breadth-first search trees for Q_n are most easily described recursively. For $n = 0$ the tree is just a vertex. Given the tree T_n for Q_n, the tree for Q_{n+1} consists of T_n with one extra child of the root, coming first in left-to-right order, and that child is the root of a copy of T_n. These trees can also be described explicitly. If we think of the vertices of Q_n as bit strings of length n, then the root is the string of n 0's, and the children of each vertex are all the vertices that can be obtained by changing one 0 that has no 1's following it to a 1. For the depth-first search tree, the tree will depend on the order in which the vertices are picked. Because Q_n has a Hamilton path, it is possible that the tree will be a path. However, if "bad" choices are made, then the path might run into a dead end before visiting all the vertices, in which case the tree will have to branch.

24. We can order the vertices of the graph in the order in which they are first encountered in the search processes. Note, however, that we already need an order (at least locally, among the neighbors of a vertex) to make the search processes well-defined. The resulting orders given by depth-first search or breadth-first search are not the same, of course.

26. In each case we will call the colors red, blue, and green. Our backtracking plan is to color the vertices in alphabetical order. We first try the color red for the current vertex, if possible, and then move on to the next vertex. When we have backtracked to this vertex, we then try blue, if possible. Finally we try green. If no coloring of this vertex succeeds, then we erase the color on this vertex and backtrack to the previous vertex. For the graph in Exercise 7, no backtracking is required. We assign red, blue, red, and green to the vertices in alphabetical order. For the graph in Exercise 8, again no backtracking is required. We assign red, blue, blue, green, green, and red to the vertices in alphabetical order. And for the graph in Exercise 9, no backtracking is required either. We assign red, blue, red, blue, and blue to the vertices in alphabetical order.

28. **a)** The largest number that can possibly be included is 19. Since the sum of 19 and any smaller number in the list is greater than 20, we conclude that no subset with sum 20 contains 19. Then we try 14 and reach the same conclusion. Finally, we try 11, and note that after we have included 8, the list has been exhausted and the sum is not 20. Therefore there is no subset whose sum is 20.

b) Starting with 27 in the set, we soon find that the subset $\{27, 14\}$ has the desired sum of 41.

c) First we try putting 27 into the subset. If we also include 24, then no further additions are possible, so we backtrack and try including 19 with 27. Now it is possible to add 14, giving us the desired sum of 60.

30. **a)** We begin at the starting position. At each position, we keep track of which moves we have tried, and we try the moves in the order up, down, right, and left. (We also assume that the direction from which we entered this position has been tried, since we do not want our solution to retrace steps.) When we try a move, we then proceed along the chosen route until we are stymied, at which point we backtrack and try the next possible move. Either this will eventually lead us to the exit position, or we will have tried all the possibilities and concluded that there is no solution.

b) We start at position X. Since we cannot go up, we try going down. At the next intersection there is only one choice, so we go left. (All directions are stated in terms of our view of the picture.) This lead us to a dead end. Therefore we backtrack to position X and try going right. This leads us (without choices) to the opening about two thirds of the way from left to right in the second row, where we have the choice of going left or down. We try going down, and then right. No further choices are possible until we reach the opening just above the exit. Here we first try going up, but that leads to a dead end, so we try going down, and that leads us to the exit.

32. There is one tree for each component of the graph.

34. First notice that the order in which vertices are put into (and therefore taken out of) the list L is level-order. In other words, the root of the resulting tree comes first, then the vertices at level 1 (put into the list while processing the root), then the vertices at level 2 (put into the list while processing vertices at level 1), and so on. (A formal proof of this is given in Exercise 47.) Now suppose that uv is an edge not in the tree, and suppose without loss of generality that the algorithm processed u before it processed v. (In other words, u entered the list L before v did.) Since the edge uv is not in the tree, it must be the case that v was already in the list L when u was being processed. In order for this to happen, the parent p of v must have already been processed before u. Note that p's level in the tree is one less than v's level. Therefore u's level is greater than or equal to p's level but less than or equal to v's level, and the proof is complete.

36. We build the spanning tree using breath-first search. If at some point as we are fanning out from a vertex v we encounter a neighbor w of v that is already in the tree, then we know that there is a simple circuit, consisting of the path from the root to v, followed by the edge vw, followed by the path from the root to w traversed backward.

38. We construct a tree using one of these search methods. We color the first vertex red, and whenever we add a new vertex to the tree, we color it blue if we reach it from a red vertex, and we color it red if we reach it from a blue vertex. When we encounter a vertex that is already in the tree (and therefore will not be added to the tree), we compare its color to that of the vertex we are currently processing. If the colors are the same, then we know immediately that the graph is not bipartite. If we get through the entire process without finding such a clash, then we conclude that the graph is bipartite.

40. The algorithm is identical to the algorithm for obtaining spanning trees by deleting edges in simple circuits. While circuits remain, we remove an edge of a simple circuit. This does not disconnect any connected component of the graph, and eventually the process terminates with a forest of spanning trees of the components.

42. We apply breadth-first search, starting from the first vertex. When that search terminates, i.e., when the list is emptied, then we look for the first vertex that has not yet been included in the forest. If no such vertex is found, then we are done. If v is such a vertex, then we begin breadth-first search again from v, constructing the second tree in the forest. We continue in this way until all the vertices have been included.

44. If the edge is a cut edge, then it provides the unique simple path between its endpoints. Therefore it must be in every spanning tree for the graph. Conversely, if an edge is not a cut edge, then it can be removed without disconnecting the graph, and every spanning tree of the resulting graph will be a spanning tree of the original graph not containing this edge. Thus we have shown that an edge of a connected simple graph must be in every spanning tree for this graph if and only if the edge is a cut edge—i.e., its removal disconnects the graph.

46. Assume that the connected simple graph G does not have a simple path of length at least k. Consider the longest path in the depth-first search tree. Since each edge connects an ancestor and a descendant, we can bound the number of edges by counting the total number of ancestors of each descendant. But if the longest path is shorter than k, then each descendant has at most $k-1$ ancestors. Therefore there can be at most $(k-1)n$ edges.

48. We modify the pseudocode given in Algorithm 1 by initializing a global variable m to be 0 at the beginning of the algorithm, and adding the statements "$m := m+1$" and "assign m to vertex v" as the first line of procedure *visit*. To see that this numbering corresponds to the numbering of the vertices created by a preorder traversal of the spanning tree, we need to show that each vertex has a smaller number than its children, and that the children have increasing numbers from left to right (assuming that each new child added to the tree comes to the right of its siblings already in the tree). Clearly the children of a vertex get added to the tree only after that vertex is added, so their number must exceed that of their parent. And if a vertex's sibling has a smaller number, then it must have already been visited, and therefore already have been added to the tree.

50. Note that a "lower" level is further down the tree, i.e., further from the root and therefore having a larger value. (So "lower" really means "greater than"!) This is similar to Exercise 34. Again notice that the order in which vertices are put into (and therefore taken out of) the list L is level-order. In other words, the root of the resulting tree comes first, then the vertices at level 1 (put into the list while processing the root), then the vertices at level 2 (put into the list while processing vertices at level 1), and so on. Now suppose that uv is a directed edge not in the tree. First assume that the algorithm processed u before it processed v. (In other words, u entered the list L before v did.) Since the edge uv is not in the tree, it must be the case that v was already in the list L when u was being processed. In order for this to happen, the parent p of v must have already been processed before u. Note that p's level in the tree is one less than v's level. Therefore u's level is greater than or equal to p's level but less than or equal to v's level, so this directed edge goes from a vertex at one level to a vertex either at the same level or one level below. Next suppose that the algorithm processed v before it processed u. Then v's level is at or above u's level, and there is nothing else to prove.

52. Maintain a global variable c, initialized to 0. At the end of procedure *visit*, add the statements "$c := c + 1$" and "assign c to v." We need to show that each vertex has a larger number than its children, and that the children have increasing numbers from left to right (assuming that each new child added to the tree comes to the right of its siblings already in the tree). A vertex v is not numbered until its processing is finished, which means that all of the descendants of v must have finished their processing. Therefore each vertex has a larger number than all of its children. Furthermore, if a vertex's sibling has a smaller number, then it must have already been visited, and therefore already have been added to the tree. (Note that listing the vertices by number gives a postorder traversal of the tree.)

54. Suppose that T_1 contains a edges that are not in T_2, so that the distance between T_1 and T_2 is $2a$. Suppose further that T_2 contains b edges that are not in T_3, so that the distance between T_2 and T_3 is $2b$. Now at worst the only edges that are in T_1 and not in T_3 are those $a+b$ edges that are in T_1 and not in T_2, or in T_1 and T_2 but not in T_3. Therefore the distance between T_1 and T_3 is at most $2(a+b)$.

56. Following the construction of Exercise 55, we reduce the distance between spanning trees T_1 and T_2 by 2 when we remove edge e_1 from T_1 and add edge e_2 to it. Thus after applying this operation d times, we can convert any tree T_1 into any other spanning tree T_2 (where d is half the distance between T_1 and T_2).

58. By Exercise 16 in Section 10.5 there is an Euler circuit C in the directed graph. We follow C and delete from the directed graph every edge whose terminal vertex has been previously visited in C. We claim that the edges that remain in C form a rooted tree. Certainly there is a directed path from the root to every other vertex, since we only deleted edges that allowed us to reach vertices we could already reach. Furthermore, there can be no simple circuits, since we removed every edge that would have completed a simple circuit.

60. Since this is an "if and only if" statement, we have two things to prove. First, suppose that G contains a circuit $v_1, v_2, \ldots, v_k, v_1$, and without loss of generality, assume that v_1 is the first vertex visited in the depth-first search process. Since there is a directed path from v_1 to v_k, vertex v_k must have been visited before the processing of v_1 is completed. Therefore v_1 is an ancestor of v_k in the tree, and the edge $v_k v_1$ is a back edge. Now we have to prove the converse. Suppose that T contains a back edge uv from a vertex u to its ancestor v. Then the path in T from v to u, followed by this edge, is a circuit in G.

SECTION 11.5 Minimum Spanning Trees

2. We start with the minimum weight edge $\{a,b\}$. The least weight edge incident to the tree constructed so far is edge $\{a,e\}$, with weight 2, so we add it to the tree. Next we add edge $\{d,e\}$, and then edge $\{c,d\}$. This completes the tree, whose total weight is 6.

4. The edges are added in the order $\{a,b\}$, $\{a,e\}$, $\{a,d\}$, $\{c,d\}$, $\{d,h\}$, $\{a,m\}$, $\{d,p\}$, $\{e,f\}$, $\{e,i\}$, $\{g,h\}$, $\{l,p\}$, $\{m,n\}$, $\{n,o\}$, $\{f,j\}$, and $\{k,l\}$, for a total weight of 28.

6. With Kruskal's algorithm, we add at each step the shortest edge that will not complete a simple circuit. Thus we pick edge $\{a,b\}$ first, and then edge $\{c,d\}$ (alphabetical order breaks ties), followed by $\{a,e\}$ and $\{d,e\}$.The total weight is 6.

8. The edges are added in the order $\{a,b\}$, $\{a,e\}$, $\{c,d\}$, $\{d,h\}$, $\{a,d\}$, $\{a,m\}$, $\{d,p\}$, $\{e,f\}$, $\{e,i\}$, $\{g,h\}$, $\{l,p\}$, $\{m,n\}$, $\{n,o\}$, $\{f,j\}$, and $\{k,l\}$, for a total weight of 28.

10. One way to do this is simply to apply the algorithm of choice to each component. In practice it is not clear what that means, since we would have to determine the components first. More to the point, we can implement the procedures as follows. For Prim's algorithm, start with the first vertex and repeatedly add to the tree the shortest edge adjacent to it that does not complete a simple circuit. When no such edges remain, we find a vertex that is not yet in the spanning forest and grow a new tree from this vertex. We repeat this process until no new vertices remain. Kruskal's algorithm is even simpler to implement. We keep choosing the shortest edge that does not complete a simple circuit, until no such edges remain. The result is a spanning forest of minimum weight.

12. If we simply replace the word "smallest" with the word "largest" (and replace the word "minimum" in the comment with the word "maximum") in Algorithm 2, then the resulting algorithm will find a maximum spanning tree.

14. The answer is unique. It uses edges $\{d,h\}$, $\{d,e\}$, $\{b,f\}$, $\{d,g\}$, $\{a,b\}$, $\{b,e\}$, $\{b,c\}$, and $\{f,i\}$.

16. We follow the procedure outlined in the solution to Exercise 17. Recall that the minimum spanning tree uses the edges Atlanta–Chicago, Atlanta–New York, Denver–San Francisco, and Chicago–San Francisco. First we delete the edge from Atlanta to Chicago. The minimum spanning tree for the remaining graph has cost \$3900. Next we delete the edge from Atlanta to New York (and put the previously deleted edge back). The minimum spanning tree now has cost \$3800. Next we look at the graph with the edge from Denver to San Francisco deleted. The minimum spanning tree has cost \$4000. Finally we look at the graph with the edge from Chicago to San Francisco deleted. The minimum spanning tree has cost \$3700. This last tree is our answer, then; it consists of the links Atlanta–Chicago, Atlanta–New York, Denver–San Francisco, and Chicago–Denver.

18. Suppose that an edge e with smallest weight is not included in some minimum spanning tree; in other words, suppose that the minimum spanning tree T contains only edges with weights larger than that of e. If we add e to T, then we will obtain a graph with exactly one simple circuit, which contains e. We can then delete some other edge in this circuit, resulting in a spanning tree with weight strictly less than that of T (since all the other edges have larger weight than e has). This is a contradiction to the fact that T is a minimum spanning tree. Therefore an edge with smallest weight must be included in T.

20. We start with the New York to Denver link and then form a spanning tree by successively adding the cheapest edges that do not form a simple circuit. In fact the three cheapest edges will do: Atlanta–Chicago, Atlanta–New York, and Denver–San Francisco. This gives a cost of \$4000.

22. The algorithm is the same as Kruskal's, except that instead of starting with the empty tree, we start with the given set of edges. (If there is already a simple circuit among these edges, then there is no solution.)

24. We prove this by contradiction. Suppose that there is a simple circuit formed after the addition of edges at some stage in the algorithm. The circuit will contain some edges that were added at that stage and perhaps some edges that were already present. Let e_1, e_2, $\ldots$, e_r be the edges that are new, in the order they are traversed in the circuit. Thus the circuit can be thought of as the sequence e_1, T_1, e_2, T_2, $\ldots$, e_r, T_r, e_1, where each T_i is a tree that existed before the addition of new edges. Each edge in this sequence was the edge picked by the tree containing one of its two endpoints, so since there are the same number of trees as there are edges in this sequence, each tree must have picked a different edge. However, let e be the shortest edge (after tie-breaking) among $\{e_1, e_2, \ldots, e_r\}$. Then the tree at both of its ends necessarily picked e to add to the tree, a contradiction. Therefore there are no simple circuits.

26. The actual implementation of this algorithm is more difficult than this pseudocode shows, of course.

```
procedure Sollin(G : simple graph)
initialize the set of trees to be the set of vertices
while |set of trees| > 1 do
        for each tree T_i in the set of trees
                e_i := the shortest edge from a vertex in T_i to a vertex not in T_i
        add all the e_i's to the trees already present and
            reorganize the resulting graph into a set of trees
```

28. This is a special case of Exercise 29, with r equal to the number of vertices in the graph (each vertex is a tree by itself at the beginning of the algorithm); see the solution to that exercise.

30. As argued in the solution to Exercise 29, each stage in the algorithm reduces the number of trees by a factor of at least 2. Therefore after k stages at most $n/2^k$ trees remain. Since the number of trees is an integer, the number must be less than or equal to $\lfloor n/2^k \rfloor$.

32. Let G be a connected weighted graph. Suppose that the successive edges chosen by Kruskal's algorithm are e_1, e_2, $\ldots$, e_{n-1}, in that order, so that the tree S containing these edges is the tree constructed by the algorithm. Let T be a minimum spanning tree of G containing e_1, e_2, $\ldots$, e_k, with k chosen as large as possible (possibly 0). If $k = n-1$, then we are done, since $S = T$. Otherwise $k < n-1$, and in this case we will derive a contradiction by finding a minimum spanning tree T' which gives us a larger value of k. Consider $T \cup \{e_{k+1}\}$. Since T is a tree, this graph has a simple circuit which must contain e_{k+1}. Some edge e in this simple circuit is not in S, since S is a tree. Furthermore, e was available to be chosen by Kruskal's algorithm at the point at which e_{k+1} was chosen, since there is no simple circuit among $\{e_1, e_2, \ldots, e_k, e\}$ (these edges are all in T). Therefore the weight of e_{k+1} is less than or equal to the weight of e (otherwise the algorithm would have chosen e instead of e_{k+1}). Now add e_{k+1} to T and delete e; call the resulting tree T'. The weight of T' cannot be any greater than the weight of T. Therefore T' is also a minimum spanning tree, which contains the edges e_1, e_2, $\ldots$, e_k, e_{k+1}. This contradicts the choice of T, and our proof is complete.

34. This algorithm converts G into its minimum spanning tree. To implement it, it is best to order the edges by decreasing weight before we start.

```
procedure reverse-delete(G : weighted connected undirected graph with n vertices)
while G has more than n − 1 edges
        e := any edge of largest weight that is in a simple circuit in G
                (i.e., whose removal would not disconnect G)
        G := G with edge e deleted
```

SUPPLEMENTARY EXERCISES FOR CHAPTER 11

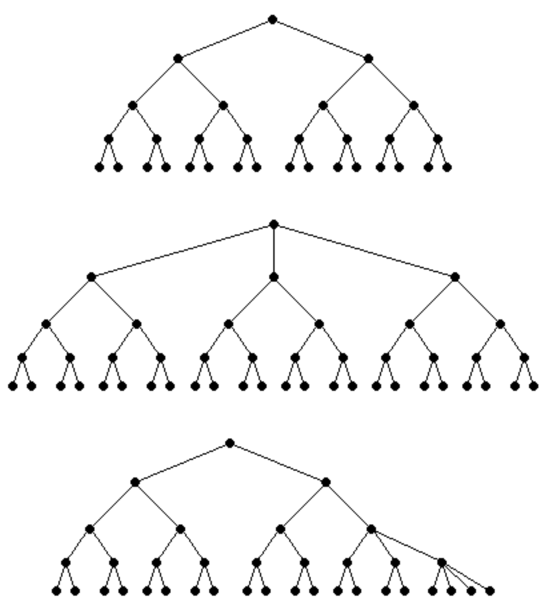
2. There are 20 such trees. We can organize our count by the height of the tree. There is just 1 rooted tree on 6 vertices with height 5. If the height is 4 (so that there is a path from the root containing 5 vertices), then there are 4 choices as to where to attach the sixth vertex. If the height is 3, fix a path of length three from the root. Two more vertices need to be added. If they are both attached directly to the original path, then there are $C(3+2-1,2)=6$ ways to attach them (since there are three possible points of attachment). On the other hand if they form a path of length 2 from their point of attachment, then there are 2 choices. Next suppose the height is 2. If there are not two disjoint paths of length 2 from the root, then there are 4 ways that the other 3 vertices can be attached to a given path of length 2 from the root (0, 1, 2, or 3 of them can be attached to the root). If there are two disjoint paths, then there are 2 choices for the sixth vertex. Finally, there is 1 tree of height 1. Thus we have $1+4+6+2+4+2+1=20$ trees in all.

4. We know that the sum of the degrees must be $2(n-1)$. The $n-1$ pendant vertices account for $n-1$ in this sum, so the degree of the other vertex must be $n-1$. This vertex is one part of $K_{1,n-1}$, therefore, and the pendant vertices are the other part.

6. We prove this by induction on n. The problem is trivial if $n \leq 2$, so assume that the inductive hypothesis holds and let $n \geq 3$. First note that at least one of the positive integers d_i must equal 1, since the sum of n numbers each greater than or equal to 2 is greater than or equal to $2n$. Without loss of generality assume that $d_n = 1$. Now it is impossible for all the remaining d_i's to equal 1, since $2n-2 > n$ (we are assuming that $n > 2$); without loss of generality assume that $d_1 > 1$. Now apply the inductive hypothesis to the sequence $d_1 - 1, d_2, d_3, \ldots, d_{n-1}$. There is a tree with these degrees. Add an edge from the vertex with degree $d_1 - 1$ to a new vertex, and we have the desired tree with degrees $d_1, d_2, \ldots, d_n$.

8. We consider the tree as a rooted tree. One part is the set of vertices at even-numbered levels, and the other part is the set of vertices at odd-numbered levels.

10. The following pictures show some B-trees with the desired height and degree. The root must have either 2 or 3 children, and the other internal vertices must have between 2 and 4 children, inclusive. Note that our first example is a complete binary tree.



12. The lower bound for the height of a B-tree of degree k with n leaves comes from the upper bound for the number of leaves in a B-tree of degree k with height h, obtained in Exercise 11. Since there we found that $n \le k^h$, we have $h \ge \log_k n$. The upper bound for the height of a B-tree of degree k with n leaves comes from the lower bound for the number of leaves in a B-tree of degree k with height h, obtained in Exercise 11. Since there we found that $n \ge 2\lceil k/2 \rceil^{h-1}$, we have $h \le 1 + \log_{\lceil k/2 \rceil}(n/2)$.

14. Since B_{k+1} is formed from two copies of B_k, the number of vertices doubles as k increases by 1. Since B_0 had $1 = 2^0$ vertices, it follows by induction that B_k has 2^k vertices.

16. Looking at the pictures for B_k leads one to conjecture that the number of vertices at depth j is $C(k,j)$. For example, in B_4 the number of vertices at the various levels form the sequence 1, 4, 6, 4, 1, which are exactly $C(4,0)$, $C(4,1)$, $C(4,2)$, $C(4,3)$, $C(4,4)$. To prove this by mathematical induction (the basis step being trivial), note that by the way B_{k+1} is constructed, the number of vertices at level $j+1$ in B_{k+1} is the sum of the number of vertices at level $j+1$ in B_k and the number of vertices at level j in B_k. By the inductive hypothesis this is $C(k,j+1)+C(k,j)$, which equals $C(k+1,j+1)$ as desired, by Pascal's identity. This holds for $j = k$ as well, and at the 0^{th} level, too, there is clearly just one vertex.

18. Our inductive hypothesis is that the root and the left-most child of the root of B_k have degree k and every other vertex has degree less than k. This is certainly true for B_0 and B_1. Consider B_{k+1}. By Exercise 17, its root has degree $k+1$, as desired. The left-most child of the root is the root of a B_k, which had degree k, and we have added one edge to connect it to the root of B_{k+1}, so its degree is now $k+1$, as desired. Every other vertex of B_{k+1} has the same degree it had in B_k, which was at most k by the inductive hypothesis, and our proof is complete.

20. That an S_k-tree has 2^k vertices is clear by induction, since an S_k-tree has twice as many vertices as an S_{k-1}-tree and an S_0-tree has $2^0 = 1$ vertex. Also by induction we see that there is a unique vertex at level k, since there was a unique vertex at level $k-1$ in the S_{k-1}-tree whose root was made a child of the root of the other S_{k-1}-tree in the construction of the S_k-tree.

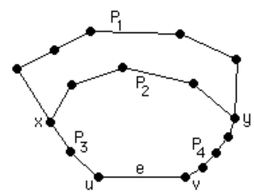
22. The level order in each case is the alphabetical order in which the vertices are labeled.

24. Given the set of universal addresses, we need to check two things. First we need to be sure that no address in our list is the address of an internal vertex. This we can accomplish by checking that no address in our list is a prefix of another address in our list. (Also of course, if the list contains 0, then it must contain no other addresses.) Second we need to make sure that all the internal vertices have a leaf as a descendant. To check this, for each address $a_1.a_2.\cdots.a_r$ in the list, and for each i from 1 to r, inclusive, and for each b with $1 \le b < a_i$, we check that there is an address in the list with prefix $a_1.a_2.\cdots.a_{i-1}.b$.

26. We assume that the graph in question is connected. (If it is not, then the statement is vacuously true.) If we remove all the edges of a cut set, the resulting graph cannot still be connected. If the resulting graph contained all the edges of a spanning tree, then it would be connected. Therefore there must be at least one edge of the spanning tree in the cut set.

28. A tree is necessarily a cactus, since no edge is in any simple circuit at all.

30. Suppose G is not a cactus; we will show that G contains a very simple circuit with an even number of edges (see the solution to Exercise 27 for the definition of "very simple circuit"). Suppose instead, then, that every very simple circuit of G contains an odd number of edges. Since G is not a cactus, we can find an edge $e = \{u, v\}$ that is in two different very simple circuits. By simplifying the second circuit if necessary, we can assume that the situation is as pictured here, where x might be u and y might be v. Since the circuits $u, P_3, x, P_1, y, P_4, v, e, u$ and $u, P_3, x, P_2, y, P_4, v, e, u$ are both odd, the paths P_1 and P_2 have to have the same parity. Therefore the very simple circuit consisting of P_1 followed by P_2 backwards has even length, as desired.



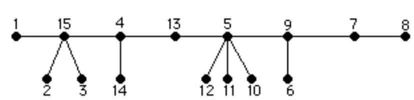
32. The only spanning tree here is the graph itself, and vertex i has degree greater than 3. Thus there is no degree-constrained spanning tree where each vertex has degree less than or equal to 3.

34. Such a tree must be a path (since it is connected and has no vertices of degree greater than 2), and since it includes every vertex in the graph, it is a Hamilton path.

36. The graphs in the first three parts are caterpillars, since every vertex is either in the horizontal path of length 3 or adjacent to a vertex in this path. In part **(d)** it is clear that there is no path that can serve as the "spine" of the caterpillar.

38. **a)** We can gracefully label the vertices in the path in the following manner. Suppose there are n vertices. We label every other vertex, starting with the first, with the numbers $1, 2, \ldots, \lceil n/2 \rceil$; we number the remaining vertices, in the same order, with $n, n-1, \ldots, \lceil n/2 \rceil + 1$. For example, if $n = 7$, then the vertices are labeled $1, 7, 2, 6, 3, 5, 4$. The successive differences are then easily seen to be $n-1, n-2, \ldots, 2, 1$, as desired.

b) We extend the idea in the solution to part **(a)**, allowing for labeling the "feet" as well as the "spine" of the caterpillar. We can assume that the first and last vertices in the spine have no feet. First we label the vertex at the beginning of the spine 1, and, as above, label the vertex adjacent to it n. If there are some feet at this vertex, then we label them $2, 3, \ldots, k$ (where the number of feet there is $k-1$). Then we label the next vertex on the spine with the smallest available number—either 2 or $k+1$ (if there were feet that needed labeling). If this vertex has feet, then we label them $n-1, n-2$, and so on. The largest available number is then used for the label of the next vertex on the spine. We continue in this manner until we have labeled the entire caterpillar. It is clear that the labeling is graceful. See the example below.



40. By Exercise 52 in Section 11.4, we can number the vertices while doing depth-first search in order of their finishing. It follows from the solution given there that this order corresponds to postorder in the spanning tree. We claim that the opposite order of these numbers gives a topological sort of the vertices in the graph. We must show that there is no directed edge uv such that u's number in this process is less than v's number (prior to reversing the order). Clearly this is true if uv is a tree edge, since the numbers of all of a vertex's descendants are less than the number of that vertex. By Exercise 60 in Section 11.4, there are no back edges in our acyclic digraph. By Exercise 51 in Section 11.4, if uv is a forward edge, then it connects a vertex to a descendant, so the number of u exceeds the number of v, and that is consistent with our given partial order. And if uv is a cross edge, then v is in a previously visited subtree, so the number on v is less than the number on u, again consistent with the given partial order.

42. We form a graph whose vertices are the allowable positions of the people and boat. Each vertex, then, contains the information as to which of the six people and the boat are on, say, the near bank (the remaining people and/or boat are on the far bank). If we label the people X, Y, Z, x, y, z (the husbands in upper case letters and the wives in the corresponding lower case letters) and the boat B, then the initial position is $XYZxyzB$ and the desired final position is the empty set. Two vertices are joined by an edge if it is possible to obtain one position from the other with one legal boat ride (where "legal" means of course that the rules of the puzzle are not violated—that no man is left alone with a woman other than his wife, and that the boat crosses the river only with one or two people in it). For example, the vertex $YZyz$ is adjacent to the vertex $XYZxyzB$, since the married couple Xx can travel to the opposite bank in the boat. Our task is to find a path in this graph from the initial position to the desired final position. Dijkstra's algorithm could be used to find such a path. The graph is too large to draw here, but with this notation (and arrows for readability), one path is $XYZxyzB \to YZyz \to YZxyzB \to YZy \to YZyzB \to Zz \to ZyzB \to Z \to ZzB \to \emptyset$.

44. We assume that what is being asked for here is not "a minimum spanning tree of the graph that also happens to satisfy the degree constraint" but rather "a tree of minimum weight among all spanning trees that satisfy the degree constraint."

a) Since b is a cut vertex we must include at least one of the two edges $\{b, c\}$ and $\{b, d\}$, and one of the other three edges incident to b. Thus the best we can do is to include edges $\{b, c\}$ and $\{a, b\}$. It is then easy to see that the unique minimum spanning tree with degrees constrained to be at most 2 consists of these two edges, together with $\{c, d\}$, $\{a, f\}$, and $\{e, f\}$.

b) Obviously we must include edge $\{a, b\}$. We cannot include edge $\{b, g\}$, because this would force some vertex to have degree greater than 2 in the spanning tree. For a similar reason we cannot include edge $\{b, d\}$. A little more thought shows that the minimum spanning tree under these constraints consists of edge $\{a, b\}$, together with edges $\{b, c\}$, $\{c, d\}$, $\{d, g\}$, $\{f, g\}$, and $\{e, f\}$.

46. The "only if" direction is immediate from the definition of arborescence. To prove the "if" direction, perform a directed depth-first search on G starting at vertex r. Because there is a directed path from r to every $v \in V$, this search will eventually visit every vertex in G and thereby produce a spanning tree of the underlying undirected graph. The directed paths in this tree are the desired paths in the arborescence.

CHAPTER 12
Boolean Algebra

SECTION 12.1 Boolean Functions

2. **a)** Since $x \cdot 1 = x$, the only solution is $x = 0$.
b) Since $0 + 0 = 0$ and $1 + 1 = 1$, the only solution is $x = 0$.
c) Since this equation holds for all x, there are two solutions, $x = 0$ and $x = 1$.
d) Since either x or $\overline{x}$ must be 0, no matter what x is, there are no solutions.

4. **a)** We compute $(\overline{1} \cdot \overline{0}) + (1 \cdot \overline{0}) = (0 \cdot 1) + (1 \cdot 1) = 0 + 1 = 1$.
b) Following the instructions, we have $(\neg \mathbf{T} \wedge \neg \mathbf{F}) \vee (\mathbf{T} \wedge \neg \mathbf{F}) \equiv \mathbf{T}$.

6. In each case, we compute the various components of the final expression and put them together as indicated. For part **(a)** we have simply

x	y	z	$\overline{z}$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

For part **(b)** we have

x	y	z	$\overline{x}$	$\overline{x}\,y$	$\overline{y}$	$\overline{y}\,z$	$\overline{x}\,y + \overline{y}\,z$
1	1	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	1	1	1
1	0	0	0	0	1	0	0
0	1	1	1	1	0	0	1
0	1	0	1	1	0	0	1
0	0	1	1	0	1	1	1
0	0	0	1	0	1	0	0

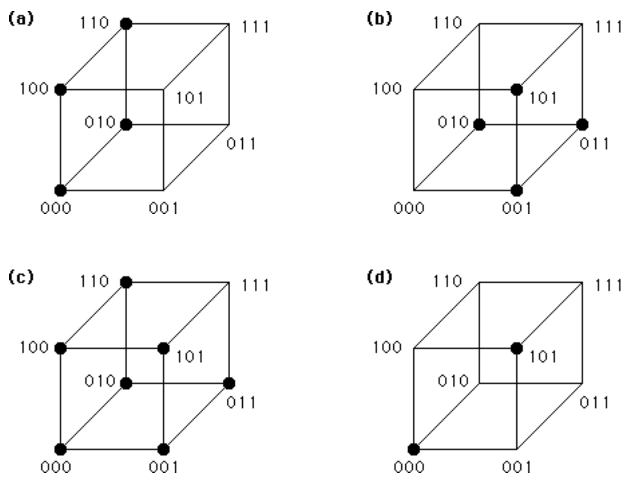
For part **(c)** we have

x	y	z	$\overline{y}$	$x\,\overline{y}\,z$	xyz	$\overline{xyz}$	$x\,\overline{y}\,z + \overline{xyz}$
1	1	1	0	0	1	0	0
1	1	0	0	0	0	1	1
1	0	1	1	1	0	1	1
1	0	0	1	0	0	1	1
0	1	1	0	0	0	1	1
0	1	0	0	0	0	1	1
0	0	1	1	0	0	1	1
0	0	0	1	0	0	1	1

For part **(d)** we have

x	y	z	$\overline{x}$	$\overline{y}$	$\overline{z}$	xz	$\overline{x}\,\overline{z}$	$xz+\overline{x}\,\overline{z}$	$\overline{y}(xz+\overline{x}\,\overline{z})$
1	1	1	0	0	0	1	0	1	0
1	1	0	0	0	1	0	0	0	0
1	0	1	0	1	0	1	0	1	1
1	0	0	0	1	1	0	0	0	0
0	1	1	1	0	0	0	0	0	0
0	1	0	1	0	1	0	1	1	0
0	0	1	1	1	0	0	0	0	0
0	0	0	1	1	1	0	1	1	1

8. In each case, we note from our solution to Exercise 6 which vertices need to be blackened in the cube, as in Figure 1.



10. There are 2^{2^n} different Boolean functions of degree n, so the answer is $2^{2^7} = 2^{128} \approx 3.4 \times 10^{38}$.

12. The only way for the sum to have the value 1 is for one of the summands to have the value 1, since $0+0+0 = 0$. Each summand is 1 if and only if the two variables in the product making up that summand are both 1. The conclusion follows.

14. If $x = 0$, then $\overline{\overline{x}} = \overline{\overline{0}} = \overline{1} = 0 = x$. We obtain $\overline{\overline{1}} = 1$ by a similar calculation. The relevant table, exhibiting this calculation, has only two rows.

16. We just plug in $x = 0$ and $x = 1$ and see that the equations hold in each case. The relevant tables, exhibiting these calculations, have only two rows.

18. We can make a table to list the four possible combinations of values for x and y in each case, and check that $x + y = y + x$ and $xy = yx$. Alternatively, we simply note that $x + y = 0$ if and only if $x = y = 0$, and $xy = 1$ if and only if $x = y = 1$, and these statement are symmetric in the variables x and y.

20. We can make a table to list all the possibilities, but instead let us argue more directly. The left-hand side of this equation is 1 precisely when either $x = 1$ or both y and z are 1. In the former case, both $x + y$ and $x + z$ are 1, so their product is 1, and in the latter case both $x + y$ and $x + z$ are 1, so again their product is 1. Conversely, the left-hand side is 0 when $x = 0$ and at least one of y and z is 0. In this case, at least one of $x + y$ and $x + z$ is 0, so their product is 0.

22. The unit property states that $x+\overline{x}=1$. There are only two things to check: $0+\overline{0}=0+1=1$ and $1+\overline{1}=1+0=1$. The relevant table, exhibiting this calculation, has only two rows.

24. **a)** Since $0\oplus 0=0$ and $1\oplus 0=1$, this expression simplifies to x.
b) Since $0\oplus 1=1$ and $1\oplus 1=0$, this expression simplifies to $\overline{x}$.
c) Looking at the definition, we see that $x\oplus x=0$ for all x.
d) This is similar to part **(c)**; this time the expression always equals 1.

26. A glance at the definition shows that $x\oplus y=y\oplus x$ for all four possibilities for x and y.

28. In each case we simply change each 0 to a 1 and vice versa, and change all the sums to products and vice versa.
a) xy **b)** $\overline{x}+\overline{y}$ **c)** $(x+y+z)(\overline{x}+\overline{y}+\overline{z})$ **d)** $(x+\overline{z})(x+1)(\overline{x}+0)$

30. By Exercise 29, what we are asked to show is equivalent to the statement that for all values of x_1, x_2, ..., x_n, we have $\overline{F(\overline{x}_1,\ldots,\overline{x}_n)}=\overline{G(\overline{x}_1,\ldots,\overline{x}_n)}$. Now this is clearly equivalent to $F(\overline{x}_1,\ldots,\overline{x}_n)=G(\overline{x}_1,\ldots,\overline{x}_n)$. But the value of the n-tuple $(\overline{x}_1,\ldots,\overline{x}_n)$ ranges over all n-tuples of 0's and 1's as the value of $(x_1,\ldots,x_n)$ ranges over all n-tuples of 0's and 1's (albeit in a different order). Since we are given that $F=G$, the desired conclusion follows.

32. Suppose that you specify $F(0,0,0)$. Then the equations determine $F(\overline{0},\overline{0},0)=F(1,1,0)$ and $F(\overline{0},0,\overline{0})=F(1,0,1)$. It also therefore determines $F(\overline{1},1,\overline{0})=F(0,1,1)$, but nothing else. If we now also specify $F(1,1,1)$ (and there are no restrictions imposed so far), then the equations tell us, in a similar way, what $F(0,0,1)$, $F(0,1,0)$, and $F(1,0,0)$ are. This completes the definition of F. Since we had two choices in specifying $F(0,0,0)$ and two choices in specifying $F(1,1,1)$, the answer is $2\cdot 2=4$.

34. We need to replace each 0 by $\mathbf{F}$, 1 by $\mathbf{T}$, $+$ by $\vee$, $\cdot$ (or Boolean product implied by juxtaposition) by $\wedge$, and $\overline{}$ by $\neg$. We also replace x by p and y by q so that the variables look like they represent propositions, and we replace the equals sign by the logical equivalence symbol. We also add parentheses for clarification. Thus for the first absorption law in Table 5, $x+xy=x$ becomes $p\vee(p\wedge q)\equiv p$, which is the first absorption law in Table 6 of Section 1.3. Dually, $x(x+y)=x$ becomes $p\wedge(p\vee q)\equiv p$ for the other absorption law.

36. To prove that the complement of x is unique, we suppose that y is a complement (i.e., $x\vee y=1$ and $x\wedge y=0$) and play with the symbols (using the axioms in Definition 1) until we have $y=\overline{x}$. The reason for each step in this proof is just one (or more) of these axioms.

$$\begin{aligned}
y=y\wedge 1&=y\wedge(x\vee\overline{x})\\
&=(y\wedge x)\vee(y\wedge\overline{x})\\
&=(x\wedge y)\vee(y\wedge\overline{x})\\
&=0\vee(y\wedge\overline{x})\\
&=y\wedge\overline{x}\\
&=(y\wedge\overline{x})\vee 0\\
&=(y\wedge\overline{x})\vee(x\wedge\overline{x})\\
&=(\overline{x}\wedge y)\vee(\overline{x}\wedge x)\\
&=\overline{x}\wedge(y\vee x)\\
&=\overline{x}\wedge(x\vee y)\\
&=\overline{x}\wedge 1=\overline{x}
\end{aligned}$$

38. This follows from Exercise 36, where we showed that the complement of an element z is that unique element y such that $z \vee y = 1$ and $z \wedge y = 0$. For this exercise, we just need to show that $y = x$ fits this definition if we choose $z = \overline{x}$. In other words, this will show that x is the complement of $\overline{x}$. But plugging into our equations we have simply $\overline{x} \vee x = 1$ and $\overline{x} \wedge x = 0$, which follow from the axioms (including commutativity).

40. We start with the left-hand side and try to obtain the right-hand side. We freely use the axioms from Definition 1 as well as the result in Exercise 35. For the first identity,

$$\begin{aligned} x \wedge (y \vee (x \wedge z)) &= (x \wedge y) \vee (x \wedge x \wedge z) \\ &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

The second proof is dual (interchange the roles of $\wedge$ and $\vee$).

42. Since all the axioms come in dual pairs, any proof of an identity can be transformed into a proof of the dual identity by interchanging $\vee$ with $\wedge$ and interchanging 0 with 1. Hence if an identity is valid, so is its dual.

SECTION 12.2 Representing Boolean Functions

2. **a)** We can rewrite this as $F(x,y) = \overline{x} \cdot 1 + \overline{y} \cdot 1 = \overline{x}(y+\overline{y}) + y(x+\overline{x})$. Expanding and using the commutative and idempotent laws, this simplifies to $\overline{x}\,y + \overline{x}\,\overline{y} + x\,y$.
b) This is already in sum-of-products form.
c) We need to write the sum of all products; the answer is $x\,y + x\,\overline{y} + \overline{x}\,y + \overline{x}\,\overline{y}$.
d) As in part **(a)**, we have $F(x,y) = 1 \cdot \overline{y} = (x+\overline{x})y = x\,y + \overline{x}\,y$.

4. **a)** We need to write all the terms that have $\overline{x}$ in them. Thus the answer is $\overline{x}\,y\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z}$.
b) We need to write all the terms that include either $\overline{x}$ or $\overline{y}$. Thus the answer is $x\,\overline{y}\,z + x\,\overline{y}\,\overline{z} + \overline{x}\,y\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z}$.
c) We need to include all the terms that have both $\overline{x}$ and $\overline{y}$. Thus the answer is $\overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z}$.
d) We need to include all the terms that have at least one of $\overline{x}$, $\overline{y}$, and $\overline{z}$. This is all the terms except $x\,y\,z$, so the answer is $x\,y\,\overline{z} + x\,\overline{y}\,z + x\,\overline{y}\,\overline{z} + \overline{x}\,y\,z + \overline{x}\,y\,\overline{z} + \overline{x}\,\overline{y}\,z + \overline{x}\,\overline{y}\,\overline{z}$.

6. We need to include all terms that have three or more of the variables in their uncomplemented form. This will give us a total of $1 + 5 + 10 = 16$ terms. The answer is

$$\begin{aligned} x_1\,x_2\,x_3\,x_4\,x_5 &+ x_1\,x_2\,x_3\,x_4\,\overline{x}_5 + x_1\,x_2\,x_3\,\overline{x}_4\,x_5 + x_1\,x_2\,\overline{x}_3\,x_4\,x_5 + x_1\,\overline{x}_2\,x_3\,x_4\,x_5 + \overline{x}_1\,x_2\,x_3\,x_4\,x_5 \\ &+ x_1\,x_2\,x_3\,\overline{x}_4\,\overline{x}_5 + x_1\,x_2\,\overline{x}_3\,x_4\,\overline{x}_5 + x_1\,x_2\,\overline{x}_3\,\overline{x}_4\,x_5 + x_1\,\overline{x}_2\,x_3\,x_4\,\overline{x}_5 + x_1\,\overline{x}_2\,x_3\,\overline{x}_4\,x_5 \\ &+ x_1\,\overline{x}_2\,\overline{x}_3\,x_4\,x_5 + \overline{x}_1\,x_2\,x_3\,x_4\,\overline{x}_5 + \overline{x}_1\,x_2\,x_3\,\overline{x}_4\,x_5 + \overline{x}_1\,x_2\,\overline{x}_3\,x_4\,x_5 + \overline{x}_1\,\overline{x}_2\,x_3\,x_4\,x_5\,. \end{aligned}$$

8. We follow the hint and form the product $(\overline{x} + \overline{y} + z)(x + y + z)(x + \overline{y} + z)$. It will have the value 0 as long as one of the factors has the value 0.

10. We follow the hint and include one maxterm in this product for each combination of variables for which the function has the value 0 (see Exercise 9). Since a product is 0 if and only if at least one of the factors is 0, this sum has the desired value.

12. We need to use De Morgan's law to replace each occurrence of $s+t$ by $\overline{(\overline{s}\,\overline{t})}$, simplifying by use of the double complement law if possible.
a) $(x+y)+z = \overline{(\overline{(x+y)}\,\overline{z})} = \overline{(\overline{x}\,\overline{y}\,\overline{z})}$ **b)** $x + \overline{y}\,(\overline{x}+z) = \overline{(\overline{x}\,\overline{(\overline{y}\,(\overline{x}+z))})} = \overline{(\overline{x}\,\overline{(\overline{y}\,\overline{(x\,\overline{z})})})}$
c) In this case we can just apply De Morgan's law directly, to obtain $\overline{x}\,\overline{\overline{y}} = \overline{x}\,y$.
d) The second factor is changed in a manner similar to part **(a)**. Thus the answer is $\overline{x}\overline{(\overline{x}\,y\,z)}$.

14. **a)** We use the definition of $|$. If $x = 1$, then $x \mid x = 0$; and if $x = 0$, then $x \mid x = 1$. These are precisely the corresponding values of $\overline{x}$.

b) We can construct a table to look at all four cases, as follows. Since the fourth and fifth columns are equal, the expressions are equivalent.

x	y	$x \mid y$	$(x \mid y) \mid (x \mid y)$	xy
1	1	0	1	1
1	0	1	0	0
0	1	1	0	0
0	0	1	0	0

c) We can construct a table to look at all four cases, as follows. Since the fifth and sixth columns are equal, the expressions are equivalent.

x	y	$x \mid x$	$y \mid y$	$(x \mid x) \mid (y \mid y)$	$x + y$
1	1	0	0	1	1
1	0	0	1	1	1
0	1	1	0	1	1
0	0	1	1	0	0

16. Since we already know that complementation, sum and product together are functionally complete, and since Exercise 15 tells us how to write all of these operations totally in terms of $\downarrow$, we can write every Boolean function totally in terms of $\downarrow$.

18. We use the results of Exercise 15.

a) $(x+y)+z = ((x+y)\downarrow z)\downarrow((x+y)\downarrow z) = (((x\downarrow y)\downarrow(x\downarrow y))\downarrow z)\downarrow(((x\downarrow y)\downarrow(x\downarrow y))\downarrow z)$

b) $(x+z)y = ((x+z)\downarrow(x+z))\downarrow(y\downarrow y) = (((x\downarrow z)\downarrow(x\downarrow z))\downarrow((x\downarrow z)\downarrow(x\downarrow z)))\downarrow(y\downarrow y)$

c) This is already in the desired form, since it has no operators.

d) $x\overline{y} = (x\downarrow x)\downarrow(\overline{y}\downarrow\overline{y}) = (x\downarrow x)\downarrow((y\downarrow y)\downarrow(y\downarrow y))$

20. We assume here that the constants 0 and 1 cannot be used (the answers to parts **(a)** and **(c)** are different if constants are allowed).

a) Note that $0+0 = 0\oplus 0 = 0$. This means that every function that uses only these two operations must have the value 0 when the inputs are all 0. Therefore using only these two operations, we cannot construct the Boolean function that is 1 for all inputs.

b) This set is not functionally complete. Note first that $\overline{(x\oplus y)} = \overline{x}\oplus y$. Thus every expression involving these two operations and x and y can be reduced to an *XOR* of the literals x, $\overline{x}$, y, and $\overline{y}$. Note that $\oplus$ is commutative and associative, so that we can rearrange such expressions to group things conveniently. Also, since $x\oplus x = 0$, $x\oplus\overline{x} = 1$, $x\oplus 1 = \overline{x}$ and $x\oplus 0 = x$, and similarly for y (see Exercise 24 in Section 12.1), we can reduce all such expressions to one of the expressions 0, 1, x, y, $\overline{x}$, $\overline{y}$, $x\oplus y$, $x\oplus\overline{y}$, $\overline{x}\oplus y$, or $\overline{x}\oplus\overline{y}$. Since none of these has the same table of values as $x+y$, we conclude that the set is not functionally complete.

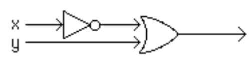
c) This is similar to part **(a)**. This time we note that $0\cdot 0 = 0\oplus 0 = 0$. Again this means that every function that uses only these two operations must have the value 0 when the inputs are all 0. Therefore using only these two operations, we cannot construct the Boolean function that is 1 for all inputs.

SECTION 12.3 Logic Gates

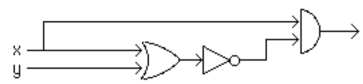
2. The inputs to the AND gate are $\overline{x}$ and $\overline{y}$. The output is then passed through the inverter. Therefore the final output is $\overline{(\overline{x}\,\overline{y})}$. Note that there is a simpler way to form a circuit equivalent to this one, namely $x+y$.

4. This is similar to the previous three exercises. The output is $\overline{(\overline{x}\,y\,z)}(\overline{x}+y+\overline{z})$.

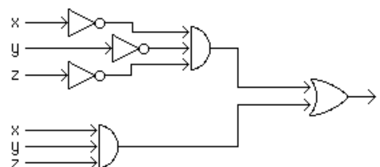
6. We build these circuits up exactly as the expressions are built up. In part **(b)**, for example, we use an AND gate to join the outputs of the inverter (which was applied to the output of the OR gate applied to x and y) and x.



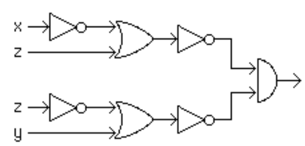
(a)



(b)

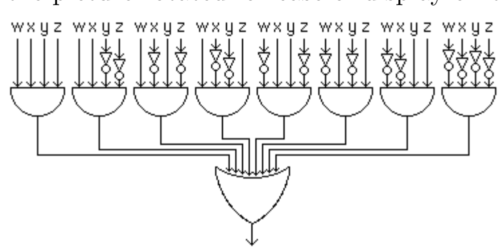


(c)

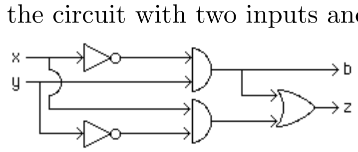


(d)

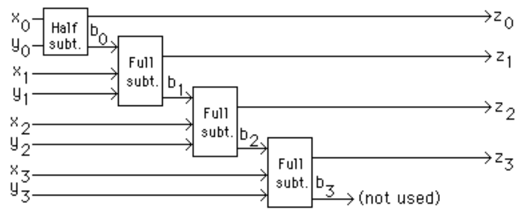
8. In analogy to the situation with three switches in Example 3, we write down the expression we want the circuit to implement: $w\,x\,y\,z + w\,x\,\overline{y}\,\overline{z} + w\,\overline{x}\,y\,\overline{z} + w\,\overline{x}\,\overline{y}\,z + \overline{w}\,x\,y\,\overline{z} + \overline{w}\,x\,\overline{y}\,z + \overline{w}\,\overline{x}\,y\,z + \overline{w}\,\overline{x}\,\overline{y}\,\overline{z}$. The circuit will have 32 inputs, combined by AND gates in groups of four, with inverters where necessary, to produce outputs corresponding to the eight minterms in this expression. These outputs are combined with one big OR gate. The circuit is shown below, with the picture rotated for ease of display on the page.



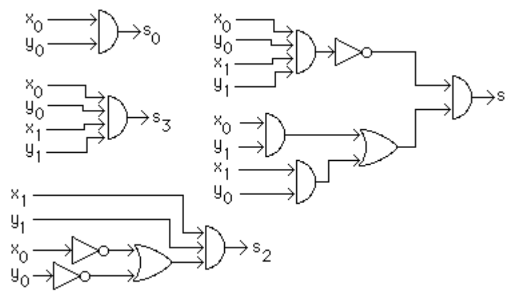
10. First we must determine what the outputs are to be. Let x and y be the input bits, where we want to compute $x-y$. There are two outputs: the difference bit z and the borrow bit b. The borrow will be 1 if a borrow is necessary, which happens only when $x=0$ and $y=1$. Thus $b=\overline{x}\,y$. The difference bit will be 1 when $x=1$ and $y=0$, and when $x=0$ and $y=1$; and it will be 0 in the cases in which $x=y$. Therefore we have $z=\overline{x}\,y+x\,\overline{y}$, which is the same as $b+x\,\overline{y}$. Thus we can draw the half subtractor as shown below. In analogy with Figure 8, we represent the circuit with two inputs and two outputs.



12. We need to combine half subtractors and full subtractors in much the same way that half adders and full adders were combined to produce a circuit to add binary numbers. The first bit of the answer (z_0) is the difference bit between the first two bits of the input (x_0 and y_0), obtained using the half subtractor. The borrow bit output from the half subtractor (b_0) is then the borrow bit input to the full subtractor for determining the second bit of the answer, and so on. Note that the final borrow b_3 must be 0 and is not used.



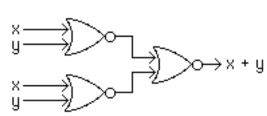
14. Let $(s_3 s_2 s_1 s_0)_2$ be the product. We need to write down Boolean expressions for each of these bits. Clearly $s_0 = x_0\, y_0$. The bit s_1 is a 1 if one, but not both, of the products $x_0\, y_1$ and $x_1\, y_0$ are 1. Therefore we have $s_1 = (x_0\, y_1 + x_1\, y_0)\overline{(x_0\, x_1\, y_0\, y_1)}$. A similar analysis will show that $s_2 = x_1\, y_1\,(\overline{x}_0 + \overline{y}_0)$, and that $s_3 = x_0\, x_1\, y_0\, y_1$. The circuit we want has one circuit for each of these bits.



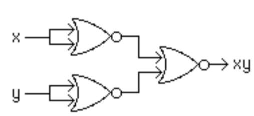
16. The answers here are duals to the answers for Exercise 15. Note that the usual symbol $\downarrow$ represents the *NOR* operation.

a) The circuit is the same as in Exercise 15a, with a NOR gate in place of a NAND gate, since $\overline{x} = x \mid x = x \downarrow x$.

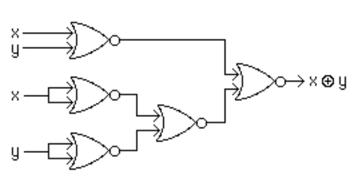
b) Since $x + y = (x \downarrow y) \downarrow (x \downarrow y)$, the answer is as shown.



c) Since $xy = (x \downarrow x) \downarrow (y \downarrow y)$, the answer is as shown.



d) We use the representation $x \oplus y = (x + y)\overline{(xy)} = \overline{(\overline{(x+y)} + x\,y)} = (x \downarrow y) \downarrow (xy) = (x \downarrow y) \downarrow ((x \downarrow x) \downarrow (y \downarrow y))$, obtaining the following circuit.



18. We know that the sum bit in the half adder is $s = x \oplus y = x\overline{y} + \overline{x}y$. The answer to Exercise 16d shows precisely this gate constructed from NOR gates, so it gives us this part of the answer. Also, the carry bit in the half adder is $c = xy$. The answer to Exercise 16c shows precisely this gate constructed from NOR gates, so it gives us this part of the answer.

20. **a)** The initial inputs have depth 0. Therefore the three AND gates all have depth 1, as do their outputs. Therefore the OR gate has depth 2, which is the depth of the circuit.

b) The AND gate at the top of Figure 6 and the two inverters have depth 1, so the AND gate at the bottom has depth 2. Therefore the inputs to the OR gate have depth 1 or 2, so its depth is 3 (one more than the maximum of these), which is the depth of the circuit.

c) The maximum of the depths of the gates is 3, for the final AND gate, since the inverter feeding it has depth 2. Therefore the depth of the circuit is 3.

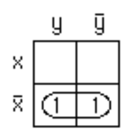
d) We have to be careful here, since the outputs of the half-adder are 3 for the sum but 1 for the carry. So the depth of the half adder at the top of this full adder is 6 for its sum output and 4 for its carry output. The carry output goes through one more gate, giving a total depth of 5 for the OR gate, but the depth of the circuit is 6, because of the output at the upper right.

SECTION 12.4 Minimization of Circuits

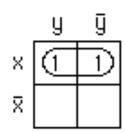
2. We just write down the minterms for which there is a 1 in the corresponding box, and join them with $+$.

a) $xy + \overline{x}y + \overline{x}\,\overline{y}$ **b)** $xy + x\overline{y}$ **c)** $xy + x\overline{y} + \overline{x}y + \overline{x}\,\overline{y}$

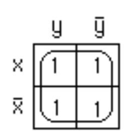
4. **a)** The K-map is shown here. The two 1's combine into the larger block representing the expression $\overline{x}$. Therefore the answer is $\overline{x}$.



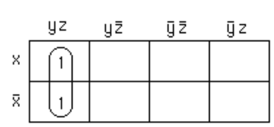
b) The K-map is as shown here. The two 1's combine into the larger block representing the expression x. Therefore the answer is x.



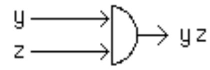
c) All four 1's combine to form the larger block which represents the term 1; this is the answer.



6. **a)** The function is already presented in its sum-of-products form, so we easily draw the following K-map.



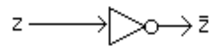
The grouping shown here tells us that the simplest Boolean expression is just yz. Therefore the circuit shown below answers this exercise.



b) This is similar to part **(a)**. The K-map is as shown here.

	yz	$y\overline{z}$	$\overline{y}\,\overline{z}$	$\overline{y}z$
x		1	1	
$\overline{x}$		1	1	

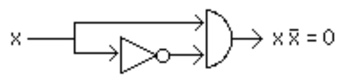
One large block suffices, so the simplest Boolean expression is just $\overline{z}$. Therefore the circuit shown below answers this exercise.



c) First we must put the expression in its sum-of-products form, by "multiplying out." We have

$$\begin{aligned}\overline{x}\,y\,z\,\big((x+\overline{z})+(\overline{y}+\overline{z})\big) &= \overline{x}\,y\,z\,(x+\overline{y}+\overline{z})\\ &= \overline{x}\,x\,y\,z+\overline{x}\,y\,\overline{y}\,z+\overline{x}\,y\,z\,\overline{z}\\ &= 0+0+0=0\,.\end{aligned}$$

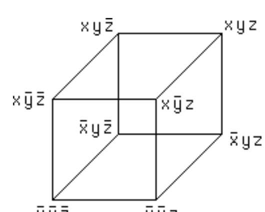
This tells us that the circuit always has the output 0. In some sense the simplest circuit is the one with no gates, but if we insist on using some gates, then we can use the fact that $x\,\overline{x}=0$ and construct the following circuit.



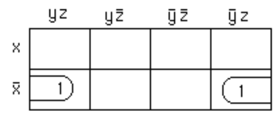
8. In the figure below we have drawn the K-map. For example, since one of the terms was xz, we put a 1 in each cell whose address contained x and z. Note that this meant two cells, one for y and one for $\overline{y}$. Each cell with a 1 in it is an implicant, as are the pairs of cells that form blocks, namely xy, xz, and yz. Since each cell by itself is contained in a block with two cells, none of them is prime. Each of the mentioned blocks with two cells is prime, since none is contained in a larger block. Furthermore, each of these blocks is essential, since each contains a cell that no other prime implicant contains: xy contains $xy\overline{z}$, xz contains $x\overline{y}z$, and yz contains $\overline{x}yz$.

	yz	$y\overline{z}$	$\overline{y}\,\overline{z}$	$\overline{y}z$
x	1	1		1
$\overline{x}$	1			

10. The figure below shows the 3-cube Q_3, labeled as requested. Compare with Figure 1 in Section 12.1. A complemented Boolean variable corresponds to 0, and an uncomplemented Boolean variable corresponds to 1. The top face 2-cube corresponds to x, since all of its vertices are labeled x. Similarly, the back face 2-cube represents y, and the right face 2-cube represents z. The opposing faces—bottom, front, and left—represent $\overline{x}$, $\overline{y}$, and $\overline{z}$, respectively.

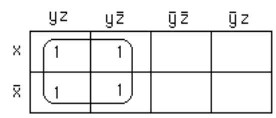


12. In each case the K-map is shown, together with all the maximal groupings and the minimal expansion. Note that in parts **(c)** and **(d)** the answer is not unique, since there is more than one minimal covering of all the squares with 1's in them.



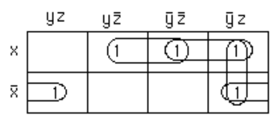
$\bar{x}z$

(a)



y

(b)

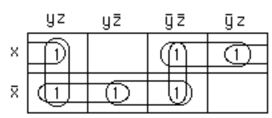


$\bar{x}z + x\bar{z} + x\bar{y}$

OR

$\bar{x}z + x\bar{z} + \bar{y}z$

(c)



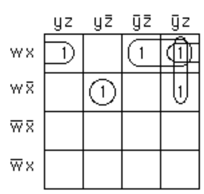
$yz + \bar{x}\bar{z} + x\bar{y}$

OR

$xz + \bar{x}y + \bar{y}\bar{z}$

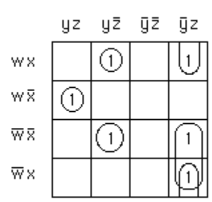
(d)

14. In each case the K-map is shown, together with the grouping that gives the answer, and the minimal expansion.



$w\bar{x}y\bar{z} + wxz + wx\bar{y} + w\bar{y}z$

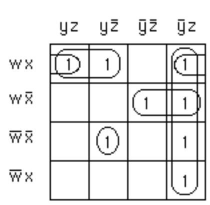
(a)



$wxy\bar{z} + w\bar{x}yz + \bar{w}\bar{x}y\bar{z} +$

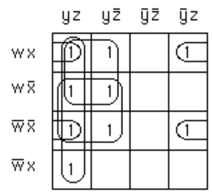
$+ \bar{w}\bar{y}z + x\bar{y}z$

(b)



$\bar{y}z + w\bar{x}\bar{y} + wxy + \bar{w}\bar{x}y\bar{z}$

(c)



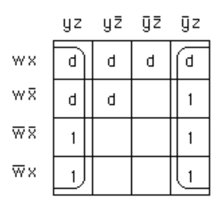
$yz + \overline{x}y + wy + wxz + \overline{w}\,\overline{x}z$

(d)

16. To represent x_1, we need to use half the cells—half correspond to x_1 and half correspond to $\overline{x}_1$. Since there are $2^6 = 64$ cells in all, we need to use $2^5 = 32$ of them. In fact, the general statement (made formal in Exercise 33 below) is that a term that involves k literals corresponds to an $(n-k)$-dimensional subcube of the n-cube, and so will have 1's in 2^{n-k} cells. Thus we see that $\overline{x}_1 x_6$ needs $2^{6-2} = 16$ cells, $\overline{x}_1 x_2 \overline{x}_6$ needs $2^{6-3} = 8$ cells, $x_2 x_3 x_4 x_5$ needs $2^{6-4} = 4$ cells, and $x_1 \overline{x}_2 x_4 \overline{x}_5$ also needs 4 cells.

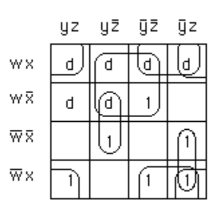
18. See the K-map shown for five variables given in the solution for Exercise 15. Minterms that differ only in their treatment of x_1 are adjacent cells in the second and third rows, or in the top and bottom rows (which are to be considered adjacent). Minterms that differ only in their treatment of x_2 are adjacent cells in the first and second rows, or in the third and fourth rows. Minterms that differ only in their treatment of x_3 are adjacent cells in the fourth and fifth columns, or in the first and eighth columns (which are to be considered adjacent), or in the second and seventh columns (which are to be considered adjacent), or in the third and sixth columns (which are to be considered adjacent). Minterms that differ only in their treatment of x_4 are adjacent cells in the second and third columns, or in the sixth and seventh columns, or in the first and fourth columns (which are to be considered adjacent), or in the fifth and eighth columns (which are to be considered adjacent). Minterms that differ only in their treatment of x_5 are adjacent cells in the first and second columns, or in the third and fourth columns, or in the fifth and sixth columns, or in the seventh and eighth columns.

20. In each case we draw the K-map, with the required squares marked by a 1 and the don't care conditions marked with a d. The required expansion is shown.



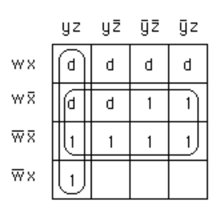
z

(a)



$w\overline{z} + x\overline{y} + xz + \overline{x}y\overline{z} + \overline{w}\,\overline{y}z$

(b)



$\overline{x} + yz$

(c)

22. We organize our work as in the text.

a)

			Step 1	
	Term	String	Term	String
1	$x\,y\,\overline{z}$	110	$(1,3)\,x\,\overline{z}$	1−0
2	$\overline{x}\,y\,z$	011	$(3,4)\,\overline{y}\,\overline{z}$	−00
3	$x\,\overline{y}\,\overline{z}$	100		
4	$\overline{x}\,\overline{y}\,\overline{z}$	000		

The products in the last column, together with minterm #2, are the products that are to be used to cover the four minterms. Each is required: $x\,\overline{z}$ to cover minterm #1, $\overline{y}\,\overline{z}$ to cover minterm #4, and minterm #2 to cover itself. Therefore the answer is $x\,\overline{z}+\overline{y}\,\overline{z}+\overline{x}\,y\,z$.

b)

			Step 1		Step 2	
	Term	String	Term	String	Term	String
1	$x\,\overline{y}\,z$	101	$(1,3)\,x\,\overline{y}$	10−	$(1,3,4,5)\,\overline{y}$	−0−
2	$\overline{x}\,y\,z$	011	$(1,4)\,\overline{y}\,z$	−01		
3	$x\,\overline{y}\,\overline{z}$	100	$(2,4)\,\overline{x}\,z$	0−1		
4	$\overline{x}\,\overline{y}\,z$	001	$(3,5)\,\overline{y}\,\overline{z}$	−00		
5	$\overline{x}\,\overline{y}\,\overline{z}$	000	$(4,5)\,\overline{x}\,\overline{y}$	00−		

The product $\overline{y}$ in the last column covers all the minterms except #2, and the third product in Step 1 ($\overline{x}\,z$) covers it. Thus the answer is $\overline{y}+\overline{x}\,z$.

c)

			Step 1		Step 2	
	Term	String	Term	String	Term	String
1	$x\,y\,z$	111	$(1,2)\,x\,y$	11−	$(1,2,3,5)\,x$	1−−
2	$x\,y\,\overline{z}$	110	$(1,3)\,x\,z$	1−1	$(1,3,4,6)\,z$	−−1
3	$x\,\overline{y}\,z$	101	$(1,4)\,y\,z$	−11	$(3,5,6,7)\,\overline{y}$	−0−
4	$\overline{x}\,y\,z$	011	$(2,5)\,x\,\overline{z}$	1−0		
5	$x\,\overline{y}\,\overline{z}$	100	$(3,5)\,x\,\overline{y}$	10−		
6	$\overline{x}\,\overline{y}\,z$	001	$(3,6)\,\overline{y}\,z$	−01		
7	$\overline{x}\,\overline{y}\,\overline{z}$	000	$(4,6)\,\overline{x}\,z$	0−1		
			$(5,7)\,\overline{y}\,\overline{z}$	−00		
			$(6,7)\,\overline{x}\,\overline{y}$	00−		

All three products in the last column are necessary and sufficient to cover the minterms. Sufficiency is seen by noticing that all the numbers from 1 to 7 are included in the 4-tuples for these terms. Necessity is seen by noticing that only the first of them covers #2, only the second covers #4, and only the third covers #7. Thus the answer is $x+\overline{y}+z$.

d)

			Step 1	
	Term	String	Term	String
1	$x\,y\,\overline{z}$	110	$(1,2)\,x\,\overline{z}$	1−0
2	$x\,\overline{y}\,\overline{z}$	100	$(3,4)\,\overline{x}\,\overline{y}$	00−
3	$\overline{x}\,\overline{y}\,z$	001		
4	$\overline{x}\,\overline{y}\,\overline{z}$	000		

Clearly both products in the last column are necessary and sufficient to cover the minterms. Thus the answer is $x\,\overline{z}+\overline{x}\,\overline{y}$.

24. We follow the procedure and notation given in the text.

a)

	Term	String	Step 1 Term	Step 1 String
1	$w\,x\,y\,z$	1111	$(1,2)\,w\,x\,y$	111−
2	$w\,x\,y\,\overline{z}$	1110	$(1,3)\,w\,y\,z$	1−11
3	$w\,\overline{x}\,y\,z$	1011	$(2,4)\,w\,x\,\overline{z}$	11−0
4	$w\,x\,\overline{y}\,\overline{z}$	1100	$(3,5)\,w\,\overline{x}\,z$	10−1
5	$w\,\overline{x}\,\overline{y}\,z$	1001	$(3,7)\,\overline{x}\,y\,z$	−011
6	$\overline{w}\,x\,\overline{y}\,z$	0101	$(4,8)\,w\,\overline{y}\,\overline{z}$	1−00
7	$\overline{w}\,\overline{x}\,y\,z$	0011	$(5,8)\,w\,\overline{x}\,\overline{y}$	100−
8	$w\,\overline{x}\,\overline{y}\,\overline{z}$	1000	$(7,9)\,\overline{w}\,\overline{x}\,y$	001−
9	$\overline{w}\,\overline{x}\,y\,\overline{z}$	0010		

The eight products in the last column as well as minterm #6 are possible products in the desired expansion, since they are not contained in any other product. We make a table of which products cover which of the original minterms.

	1	2	3	4	5	6	7	8	9
$w\,x\,y$	X	X							
$w\,y\,z$	X		X						
$w\,x\,\overline{z}$		X		X					
$w\,\overline{x}\,z$			X		X				
$\overline{x}\,y\,z$			X				X		
$w\,\overline{y}\,\overline{z}$				X				X	
$w\,\overline{x}\,\overline{y}$					X			X	
$\overline{w}\,\overline{x}\,y$							X		X
$\overline{w}\,x\,\overline{y}\,z$						X			

Since only the last of these terms covers minterm #6, it must be included. Similarly, the next to last product must be included, since it is the only one that covers minterms #9. At this point no other minterm is covered by a unique product, so we have to figure out a minimum covering. There are six minterms left to be covered, and each product covers only two of them. Therefore we need at least three products. In fact three products will suffice, if, for instance, we take the first, fourth, and sixth rows. Therefore one possible answer is $w\,x\,y + w\,\overline{x}\,z + w\,\overline{y}\,\overline{z} + \overline{w}\,\overline{x}\,y + \overline{w}\,x\,\overline{y}\,z$.

b)

	Term	String	Step 1 Term	Step 1 String	Step 2 Term	Step 2 String
1	$w\,\overline{x}\,y\,z$	1011	$(1,3)\,w\,\overline{x}\,y$	101−	$(2,4,5,7)\,\overline{y}\,\overline{z}$	−−00
2	$w\,x\,\overline{y}\,\overline{z}$	1100	$(2,4)\,w\,\overline{y}\,\overline{z}$	1−00	$(3,4,6,7)\,\overline{x}\,\overline{z}$	−0−0
3	$w\,\overline{x}\,y\,\overline{z}$	1010	$(2,5)\,x\,\overline{y}\,\overline{z}$	−100		
4	$w\,\overline{x}\,\overline{y}\,\overline{z}$	1000	$(3,4)\,w\,\overline{x}\,\overline{z}$	10−0		
5	$\overline{w}\,x\,\overline{y}\,\overline{z}$	0100	$(3,6)\,\overline{x}\,y\,\overline{z}$	−010		
6	$\overline{w}\,\overline{x}\,y\,\overline{z}$	0010	$(4,7)\,\overline{x}\,\overline{y}\,\overline{z}$	−000		
7	$\overline{w}\,\overline{x}\,\overline{y}\,\overline{z}$	0000	$(5,7)\,\overline{w}\,\overline{y}\,\overline{z}$	0−00		
			$(6,7)\,\overline{w}\,\overline{x}\,\overline{z}$	00−0		

The two products in the last column, as well as the first product in Step 1 are possible products in the desired expansion, since they are not contained in any other product. Furthermore they are necessary and sufficient to cover all the minterms (they are necessary because of minterms #2, #6, and #1, respectively). Therefore the answer is $\overline{y}\,\overline{z} + \overline{x}\,\overline{z} + w\,\overline{x}\,y$.

c) This problem requires three steps, rather than just two, and there is not enough room across the page to show all the work. Suffice it to say that there are 11 minterms, 16 products of three literals, 7 products of two literals, and one "product" of one literal, namely $\overline{z}$. The products that are not superseded by other products are $\overline{z}$, $\overline{w}\,x$, and $w\,\overline{x}\,y$, and all of them are necessary and sufficient to cover the literals. Therefore the answer is $\overline{z} + \overline{w}\,x + w\,\overline{x}\,y$.

26. We use the same picture as for the sum-of-products expansion with three variables, except that the labels across the top are sums, rather than products: $y+z$, $y+\overline{z}$, $\overline{y}+\overline{z}$, and $\overline{y}+z$. We put a 0 in each square that corresponds to a maxterm in the expansion. For example, if the maxterm $x+y+z$ is present, we put a 0 in the upper left-hand corner. Then we combine the squares to produce larger blocks, exactly as in the usual K-map procedure. The product of enough corresponding sums to cover all the 0's is the desired product-of-sums expansion. See the solution to Exercise 27 for a worked example.

28. It would be hard to see the picture in three-dimensional perspective, so we content ourselves with a planar view. The usual drawing (see Figure 8) *is* a torus, if we think of the left-hand edge as wrapped around and glued to the right-hand edge, and simultaneously the top edge wrapped around and glued to the bottom edge.

30. We need to find blocks that cover all the 1's, and we do not care whether the d's are covered. It is clear that we want to include a large rectangular block covering the entire middle two columns of the K-map; its minterm is $\overline{z}$. The only other 1 needing coverage is in the upper right-hand corner, and the largest block covering it would be the entire first row, whose minterm is $w\,x$. Therefore the answer is $\overline{z}+w\,x$. It happened that all the d's were covered as well.

32. We need to find blocks that cover all the 1's, and we do not care whether the d's are covered. The best way to cover the 1's in the bottom row is to take the entire bottom row, whose minterm is $\overline{w}\,x$. To cover the remaining 1's, the largest block would be the upper right-hand quarter of the diagram, whose minterm is $w\,\overline{y}$. Therefore the minimal sum-of-products expansion is $\overline{w}\,x + w\,\overline{y}$. It did not matter that some of the d's remained uncovered.

SUPPLEMENTARY EXERCISES FOR CHAPTER 12

2. **a)** If $z=0$, then the equation is the true statement $0=0$, independent of x and y. Hence the answer is no.
b) This is dual to part **(a)**, so the answer is again no (take $z=1$ this time).
c) Here the answer is yes. If we take this equation and take the exclusive *OR* of both sides with z, then, since $z \oplus z = 0$ and $s \oplus 0 = s$ for all s, the equation reduces to $x=y$.
d) If we take $z=1$, then both sides equal 0, so the answer is no.
e) This is dual to part **(d)**, so again the answer is no.

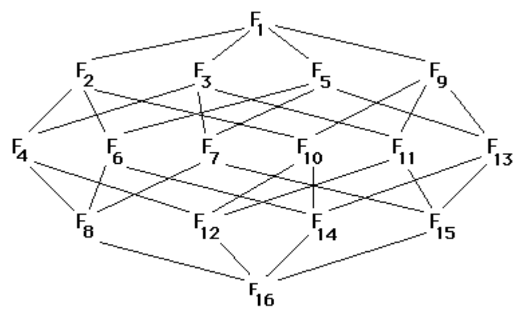
4. A simple example is the function $F(x,y,z)=x$. Indeed $\overline{F(\overline{x},\overline{y},\overline{z})} = \overline{\overline{x}} = x = F(x,y,z)$.

6. **a)** Since $x+y$ is certainly 1 whenever $x=1$, we see that $F \le G$. Clearly the reverse relationship does not hold, since we could have $x=0$ and $y=1$.
b) If $G(x,y)=1$, then necessarily $x=y=1$, whence $F(x,y)=1+1=1$. Thus $G \le F$. It is not true that $F \le G$, since we can take $x=1$ and $y=0$.
c) Neither $F \le G$ nor $G \le F$ holds. For the first, take $x=y=0$, and for the second take $x=y=1$.

8. First suppose that $F+G \le H$. We must show that $F \le H$ and $G \le H$. By symmetry it is enough to show that $F \le H$. So suppose that $F(x_1,\ldots,x_n)=1$. Then clearly $(F+G)(x_1,\ldots,x_n)=1$ as well. Now since we are given $F+G \le H$, we conclude that $H(x_1,\ldots,x_n)=1$, as desired.

For the converse, assume that $F \leq H$ and $G \leq H$. We want to show that $F + G \leq H$. Suppose that $(F+G)(x_1,\ldots,x_n) = 1$. This means that either $F(x_1,\ldots,x_n) = 1$ or $G(x_1,\ldots,x_n) = 1$. In either case, by the assumption we conclude that $H(x_1,\ldots,x_n) = 1$, and the proof is complete.

10. The picture is the 4-cube.



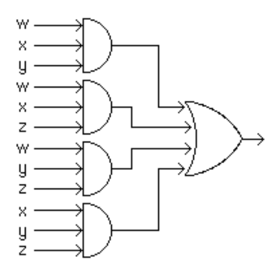
12. From the definition, it is obvious that the value is 1 if and only if either x and y are both 1 or x and y are both 0. This is exactly what $x\,y + \overline{x}\,\overline{y}$ says, so the identity holds.

14. **a)** This is clear from looking at the definition in the two cases $x = 0$ and $x = 1$.
b) This is clear from looking at the definition in the two cases $x = 0$ and $x = 1$.
c) This is clear from the symmetry of the definition.

16. It is not functionally complete. Every expression involving just x and the operator must have the value 1 when $x = 1$; thus we cannot achieve $\overline{x}$ with just this operator.

18. **a)** The first XOR gate has input $\overline{x}$ and y, so its output is $\overline{x} \oplus y$. Thus the output of the entire circuit is $(\overline{x} \oplus y) \oplus x$. Note that by the properties of $\oplus$, this simplifies to $1 \oplus y = \overline{y}$.
b) This is similar to part **(a)**. The answer is $((x \oplus y) \oplus (\overline{x} \oplus z)) \oplus (\overline{y} \oplus \overline{z})$, which simplifies to 1.

20. We use four AND gates, the outputs of which are joined by an OR gate.



22. In each case we need to give the weights and the threshold.
a) Let the weight on x be -1, and let the threshold be $-1/2$. If $x = 1$, then the value is -1, which is not greater than the threshold; if $x = 0$, then the value is 0, which is greater than the threshold. Thus the value is greater than the threshold if and only if $\overline{x} = 1$.
b) We can take the weights on x and y to be 1 each, and the threshold to be $1/2$. Then the weighted sum is greater than the threshold if and only if $x = 1$ or $y = 1$, as desired.
c) We can take the weights on x and y to be 1 each, and the threshold to be $3/2$. Then the weighted sum is greater than the threshold if and only if $x = y = 1$, as desired.
d) We can take the weights on x and y to be -1 each, and the threshold to be $-3/2$. Then the weighted sum is greater than the threshold if and only if $x = 0$ or $y = 0$, as desired.

e) We can take the weights on x and y to be -1 each, and the threshold to be $-1/2$. Then the weighted sum is greater than the threshold if and only if $x = y = 0$, as desired.

f) In this case we can take the weight on x to be 2, and the weights on y and z to be 1 each. The threshold is $3/2$. In order for the weighted sum to be greater than the threshold, we need either $x = 1$ or $y = z = 1$, which is precisely what we need for $x + yz$ to have the value 1.

g) This is similar to part **(f)**. Take the weights on w, x, y, and z to be 2, 1, 1, and 2, respectively, and the threshold to be $3/2$.

h) Note that the function is equivalent to $xz(w + \overline{y})$. Thus we want weights and a threshold that requires x and z to be 1 in order to get past the threshold, but in addition requires either $w = 1$ or $y = 0$. A little thought will convince one that letting the weights on x and z be 1, the weight on w be $1/2$, and the weight on y be $-1/2$ will do the job, if the threshold is $9/4$.

24. We prove this by contradiction, assuming that this is a threshold function. Suppose that the weights on w, x, y, and z are a, b, c, and d, respectively, and let the threshold be T. Since $w = x = 1$ and $y = z = 0$ gives a value of 1, we need $a + b \geq T$. Similarly we need $c + d \geq T$. On the other hand, since $w = y = 1$ and $x = z = 0$ gives a value of 0, we need $a + c < T$. Similarly we need $b + d < T$. Adding the first two inequalities shows that $a + b + c + d \geq 2T$; adding the last two shows that $a + b + c + d < 2T$. This contradiction tells us that $wx + yz$ is not a threshold function.

CHAPTER 13
Modeling Computation

SECTION 13.1 Languages and Grammars

2. There are of course a large number of possible answers. Five of them are *the sleepy hare runs quickly*, *the hare passes the tortoise*, *the happy hare runs slowly*, *the happy tortoise passes the hare*, and *the hare passes the happy hare*.

4. **a)** It suffices to give a derivation of this string. We write the derivation in the obvious way. $S \Rightarrow 1S \Rightarrow 11S \Rightarrow 111S \Rightarrow 11100A \Rightarrow 111000$.

b) Every production results in a string that ends in S, A, or 0. Therefore this string, which ends with a 1, cannot be generated.

c) Notice that we can have any number of 1's at the beginning of the string (including none) by iterating the production $S \to 1S$. Eventually the S must turn into $00A$, so at least two 0's must come next. We can then have as many 0's as we like by using the production $A \to 0A$ repeatedly. We must end up with at least one more 0 (and therefore a total of at least three 0's) at the right end of the string, because the A disappears only upon using $A \to 0$. So the language generated by G is the set of all strings consisting of zero or more 1's followed by three or more 0's. We can write this as $\{\, 0^n 1^m \mid n \geq 0 \text{ and } m \geq 3 \,\}$.

6. **a)** There is only one terminal string possible here, namely $abbb$. Therefore the language is $\{abbb\}$.

b) This time there are only two possible strings, so the answer is $\{aba, aa\}$.

c) Note that A must eventually turn into ab. Therefore the answer is $\{abb, abab\}$.

d) If the rule $S \to AA$ is applied first, then the string that results must be N a's, where N is an even number greater than or equal to 4, since each A becomes a positive even number of a's. If the rule $S \to B$ is applied first, then a string of one or more b's results. Therefore the language is $\{\, a^{2n} \mid n \geq 2 \,\} \cup \{\, b^n \mid n \geq 1 \,\}$.

e) The rules imply that the string will consist of some a's, followed by some b's, followed by some more a's ("some" might be none, though). Furthermore, the total number of a's equals the total number of b's. Thus we can write the answer as $\{\, a^n b^{n+m} a^m \mid m, n \geq 0 \,\}$.

8. If we apply the rule $S \to 0S1$ n times, followed by the rule $S \to \lambda$, then the string $0^n 1^n$ results. On the other hand, no other derivations are possible, since once the rule $S \to \lambda$ is used, the derivation stops. This proves the given statement.

10. **a)** It follows by induction that unless the derivation has stopped, the string generated by any sequence of applications of the rules must be of the form $0^n S 1^m$ for some nonnegative integers n and m. Conversely, every string of this form can be obtained. Since the only other rule is $S \to \lambda$, the only terminal strings generated by this grammar are $0^n 1^m$.

b) A derivation consists of some applications of the rules until the S disappears, followed, perhaps, by some more applications of the rules. First let us see what can happen up to the point at which the S disappears. The first rule adds 0's to the left of the S. The last rule makes the S disappear, whereas rules two and three turn the S into $1A$ or 1. Therefore the possible strings generated at the point the S disappears are 0^n, 0^n1, and 0^n1A, where n is a nonnegative integer. By rules four and five, the A eventually turns into one or more 1's. Therefore the possible strings are 0^n1^m for nonnegative integers n and m.

12. By following the pattern given in the solution to Exercise 11, we can certainly generate all the strings $0^n1^n2^n$, for $n \geq 0$. We must show that no other terminal strings are possible. First, the number of 0's, A's, and B's must be equal at the point at which S disappears, with all the 0's on the left (where they must stay). The rule $BA \to BA$ tells us the A's can only move left across the B's, not conversely. Furthermore, A's turn into 1's, but only if connected by 1's to a 0; therefore the only way to get rid of the A's is for them all to move to the left of the B's and then turn into 1's. Finally, the B's can only turn into 2's, and they are all on the right.

14. In each case we will list only the productions, because V and T will be obvious from the context, and S speaks for itself.

a) For this finite set of strings, we can simply have $S \to 10$, $S \to 01$, and $S \to 101$.

b) To get started we can have $S \to 00A$; this gives us the two 0's at the start of each string in the language. After that we can have anything we want in the middle, so we want $A \to 0A$ and $A \to 1A$. Finally we insist on ending with a 1, so we have $A \to 1$.

c) The even number of 1's can be accomplished with $S \to 11S$, and the final 0 tells us to include $S \to 0$ as the only other production. Note that zero is an even number, so the string 0 is in the language.

d) If there are not two consecutive 0's or two consecutive 1's, the symbols must alternate. We can accomplish this by having an optional 0 to start, then any number of repetitions of 10, and then an optional 1 at the end. One way to do this is with these productions: $S \to ABC$, $A \to 0$, $A \to \lambda$, $B \to 10B$, $B \to \lambda$, $C \to 1$, $C \to \lambda$.

16. In each case we will list only the productions, because V and T will be obvious from the context, and S speaks for itself.

a) It suffices to have $S \to 1S$ and $S \to \lambda$.

b) We let A represent the string of 0's. Thus we take $S \to 1A$, $A \to 0A$, and $A \to \lambda$. (Here $A \to A0$ works just as well as $A \to 0A$, so either one is fine.)

c) It suffices to have $S \to 11S$ and $S \to \lambda$.

18. **a)** We want exactly one 0 and an even number of 1's to its right. Thus we can use the rules $S \to 0A$, $A \to 11A$, and $A \to \lambda$.

b) We can have the new symbols grow out from the center, using the rules $S \to 0S11$ and $S \to \lambda$.

c) We can have the 0's grow out from the center, and then have the center turn into a 1-making machine. The rules we propose are $S \to 0S0$, $S \to A$, $A \to 1A$, and $A \to \lambda$.

20. We can simply have identical symbols grow out from the center, with an optional final symbol in the center itself. Thus we use the rules $S \to 0S0$, $S \to 1S1$, $S \to \lambda$, $S \to 0$, and $S \to 1$. Note that this grammar is context-free since each left-hand side is a single nonterminal symbol.

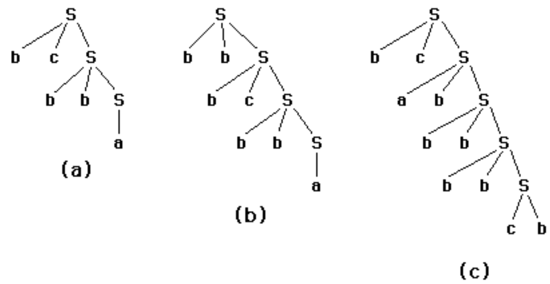
22. **a)** The string is the leaves of the tree, read from left to right. Thus the string is "a large mathematician hops wildly."

b) Again, the string is the leaves from left to right, namely $+987$.

24. **a)** If we look at the beginning of the string, we see that we can use the rule $S \to bcS$ first. Then since the remainder of the string (after the initial bc) starts with bb, we can use the rule $S \to bbS$. Finally, we can use the rule $S \to a$. We therefore obtain the first tree shown below.

b) This is similar to part **(a)**, using three rules to take care of the first six characters, two by two.

c) Again we work two by two from the left, producing the tree shown.



26. a) Since the string starts with a b, we might have either $Baba \Rightarrow baba$ or $Caba \Rightarrow baba$ as the last step in the derivation. The latter looks more hopeful, since the Ca could have come from the rule $A \to Ca$, meaning that the derivation ended $Aba \Rightarrow Caba \Rightarrow baba$. Now we see that since $B \to Ba$ and $B \to b$ are rules, the derivation could have been $S \Rightarrow AB \Rightarrow ABa \Rightarrow Aba \Rightarrow Caba \Rightarrow baba$.

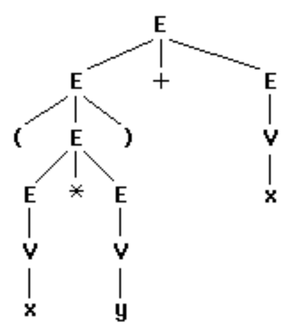
b) There is no way to have obtained an a on the left, since every rule has every a preceded by another symbol (which does not ever turn into λ).

c) This is just like part **(a)**, since we could have used the rule $C \to cb$ instead of the rule $C \to b$, obtaining the extra c on the left. Thus the derivation is $S \Rightarrow AB \Rightarrow ABa \Rightarrow Aba \Rightarrow Caba \Rightarrow cbaba$.

d) The only way for the symbol c to have appeared is through the rule $C \to cb$. Thus we may assume (without loss of generality) that the last step in the derivation was $bbbCa \Rightarrow bbbcba$. Now the only way for Ca to have occurred is from the rule $A \to Ca$. Thus we can assume that the derivation ends $bbbA \Rightarrow bbbCa \Rightarrow bbbcba$. But there is no way for the A to appear at the end (the only rule producing an A puts a B after it). Therefore this string is not in the language.

28. a) We just translate mechanically from the Backus-Naur form to the productions. Let us use E for $\langle expression \rangle$ (which we assume is the starting symbol), and V for $\langle variable \rangle$ for convenience. The rules are $E \to (E)$, $E \to E + E$, $E \to E * E$, and $E \to V$ (from the first form), together with $V \to x$ and $V \to y$ (from the second).

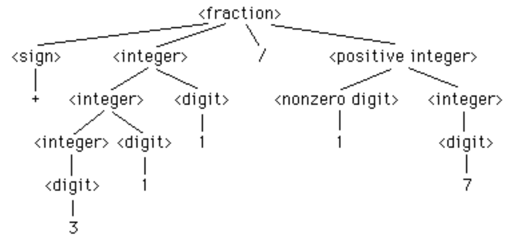
b) The tree is easy to construct. The outermost operation is $+$, so the top part of the tree shows E becoming $E + E$. The right E now is the variable x. The left E is an expression in parentheses, which is itself the product of two variables.



30. a) We first incorporate all the rules from the solution to Exercise 29a except the first two. Then we simply add the rule $S \to \langle sign \rangle \langle integer \rangle / \langle positive\ integer \rangle$.

b) We incorporate all of the solution to Exercise 29b except for the first line, together with a rule $\langle fraction \rangle ::= \langle sign \rangle \langle integer \rangle / \langle positive\ integer \rangle$.

c) The tree practically draws itself from the rules.



32. We ignore the need for spaces between the names, and we assume that names need to be nonempty. We also do not assume anything more than was given in the statement of the exercise.

$\langle person\rangle ::= \langle firstname\rangle\langle middleinitial\rangle\langle lastname\rangle$
$\langle lastname\rangle ::= \langle letterstring\rangle$
$\langle middleinitial\rangle ::= \langle letter\rangle$
$\langle firstname\rangle ::= \langle ucletter\rangle \mid \langle ucletter\rangle letterstring$
$\langle letterstring\rangle ::= \langle letter\rangle \mid \langle letterstring\rangle\langle letter\rangle$
$\langle letter\rangle ::= \langle lcletter\rangle \mid \langle ucletter\rangle$
$\langle lcletter\rangle ::= a \mid b \mid c \mid \ldots \mid z$
$\langle ucletter\rangle ::= A \mid B \mid C \mid \ldots \mid Z$

34. a) Strings in this set consist of one or more letters followed by an optional binary digit, followed by one or more letters. Only the letters a, b, and c are used, however.

b) Strings in this set consist of an optional plus or minus sign followed by one or more digits.

c) Strings in this set consist of any number of letters, followed by any number of binary digits, followed by any number of letters. "Any number" includes 0, so the string could consist of letters only or of binary digits only, and it could also be empty. Only the letters x and y are used, however. Note that $(D+)?$ is equivalent to $D*$.

36. This is straightforward, using the conventions. We assume that the string gives the sandwich from top to bottom. Note that words in roman font are constants here, and words in italics are variables.

sandwich ::= bread *dressing* lettuce?tomato?*meat*+ cheese∗ bread
dressing ::= mustard | mayonnaise
meat ::= turkey | chicken | beef

38. The cosmetic change is to put angled brackets around the variables used for nonterminal symbols. The substantive changes are to replace uses of +, ∗, and ? with rules that have the same effect. For the plus sign, we replace $x+$, where x is a symbol by a new symbol, let's call it $\langle xplus\rangle$, and the new rule

$\langle xplus\rangle ::= x \mid \langle xplus\rangle x$

Similarly, we replace $x*$, where x is a symbol by a new symbol, let's call it $\langle xstar\rangle$, and the new rule

$\langle xstar\rangle ::= \lambda \mid \langle xstar\rangle x$

where λ is the empty string. Finally, we replace each occurrence of $x?$ by a new symbol, let's call it $\langle xquestion\rangle$, and the new rule

$\langle xquestion\rangle ::= \lambda \mid x$

where x is a symbol; and we replace each occurrence of $(junk)?$ by a new symbol, let's call it $\langle junkquestion\rangle$, and the new rule

$\langle junkquestion\rangle ::= \lambda \mid junk$

where *junk* is a string of symbols.

40. This is very similar to the preamble to Exercise 39. The only difference is that the operators are placed between their operands, rather than behind them, and parentheses are required in expressions used as factors. Thus we have the following Backus–Naur form:

$\langle expression \rangle ::= \langle term \rangle \mid \langle term \rangle \langle addOperator \rangle \langle term \rangle$
$\langle addOperator \rangle ::= + \mid -$
$\langle term \rangle ::= \langle factor \rangle \mid \langle factor \rangle \langle mulOperator \rangle \langle factor \rangle$
$\langle mulOperator \rangle ::= * \mid /$
$\langle factor \rangle ::= \langle identifier \rangle \mid (\langle expression \rangle)$
$\langle identifier \rangle ::= a \mid b \mid \cdots \mid z$

42. The definition of "derivable from" says that it is the reflexive, transitive closure of the relation "directly derivable from." Indeed, taking $n = 0$ in that definition gives us the fact that every string is derivable from itself; and the existence of a sequence $w_0 \Rightarrow w_1 \Rightarrow \cdots \Rightarrow w_n$ for $n \geq 1$ means that (w_0, w_n) is in the transitive closure of the relation $\Rightarrow$ (see Theorem 2 in Section 9.4).

SECTION 13.2 Finite-State Machines with Output

2. In each case we need to write down, in a table, all the information contained in the arrows in the diagram. In part **(a)**, for example, there are arrows from state s_1 to s_1 labeled $1, 0$ and from s_1 to s_2 labeled $0, 0$. Therefore the row of our table for this machine that gives the information for transitions from s_1 shows that on input 1 the transition is to state s_1 and the output is 0, and on input 0 the transition is to state s_2 and the output is 0.

a)

	Next State		Output	
State	0	1	0	1
s_0	s_1	s_2	0	1
s_1	s_2	s_1	0	0
s_2	s_2	s_0	1	0

b)

	Next State		Output	
State	0	1	0	1
s_0	s_1	s_2	1	0
s_1	s_0	s_3	1	0
s_2	s_3	s_0	0	0
s_3	s_1	s_2	1	1

c)

	Next State		Output	
State	0	1	0	1
s_0	s_3	s_1	0	1
s_1	s_0	s_1	0	1
s_2	s_3	s_1	0	1
s_3	s_1	s_3	0	0

4. a) The machine starts in state s_0. On input 1 it moves to state s_2 and outputs 0. The next three inputs (all 0's) drive it to s_3, then s_1, then back to s_0, with outputs 011. The final 1 drives it back to s_2 and outputs 0 again. So the output generated is 00110.

b) The machine starts in state s_0. On input 1 it moves to state s_2 and outputs 1. The next three inputs (all 0's) keep it at s_2, outputting 1 each time. The final 1 drives it back to s_0 and outputs 0. So the output generated is 11110.

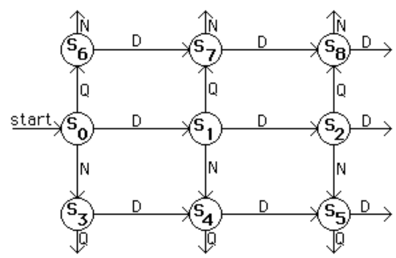
c) The machine starts in state s_0. Since the first input symbol is 1, the machine goes to state s_1 and gives 1 as output. The next input symbol is 0, so the machine moves back to state s_0 and gives 0 as output. The third input is 0, so the machine moves to state s_3 and gives 0 as output. The fourth input is 0, so the machine moves to state s_1 and gives 0 as output. The fifth input is 1, so the machine stays in state s_1 and gives 1 as output. Thus the output is 10001.

6. **a)** The machine starts in state s_0. On input 0 it moves to state s_1 and outputs 1. On the next three inputs it stays in state s_1 and outputs 1. Therefore the output is 1111.

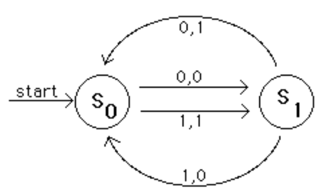
b) The machine starts in state s_0. On input 1 it moves to state s_3 and outputs 0. Then on the next input, which is 0, it moves to state s_1 and outputs 0. The next four moves are to states s_2, s_3, s_0, and s_1, with outputs 1001. Thus the answer is 001001.

c) The idea is the same as in the other parts. The answer is 00110000110.

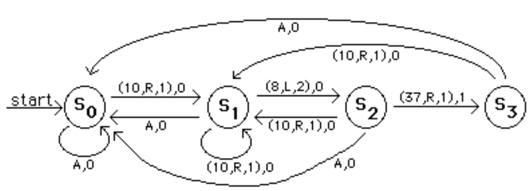
8. We need 9 states. The middle row of states in our picture correspond to no quarters or nickels having been deposited. The top row takes care of the cases in which a nickel has been deposited, and the bottom row handles the cases in which a quarter has been deposited. The columns record the number of dimes (0, 1, or 2). The transitions back to state s_0 are shown as leading off into open space to avoid clutter. Furthermore to avoid clutter we have not drawn six loops, namely loops at states s_3, s_4, and s_5 on input N (since additional nickels are not recorded), and loops at states s_6, s_7, and s_8 on input Q (since additional quarters are not recorded). We do not show the output, since there is none except for all the transitions back to state s_0; there the output is "unlock the door." The letters stand for the obvious coins.



10. We need only two states, since the action depends only on the parity of the number of bits we have read in so far. Transitions from state s_0 to state s_1 are made on the odd-numbered bits, so there we output the same bit as the input. The transitions back to s_0 are made on the even-numbered bits, and there we make the output opposite to the input.



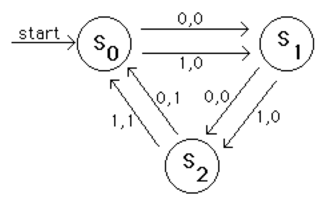
12. To avoid having the machine being too complex, we will keep the model very simple, assuming that the lock opens if and only if the input is $(10, R, 1)(8, L, 2)(37, R, 1)$. In our picture, the "input" A stands for all the inputs other than the inputs shown leading elsewhere. The output 0 means nothing happens; the output U means the lock is unlocked. If we wished to make our model more realistic, we could, for instance, allow the input $(10, R, 1)(8, L, 1)(8, L, 1)(37, R, 1)$ to open the lock, as well as, say, $(10, R, 1)(8, L, 2)(30, R, 1)(37, R, 1)$ (assuming the numbers on the dial are arranged counterclockwise).



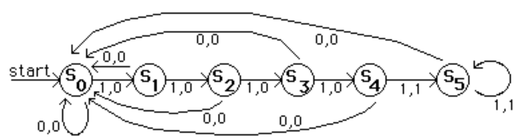
14. The picture for this machine would be a little cumbersome to draw; it has 25 states. Instead, we will describe the machine verbally. We assume that possible inputs are the digits 0 through 9. We will let s_0 be the start state. States s_1, s_2, s_3, and s_4 will be the states reached after the user has entered the successive digits of the correct password, so on the transition from s_3 to s_4, the output is the welcome screen. No output is given for the transitions from s_0 to s_1, from s_1 to s_2, or from s_2 to s_3. States s_{11}, s_{12}, s_{13}, and s_{14} will correspond to wrong digits. Thus there is a transition from s_0 to s_{11} if the first digit is wrong, from s_1 to s_{12} if the second digit is wrong, and so on. There are transitions from s_{11} to s_{12} to s_{13} to s_{14} on all inputs. No output is given for the transitions to s_{11}, s_{12}, or s_{13}. On transition to s_{14} an error message is given.

Now state s_{14} plays the role of s_0, with eight more states to take care of the user's second attempt at a correct password, either terminating in a successful sign-on (say, state s_{104}) or another failure (say, state s_{114}). Then another set of eight states takes care of the third attempt. State s_{214} is the last straw—transitions to it tell the user that the account is locked.

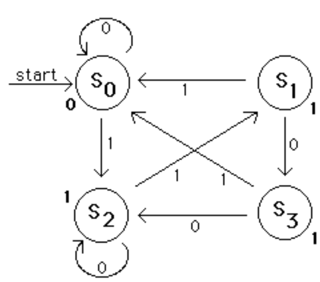
16. We need just three states, to keep track of the remainder when the number of bits read so far is divided by 3. We output 1 when we enter the state s_0 (remainder equals 0).



18. Here we just need to keep track of the number of consecutive 1's most recently encountered.



20. We draw the diagram just as we draw diagrams for finite-state machines with output, except that the transitions are labeled with just an input (since no outputs are associated with the transitions), and each state is labeled with an output. For example, since the table tells us that the output of state s_2 is 1, we write a 1 next to state s_2; and since the transition from state s_3 on input 1 is to state s_0, we draw an arrow from s_3 to s_0 labeled 1.



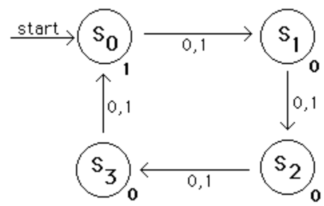
22. Note that the output for a Moore machine is one bit longer than the input: it always starts with the output for state s_0 (which is 0 for this machine).

a) The states that are encountered, after s_0, are s_0, s_2, s_2, and s_1, in that order. Therefore the output is 00111.

b) The states visited are s_2, s_1, s_0, s_2, s_1, s_0, in that order (after the initial state). Therefore the output is 0110110.

c) The procedure is similar to the other parts. The answer is 011001100110.

24. The machine is shown here. Note that state s_i represents the condition that the number of symbols read in so far is congruent to i modulo 4. Thus we make the output 1 at state s_0 and 0 for each of the other states. Each arrow, labeled $0,1$, stands for two arrows with the same beginning and end, one labeled 0 and one labeled 1.



SECTION 13.3 Finite-State Machines with No Output

2. By definition $A\emptyset = \{\, xy \mid x \in A \wedge y \in \emptyset \,\}$. Since there are no elements of the empty set, this set is empty. Similarly $\emptyset A = \emptyset$. (This result is also a corollary of Exercise 6, since a set is empty if and only if its cardinality is 0.)

4. **a)** If we concatenate any number of copies of the empty string, then we get the empty string.

b) Clearly $A^* \subseteq (A^*)^*$, since $B \subseteq B^*$ for all sets B. To show that $(A^*)^* \subseteq A^*$, let w be an element of $(A^*)^*$. Then $w = w_1 w_2 \ldots w_k$ for some strings $w_i \in A^*$. This means that each $w_i = w_{i1} w_{i2} \ldots w_{in_i}$ for some strings $w_{ij} \in A$. But then $w = w_{11} w_{12} \ldots w_{1n_1} w_{21} w_{22} \ldots w_{2n_2} \ldots w_{k1} w_{k2} \ldots w_{kn_k}$, a concatenation of elements of A, so $w \in A^*$.

6. At most, AB contains one element for each element in $A \times B$, namely $uv \in AB$ when $(u,v) \in A \times B$. (It might contain fewer elements than this, since the same string in AB may arise in two different ways, i.e., from two different ordered pairs.) Therefore $|AB| \le |A \times B| = |A||B|$.

8. **a)** This is false; take $A = \{1\}$, so that $A^2 = \{11\}$.

b) This is not true if we take $A = \emptyset$. If we exclude that possibility, then the length of every string in A^2 would be greater than the length of the shortest string in A if $\lambda \notin A$. Thus the statement is true for $A \ne \emptyset$.

c) This is true since $w\lambda = w$ for all strings.

d) This was Exercise 4b.

e) This is false if $\lambda \notin A$, since then the right-hand side contains the empty string but the left-hand side does not.

f) This is false. Take $A = \{0, \lambda\}$. Then $A^2 = \{\lambda, 0, 00\}$, so $|A^2| = 3 \ne 4 = |A|^2$.

10. **a)** This set contains all bit strings, so of course the answer is yes.

b) Every string in this set cannot have two consecutive 0's except possibly at the very start of the string. Because 01001 violates this condition, it is not in the set.

c) Our string is $(010)^1 0^1 1$ and so is in this set.

d) The answer is yes; just take 010 from the first set and 01 from the second.

e) Every string in this set must begin 00; since our string does not, it is not in the set.

f) Every string in this set cannot have two consecutive 0's. Because 01001 violates this condition, it is not in the set.

12. a) The first input keeps the machine in state s_0. The second input drives it to state s_1. The third input drives it back to state s_0. Since this state (s_0) is final, the string is accepted.

b) The input string drives the machine to states s_1, s_2, s_0, and s_1, respectively. Since s_1 is not a final state, this string is not accepted.

c) The input string drives the machine to states s_1, s_2, s_0, s_1, s_2, s_0, and s_1, respectively. Since s_1 is not a final state, this string is not accepted.

d) The input string drives the machine to states s_0, s_1, s_0, s_1, s_0, s_1, s_0, s_1, and s_0, respectively. Since s_0 is a final state, this string is accepted.

14. We can prove this by mathematical induction. For $n = 0$ (the basis step) we want to show that $f(s, \lambda) = s$, and this is true by the basis step of the recursive definition following Example 4. The inductive step follows directly from Exercise 15, since $x^{n+1} = x^n x$.

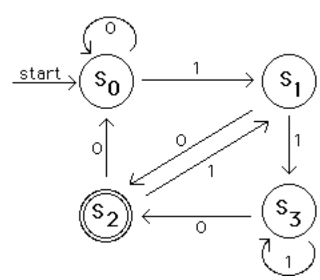
16. Since s_0 is a final state, the empty string is in the language recognized by this machine; note that no other string leads to s_0. The only other final state is s_1, and it is clear that it can be reached if the input string is in $\{1\}\{0,1\}^*$ or in $\{0\}\{1\}^*\{0\}\{0,1\}^*$. Therefore the answer can be summarized as $\{\lambda\} \cup \{1\}\{0,1\}^* \cup \{0\}\{1\}^*\{0\}\{0,1\}^*$.

18. Since state s_0 is final, the empty string is accepted. The only other strings that are accepted are those that drive the machine to state s_1, namely a 0 followed by any number of 1's. Therefore the answer is $\{\lambda\} \cup \{\, 01^n \mid n \geq 0 \,\}$.

20. We need to write down the strings that drive the machine to states s_1 or s_3. It is not hard to see that the answer is $\{1\}^*\{0\}\{0\}^* \cup \{1\}^*\{0\}\{0\}^*\{10, 11\}\{0,1\}^*$.

22. We need to write down the strings that drive the machine to states s_0, s_1, or s_5. It is not hard to see that the answer is $\{0\}^* \cup \{0\}^*\{1\} \cup \{0\}^*\{100\}\{1\}^* \cup \{0\}^*\{1110\}\{1\}^*$. This can be written more compactly as $\{0\}^*\{\lambda, 1\} \cup \{0\}^*\{100, 1110\}\{1\}^*$.

24. We need states to keep track of what the last two symbols of input were, so we create four states, s_0, s_1, s_2, and s_3, corresponding to having just seen 00, 01, 10, and 11, respectively. Only s_2 will be final, because we want to accept precisely those strings that end with 10. We make s_0 the start state, so in effect we are pretending that the string began with two 0's before we started accepting input; this causes no harm.



26. This is very similar to Exercise 29, except that the role of 0 and 1 are reversed, and we want to accept exactly those strings that are not accepted in Exercise 29. Therefore we take the machine given in the solution to that exercise, interchange inputs 0's and 1's throughout, and make s_3 the only nonfinal state (see Exercise 39).

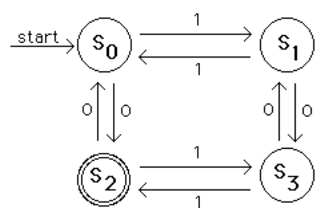
28. We have four states: s_0 (the start state) represents having seen no 0's; s_1 represents having seen exactly one 0; s_2 represents having seen exactly two 0's; and s_3 represents having seen at least three 0's. Only state s_3 is final. The transitions are the obvious ones: from each state to itself on input 1, from s_i to s_{i+1} on input 0 for $i = 0, 1, 2$, and from s_3 to itself on input 0.

30. We have five states: nonfinal state s_0 (the start state); final state s_1 representing that the string began with 0; nonfinal state s_2 representing that the first symbol in the string was 1; final state s_3 representing that the first two symbols in the string were 11; and nonfinal state s_4, a graveyard. The transitions are from s_0 to s_1 on input 0, from s_0 to s_2 on input 1, from s_2 to s_3 on input 1, from s_2 to s_4 on input 0, and from each of the states s_1, s_3, and s_4 to itself on either input.

32. This is very similar to Exercise 33, except that the role of 0 and 1 are reversed, and we want to accept exactly those strings that are not accepted in Exercise 33. Therefore we take the machine given in the solution to that exercise, interchange inputs 0's and 1's throughout, and make s_0 the only final state (see Exercise 39).

34. This is exactly the same as Exercise 36, except that s_1 is the one and only final state here.

36. This deterministic machine is the obvious choice. The top row represents having seen an even number of 0's (and the bottom row represents having seen an odd number of 0's); the left column represents having seen an even number of 1's (and the right column represents having seen an odd number of 1's).



38. We prove this by contradiction. Suppose that such a machine exists, with start state s_0. Because the empty string is in the language, s_0 must be a final state. There must be transitions from s_0 on each input, but they cannot be to s_0 itself, because neither the string 0 nor the string 1 is accepted. Furthermore, it cannot be that both transitions from s_0 lead to the same state s', because a 0 transition from s' would have to lead to an accepting state (since 00 is in the language), but that would cause our machine also to accept 10, which is not in the language. Therefore there must be nonfinal states s_1 and s_2 with transitions from s_0 to s_1 on input 0 and from s_0 to s_2 on input 1. If our machine has only three states, then there are no other states. Since the string 00 is accepted, there has to be a transition from s_1 to s_0 on input 0. Similarly, since the string 11 is accepted, there has to be a transition from s_2 to s_0 on input 1. Since the string 01 is not accepted (but some longer strings that start this way are accepted), there has to be a transition from s_1 on input 1 either to itself or to s_2. If it goes to s_1, then our machine accepts 010, which it should not; and if it goes to s_2, then our machine accepts 011, which it should not. Having obtained a contradiction, we conclude that no such finite-state automaton exists.

40. By the solution to Exercise 39, all we have to do is take the deterministic automata constructed in the relevant parts (**(a)**, **(d)**, and **(e)**) of Example 6 and change the status of each state (from final to nonfinal, and from nonfinal to final).

42. We use exactly the same machine as in Exercise 29, but make s_0, s_1, and s_2 the final states and make s_3 nonfinal. See also Exercise 26.

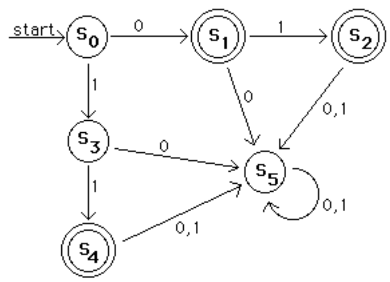
44. The empty string is accepted, since the start state is final. No other string drives the machine to state s_0, so the only other accepted strings are the ones that can drive the machine to state s_1. Clearly the strings 0 and 1 do so. Also, every string of one or more 1's can drive the machine to state s_2, after which a 0 will take it to state s_1. Therefore all the strings of the form 1^n0 for $n \geq 1$ are also accepted. Thus the answer is $\{\lambda, 0, 1\} \cup \{\, 1^n0 \mid n \geq 1\,\}$. (This can also be written as $\{\lambda, 1\} \cup \{\, 1^n0 \mid n \geq 0\,\}$, since $0 = 1^00$.)

46. We can end up at state s_0 by doing nothing, and we can end up at state s_1 by reading a 1. We can also end up at these final states by reading $\{10\}\{0,1\}$ first, any number of times. Therefore the answer is $(\{10\}\{0,1\})^*\{\lambda,1\}$.

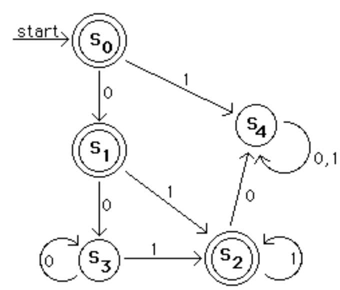
48. We just write down the paths that take us to state s_0 (namely, $\{0\}^*$), to state s_1 (namely, $\{0\}^*\{0,1\}\{0\}^*$), and to state s_4 via s_3 (namely $\{0\}^*\{0,1\}\{0\}^*\{10\}\{0\}^*$) or via s_2 (namely $\{0\}^*\{0,1\}\{0\}^*\{1\}\{0\}^*\{0,1\}\{0\}^*$). Our final answer is then the union of these:

$$\{0\}^* \cup \{0\}^*\{0,1\}\{0\}^* \cup \{0\}^*\{0,1\}\{0\}^*\{10\}\{0\}^* \cup \{0\}^*\{0,1\}\{0\}^*\{1\}\{0\}^*\{0,1\}\{0\}^*$$

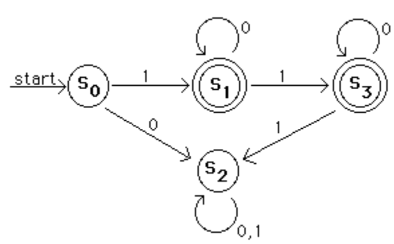
50. One way to do Exercises 50–54 is to construct a machine following the proof of Theorem 1. Rather than do that, we construct the machines in an ad hoc way, using the answers obtained in Exercises 43–47. As we saw in the solution to Exercise 43, the language recognized by this machine is $\{0,01,11\}$. A deterministic machine to recognize this language is shown below. Note that state s_5 is a graveyard state.



52. This is similar to Exercise 44; here is the machine.



54. This one is fairly simple, since the nondeterministic machine is almost deterministic. In fact, all we need to do is to eliminate the transition from s_1 to the graveyard state s_2 on input 0, and the transition from s_3 to s_2 on input 0.



56. The machines in the solutions to Exercise 55, with the graveyard state removed, satisfy the requirements of this exercise.

58. **a)** That R_k is reflexive is tautological; and that R_k is symmetric is clear from the symmetric nature of its definition. To see that R_k is transitive, suppose sR_kt and tR_ku; we must show that sR_ku. Let x be an arbitrary string of length at most k. If $f(s,x)$ is final, then $f(t,x)$ is final, and so $f(u,x)$ is final; similarly, if $f(s,x)$ is nonfinal, then $f(t,x)$ is nonfinal, and so $f(u,x)$ is nonfinal. This is the definition of tR_ku.

b) Notice that $R_0 \supseteq R_1 \supseteq R_2 \supseteq \cdots$ (see part **(c)**) and that $R_* = \bigcap_{k=0}^{\infty} R_k$ (see part **(e)**). To see that R_* is reflexive, just note that for every state s and every nonnegative integer k we have $(s,s) \in R_k$, so $(s,s) \in R_*$. To see that R_* is symmetric, suppose that sR_*t. Then sR_kt for every k, whence tR_ks, whence tR_*s. To see that R_* is transitive, suppose that sR_*t and tR_*u. Then sR_kt and tR_ku for every k. By the transitivity of R_k we have sR_ku, whence sR_*u.

c) The condition sR_kt is stronger than the condition $sR_{k-1}t$, because all the strings considered for $sR_{k-1}t$ are also strings under consideration for sR_kt. Therefore if sR_kt, then $sR_{k-1}t$.

d) This is an example of the general result proved in Exercise 54 in Section 8.5.

e) Suppose that s and t are k-equivalent for every k. Let x be a string of length k. Then $f(s,x)$ and $f(t,x)$ are either both final or both nonfinal, so by definition, s and t are $*$-equivalent.

f) If s and t are $*$-equivalent, then in particular the empty string drives them both to a final state or drives them both to a nonfinal state. But the empty string drives a state to itself, and the result follows.

g) We must show that $f(f(s,a),x)$ and $f(f(t,a),x)$ are either both final or both nonfinal. By Exercise 15 we have $f(f(s,a),x) = f(s,ax)$ and $f(f(t,a),x) = f(t,ax)$. But because s and t are $*$-equivalent, we know that $f(s,ax)$ and $f(t,ax)$ are either both final or both nonfinal.

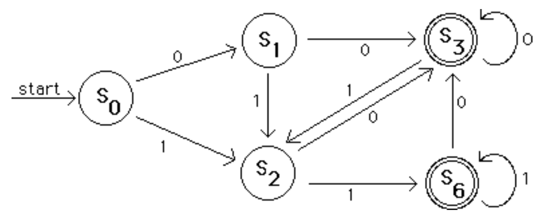
60. **a)** Two states are 0-equivalent if the empty string drives both to a final state or drives both to a nonfinal state. But the empty string drives a state to itself. Therefore two states are 0-equivalent if they are both final states or both nonfinal states. Thus each equivalence class of R_0 consists of only final states or of only nonfinal states. Since the equivalence classes of R_* are a refinement of the equivalence classes of R_0, each equivalence class of R_* consists of only final states or of only nonfinal states.

b) First suppose that s and t are k-equivalent. By Exercise 58c, s and t are $(k-1)$-equivalent. Furthermore, if $f(s,a)$ and $f(t,a)$ were not $(k-1)$-equivalent, then some string x of length $k-1$ would drive $f(s,a)$ and $f(t,a)$ to different types of states (one final, one nonfinal). That would mean that ax, which is a string of length k, would drive s and t to different types of states, contradicting the fact that s and t are k-equivalent. Conversely, suppose that s and t are $(k-1)$-equivalent and $f(s,a)$ and $f(t,a)$ are $(k-1)$-equivalent for every $a \in I$. We must show that s and t are k-equivalent. A string of length less than k drives both to the same type of state because s and t are $(k-1)$-equivalent. So suppose $x = aw$ is a string of length k. Then x drives both s and t to the same type of state because the machine moves first to $f(s,a)$ and $f(t,a)$, respectively, but we are given that $f(s,a)$ and $f(t,a)$ are $(k-1)$-equivalent. Thus the definition of the transition function $\overline{f}$ does not depend on the choice of representative from the equivalence class and so is well defined.

c) There are only a finite number of strings of length k for each k. Therefore we can test two states for k-equivalence in a finite length of time by just tracing all possible computations. If we do this for $k = 0, 1, 2, \ldots$, then by Exercise 59 we know that eventually we will find nothing new, and at that point we have determined the equivalence classes of R_*. This tells us the states of $\overline{M}$, and the definition in the preamble to this exercise gives us the transition function, the start state, and the set of final states of $\overline{M}$. For more details, see a source such as *Introduction to Automata Theory, Languages, and Computation* (2nd Edition) by John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman (Addison Wesley, 2000).

62. **a)** For $k = 0$ the only issue is whether the states are final or not. Thus one equivalence class is $\{s_0, s_1, s_2, s_4\}$ (the nonfinal states) and the other is $\{s_3, s_5, s_6\}$ (the final states). For $k = 1$, we need to try to refine these classes by seeing whether strings of length 1 drive the machine from the given state to final or nonfinal states. The string 0 takes us from s_0 to a nonfinal state, and the string 1 takes us from s_0 to a nonfinal state, so let's call s_0 type NN. Then we see that s_1 is type FN, that s_2 is type FF, and that s_4 is type FF. Therefore s_2 and s_4 are still equivalent (they have the same type, so they behave the same, in terms of driving to final states, on strings of length 1), but s_0 and s_1 are not 1-equivalent to either of them or to each other. Similarly, states s_3, s_5, and s_6 are types FN, FN, and FF, respectively, so s_3 and s_5 are 1-equivalent, but s_6 is not 1-equivalent to either of them. This gives us the following 1-equivalence classes: $\{s_0\}$, $\{s_1\}$, $\{s_2, s_4\}$, $\{s_3, s_5\}$, and $\{s_6\}$. Notice that not only are s_2 and s_4 1-equivalent, but they will be k-equivalent for all k, because they have exactly the same transitions (to s_5 on input 0, and to s_6 on input 1). The same can be said for s_3 and s_5. Therefore the 2-equivalence classes will be the same as the 1-equivalence classes, and these will be the k-equivalence classes for all $k \geq 1$, as well as the $*$-equivalence classes.

b) We turn s_2 and s_4 into one state (labeled s_2 below), and we turn s_3 and s_5 into one state (labeled s_3 below). The transitions can be copied from the diagram for M.



SECTION 13.4 Language Recognition

2. **a)** This regular expression generates all strings consisting of exactly two 0's followed by zero or more 1's.

b) This regular expression generates all strings consisting of zero or more repetitions of 01.

c) This is the string 01 together with all strings consisting of exactly two 0's followed by zero or more 1's.

d) This set contains all strings that start with a 0 and satisfy the condition that all the maximal substrings of 1's have an even number of 1's in them.

e) This set consists of all strings in which every 0 is preceded by a 1, and furthermore the string must start 10 if it is not empty.

f) This gives us all strings that consist of zero or more 0's followed by 11, together with the string 111.

4. **a)** The string is in the set, since it is $10^1 1^2$.

b) The string is in the set, since it is (10)(11).

c) The string is in the set, since it is 1(01)1.

d) The string is in the set: take the first $*$ to be 1, and take the 1 in the union.

e) The string is in the set, since it is (10)(11).

f) The strings in this set must have odd length, so the given string is not in the set.

g) The string is in the set: take $*$ to be 0.

h) The string is in the set: choose 1 from the first group, 01 from the second, and take $* = 1$.

6. **a)** There are many ways to do this, such as $(\lambda \cup \mathbf{0} \cup \mathbf{1})(\lambda \cup \mathbf{0} \cup \mathbf{1})(\lambda \cup \mathbf{0} \cup \mathbf{1})$.

b) $\mathbf{001^*0}$

c) We assume it is not intended that every 1 is followed by *exactly* two 0's, so we can write $\mathbf{0}^*(\mathbf{100} \cup \mathbf{0})^*$.

d) One way to say this is that every 1 must be followed by a 0. Thus we can write $\mathbf{0}^*(\mathbf{10} \cup \mathbf{0})^*\mathbf{00}$.

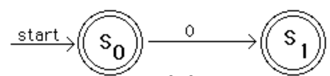
e) To get an even number of 1's, we can write something like $(\mathbf{0}^*\mathbf{10}^*\mathbf{10}^*)^*$.

8. **a)** Since we want to accept no strings, we will have no final states. We need only one state, the start state, and there is a transition from this state to itself on all inputs.

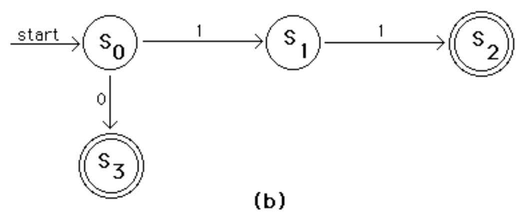
b) This is just like part **(a)**, except that we want to accept the empty string. Our machine will have two states. The start state will be final, the other state will not be final. On all inputs, there is a transition from each of the states to the nonfinal state.

c) This time we need three states, s_0 (the start state), s_1, and s_2. Only s_1 is final. On input a, there is a transition from s_0 to s_1: this will make sure that a is accepted. All other transitions are to s_2, which serves as a graveyard state: from s_0 on all inputs except a, and from s_1 and s_2 on all inputs. (It is not clear from the exercise whether a is meant to be one fixed element of I, as we have assumed, or rather whether we are to accept all strings of length 1. If the latter is intended, then we have a transition from state s_0 to state s_1 for every $a \in I$.)

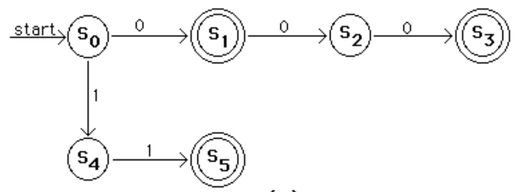
10. The construction is straightforward in each case: we just lead to final states on the desired inputs.



(a)



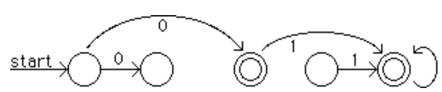
(b)



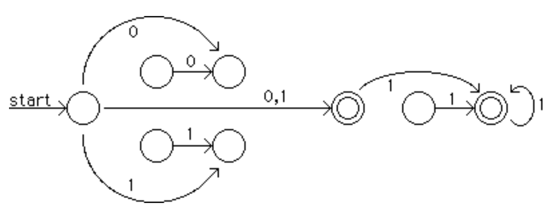
(c)

12. These are quite messy to draw in detail.

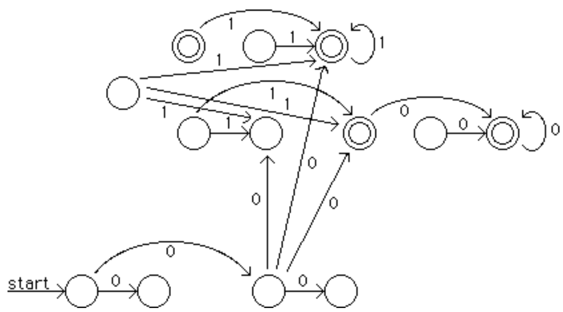
a) The machine for 0 is shown in Figure 3 (third machine). The machine for 1^* is shown in Figure 3 (second machine). We need to concatenate them, so we get the following picture:



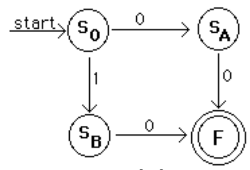
b) The machine for 0 is shown in Figure 3 (third machine). The machine for 1 is similar. We need to take their union. Then we need to concatenate that with the machine for 1^*, shown in Figure 3 (second machine). So we get the following picture:



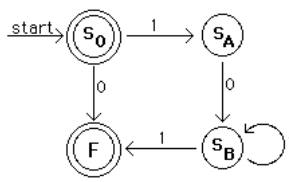
c) The machine for 10^* is like our answer for part **(a)**, with the roles of 0 and 1 reversed. We need to take the union of that with the machine for 1^* shown in Figure 3 (second machine). We then need to concatenate two copies of the machine for 0 (third machine in Figure 3) in front of this, so we get the following picture:



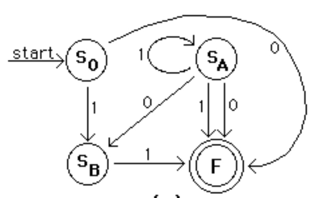
14. In each case we follow the construction inherent in the proof of Theorem 2. There is one state for each nonterminal symbol (which we have denoted with the name of the symbol), and there is one more state—the only final one unless $S \to \lambda$ is a transition—which we call F.



(a)



(b)



(c)

16. The transitions between states cause us to put in the rules $S \to 0A$, $S \to 1B$, $A \to 0B$, $A \to 1A$, $B \to 0B$, and $B \to 1A$. The transitions to final states cause us to put in the rules $S \to 0$, $A \to 1$, and $B \to 1$. Finally, since s_0 is a final state, we add the rule $S \to \lambda$.

18. This is clear, since the unique derivation of every terminal string in the grammar is exactly reflected in the operation of the machine. Precisely those nonempty strings that are generated drive the machine to its final state, and the empty string is accepted if and only if it is in the language.

20. We construct a new nondeterministic finite-state automaton from a given one as follows. A new state s_0' is added (but s_0 is still the start state). The new state is final if and only if s_0 is final. All transitions into s_0 are redirected so that they end at s_0'. Then all transitions out of s_0 are copied to become transitions out of s_0'. It is clear that s_0 can never be revisited, since all the transitions into it were redirected. Furthermore, s_0' is playing the same role that s_0 used to play (after one or more symbols of input have been read), so exactly the same set of strings is accepted.

22. Let the states that were encountered on input x be, in order, s_0, s_{i_1}, s_{i_2}, $\ldots$, s_{i_n}, where $n = l(x)$. Since we are given that $n \geq |S|$, this list of $n+1$ states must, by the pigeonhole principle, contain a repetition;

suppose that the first repeated state is s_r. Let v be that portion of x that caused the machine to move from s_r on its first encounter back to s_r for the second encounter. Let u be the portion of x before v, and let w be the portion of x after v. In particular $l(v) \geq 1$ and $l(uv) \leq |S|$ (since all the states appearing before the second encounter with s_r are different). Furthermore, the string uv^iw, for each nonnegative integer i, must drive the machine to exactly the same final state as $x = uvw$ did, since the v^i part of the string simply drives the machine around and around in a loop starting and ending at s_r (the loop is traversed i times). Therefore all these strings are accepted (since x was accepted), and so all of them are in the language.

24. Assume that this set is regular, accepted by a deterministic finite-state automaton with state set S. Let $x = 1^{n^2}$ for some $n \geq \sqrt{|S|}$. By the pumping lemma, we can write $x = uvw$ with v nonempty, so that uv^iw is in our set for all i. Since there is only one symbol involved, we can write $u = 1^r$, $v = 1^s$ and $w = 1^t$, so that the statement that uv^iw is in our set is the statement that $(r+t)+si$ is a perfect square. But this cannot be, since successive perfect squares differ by increasing large amounts as they grow larger, whereas the terms in the sequence $(r+t)+si$ have a constant difference for $i = 0, 1, \ldots$. This contradiction tells us that the set is not regular.

26. This (far from easy) proof is similar in spirit to Warshall's algorithm. The interested reader should consult a reference in computation theory, such as *Elements of the Theory of Computation* by H. R. Lewis and C. H. Papadimitriou (Prentice-Hall, 1981).

28. It's just a matter of untangling the definition. If x and y are distinguishable with respect to $L(M)$, then without loss of generality there must be a string z such that $xz \in L(M)$ and $yz \notin L(M)$. This means that the string xz drives M from its initial state to a final state, and the string yz drives M from its initial state to a nonfinal state. For a proof by contradiction, suppose that $f(s_0, x) = f(s_0, y)$; in other words, x and y both drive M to the same state. But then xz and yz both drive M to the same state, after $l(z)$ more steps of computation (where $l(z)$ is the length of z), and this state can't be both final and nonfinal. This contradiction shows that $f(s_0, x) \neq f(s_0, y)$.

30. We claim that all 2^n bit strings of length n are distinguishable with respect to L. If x and y are two bit strings of length n that differ in bit i, where $i \leq 1 \leq n$, then they are distinguished by any string z of length $i-1$, because one of xz and yz has a 0 in the n^{th} position from the end and the other has a 1. Therefore by Exercise 29, any deterministic finite-state automaton recognizing L_n must have at least 2^n states.

SECTION 13.5 Turing Machines

2. We will indicate the configuration of the Turing machine using a notation such as $0[s_2]1B1$, as described in the solution to Exercise 1. (This means that the machine is in state s_2, the tape is blank except for a portion that reads $01B1$, and the tape head points to the left-most 1.) We indicate the successive configurations with arrows.

a) Initially the configuration is $[s_0]0101$. Using the first five-tuple, the machine next enters configuration $0[s_1]101$. Thereafter it proceeds as follows: $0[s_1]101 \to 01[s_1]01 \to 011[s_2]1$. Since there is no five-tuple for this combination (in state s_2 reading a 1), the machine halts. Thus (the nonblank portion of) the final tape reads 0111.

b) $[s_0]111 \to [s_1]B011 \to 0[s_2]011 \to$ halt; final tape 0011

c) $[s_0]00B00 \to 0[s_1]0B00 \to 01[s_2]B00 \to 010[s_3]00 \to$ halt; final tape 01000

d) $[s_0]B \to 1[s_1]B \to 10[s_2]B \to 100[s_3]B \to$ halt; final tape 100

4. **a)** The machine starts in state s_0 and sees the first 1. Therefore using the first five-tuple, it replaces the 1 by a 1 (i.e., leaves it unchanged), moves to the right, and stays in state s_0. Now it sees the 0, so, using the second five-tuple, it replaces the 0 by a 1, moves to the right, and stays in state s_0. When it sees the second 1, it again leaves it unchanged, moves to the right, and stays in state s_0. Now it reads the blank, so, using the third five-tuple, it leaves the blank alone, moves left, and enters state s_1. At this point it sees the 1 and so leaves it alone and enters state s_2 (using the fourth five-tuple). Since there are no five-tuples telling the machine what to do in state s_2, it halts. Note that 111 is on the tape, and the input was accepted, because s_2 is a final state.

b) This is essentially the same as part **(a)**. Every 0 on the tape is changed to a 1 (and the 1's are left unchanged), and the input is accepted. (The only exception is that if the input is initially blank, then the machine will, after one transition, be in state s_1 looking at a blank and have no five-tuple to apply. Therefore it will halt without accepting.)

6. We need to scan from left to right, leaving things unchanged, until we come to the blank. The five-tuples $(s_0, 0, s_0, 0, R)$ and $(s_0, 1, s_0, 1, R)$ do this. One more five-tuple will take care of adding the new bit: $(s_0, B, s_1, 1, R)$.

8. We can do this with just one state. The five-tuples are $(s_0, 0, s_0, 1, R)$ and $(s_0, 1, s_0, 1, R)$. When the input is exhausted, the machine just halts.

10. We need to have the machine look for a pair of consecutive 1's. The following five-tuples will do that: $(s_0, 0, s_0, 0, R)$, $(s_0, 1, s_1, 1, R)$, $(s_1, 0, s_0, 0, R)$, and $(s_1, 1, s_2, 0, L)$. Once the machine is in state s_2, it has just replaced the second 1 in the first pair of consecutive 1's with a 0 and backed up to the first 1 in this pair. Thus the five-tuple $(s_2, 1, s_3, 0, R)$ will complete the job.

12. We can stay in state s_0 until we have hit the first 1; then stay in state s_1 until we have hit the second 1. At that point we can enter state s_2 which will be an accepting state. If we come to the final blank while still in states s_0 or s_1, then we will not accept. The five-tuples are simply $(s_0, 0, s_0, 0, R)$, $(s_0, 1, s_1, 1, R)$, $(s_1, 0, s_1, 0, R)$, and $(s_1, 1, s_2, 1, R)$.

14. We use the notation mentioned in the solution to Exercise 2. The tape contents are the symbols shown in each configuration, without the state.

a) $[s_0]0011 \to M[s_1]011 \to M0[s_1]11 \to M01[s_1]1 \to M011[s_1]B \to M01[s_2]1 \to M0[s_3]1M \to M[s_3]01M \to [s_4]M01M \to M[s_0]01M \to MM[s_1]1M \to MM1[s_1]M \to MM[s_2]1M \to M[s_3]MMM \to MM[s_5]MM \to MMM[s_6]M \to$ halt and accept

b) $[s_0]00011 \to M[s_1]0011 \to M0[s_1]011 \to M00[s_1]11 \to M001[s_1]1 \to M0011[s_1]B \to M001[s_2]1 \to M00[s_3]1M \to M0[s_3]01M \to M[s_4]001M \to [s_4]M001M \to M[s_0]001M \to MM[s_1]01M \to MM0[s_1]1M \to MM01[s_1]M \to MM0[s_2]1M \to MM[s_3]0MM \to M[s_4]M0MM \to MM[s_0]0MM \to MMM[s_1]MM \to MM[s_2]MMM \to$ halt and reject

c) $[s_0]101100 \to$ halt and reject

d) $[s_0]000111 \to M[s_1]00111 \to M0[s_1]0111 \to M00[s_1]111 \to M001[s_1]11 \to M0011[s_1]1 \to M00111[s_1]B \to M0011[s_2]1 \to M001[s_3]1M \to M00[s_3]11M \to M0[s_3]011M \to M[s_4]0011M \to [s_4]M0011M \to M[s_0]0011M \to MM[s_1]011M \to MM0[s_1]11M \to MM01[s_1]1M \to MM011[s_1]M \to MM01[s_2]1M \to MM0[s_3]1MM \to MM[s_3]01MM \to M[s_4]M01MM \to MM[s_0]01MM \to MMM[s_1]1MM \to MMM1[s_1]MM \to MMM[s_2]1MM \to MM[s_3]MMMM \to MMM[s_5]MMM \to MMMM[s_6]MM \to$ halt and accept

16. This task is similar to the task accomplished in Example 3. There is one sense in which it is simpler: since we are allowing $n = 0$, we do not need to make any special efforts to reject the empty string. There is one sense, of course, in which it is harder, namely the need to change two 0's to M's at the left for every one 1 changed to an M at the right. The following five-tuples should accomplish the job: $(s_0, 0, s_1, M, R)$, (s_0, B, s_5, B, R), (s_0, M, s_5, M, R), $(s_1, 0, s_2, M, R)$, $(s_2, 0, s_2, 0, R)$, $(s_2, 1, s_2, 1, R)$, (s_2, M, s_3, M, L), (s_2, B, s_3, B, L), $(s_3, 1, s_4, M, L)$, $(s_4, 0, s_4, 0, L)$, $(s_4, 1, s_4, 1, L)$, (s_4, M, s_0, M, R).

18. This is pretty simple, since all we need to do is to put in two extra 1's. The following five-tuples will do the job: $(s_0, 1, s_1, 1, L)$, $(s_1, B, s_2, 1, L)$, $(s_2, B, s_3, 1, L)$.

20. We want to erase 1's in sets of three, as long as there are at least four 1's left. We can accomplish this by first checking for the presence of the four 1's, then erasing them, and then repositioning the tape head to repeat this task. The following five-tuples will do the job: $(s_0, 1, s_1, 1, R)$, $(s_1, 1, s_2, 1, R)$, $(s_2, 1, s_3, 1, R)$, $(s_3, 1, s_4, 1, L)$, $(s_4, 1, s_5, B, L)$, $(s_5, 1, s_6, B, L)$, $(s_6, 1, s_7, B, R)$, (s_7, B, s_8, B, R), (s_8, B, s_0, B, R).

22. We start with a string of $n+1$ 1's, and we want to end up with a string of $2n+1$ 1's. Our idea will be to replace the last 1 with a 0, then for each 1 to the left of the 0, write a new 1 to the right of the 0. To keep track of which 1's we have processed so far, we will change each left-side 1 with a 0 as we process it. At the end, we will change all the 0's back to 1's. Basically our states will mean the following ("first" means "first encountered"): s_0, scan right for last 1; s_1, change the last 1 to 0; s_2, scan left to first 1; s_3, scan right for end of tape (having replaced the 1 where we started with a 0) and add a 1 at the end; s_4, scan left to first 0; s_5, replace the remaining 0's with 1's; s_6, halt.

The needed five-tuples are as follows: $(s_0, 1, s_0, 1, R)$, (s_0, B, s_1, B, L), $(s_1, 1, s_2, 0, L)$, $(s_2, 0, s_2, 0, L)$, $(s_2, 1, s_3, 0, R)$, (s_2, B, s_5, B, R), $(s_3, 0, s_3, 0, R)$, $(s_3, 1, s_3, 1, R)$, $(s_3, B, s_4, 1, L)$, $(s_4, 1, s_4, 1, L)$, $(s_4, 0, s_2, 0, L)$, $(s_5, 0, s_5, 1, R)$, $(s_5, 1, s_6, 1, R)$, (s_5, B, s_6, B, R).

24. We need to erase the first input, then replace the asterisk by a 1 and write one more 1. This straightforward task can be done with the following five-tuples: $(s_0, 1, s_0, B, R)$, $(s_0, *, s_1, 1, L)$, $(s_1, B, s_2, 1, L)$.

26. Since the number n is represented by $n+1$ 1's, we need to be a little careful here. The most straightforward approach is to replace the middle asterisk by a 1 and erase one 1 from each end of the input. The following five-tuples will do the job: $(s_0, 1, s_1, B, R)$, $(s_1, 1, s_1, 1, R)$, $(s_1, *, s_2, 1, R)$, $(s_2, 1, s_2, 1, R)$, (s_2, B, s_3, B, L), $(s_3, 1, s_4, B, R)$.

28. The discussion in the preamble tells how to take the machines from Exercises 18 and 23 and create a new machine. The only catch is that the tape head needs to be back at the leftmost 1. Suppose that s_m, where m is the largest index, is the state in which the Turing machine for Exercise 18 halts after completing its work, and suppose that we have designed that machine so that when the machine halts the tape head is reading the leftmost 1 of the answer. Then we renumber each state in the machine for Exercise 23 by adding m to each subscript, and take the union of the two sets of five-tuples.

30. A decision problem is one with a yes/no answer. These are all decision problems except for part **(c)**; in that case, the answer is a vertex number rather than "yes" or "no."

32. The technical details here are rather messy. The reader should consult the article on the busy beaver problem in A. K. Dewdney's *The New Turing Omnibus: 66 Excursions in Computer Science* (Freeman, 1993); further references are given there.

SUPPLEMENTARY EXERCISES FOR CHAPTER 13

2. We will construct a grammar that will initially generate a string of the form $DD\ldots D0E$, with zero or more D's on the left, a 0 in the middle, and an E on the right. The D's will migrate across the 0's in the middle, each one doubling the number of 0's present. When the D reaches the E on the right, it is absorbed. Thus our grammar has the following rules. The rules $S \to A0E$, $A \to AD$, and $A \to \lambda$ create the strings of the formed mentioned above. The rule $D0 \to 00D$ causes the doubling. The rule $DE \to E$ absorbs the D's. Finally, we need to add the rule $E \to \lambda$ to finish off every derivation.

4. It can be proved by induction on the length of the derivation that every terminal string derivable from A or B is a well-formed string of parentheses. It follows that the language generated by this grammar is contained in the set of well-formed strings of parentheses. Conversely, it can be proved by induction on the length of the string that every well-formed string of parentheses is derivable from this grammar.

6. There is only one derivation of length n, for each n, namely $S \Rightarrow 0S \Rightarrow 00S \Rightarrow \cdots \Rightarrow 0^{n-1}S \Rightarrow 0^n$. Therefore derivation trees are unique.

8. a) This is true: $A(B \cup C) = \{\, ax \mid a \in A \wedge x \in B \cup C \,\} = \{\, ax \mid a \in A \wedge (x \in B \vee x \in C) \,\} = \{\, ax \mid (a \in A \wedge x \in B) \vee (a \in A \wedge x \in C) \,\} = \{\, ax \mid a \in A \wedge x \in B \,\} \cup \{\, ax \mid a \in A \wedge x \in C \,\} = AB \cup AC$.

b) This is also true; the proof is similar to that in part **(a)**.

c) This is true: $(AB)C = \{\, xc \mid x \in AB \wedge c \in C \,\} = \{\, abc \mid a \in A \wedge b \in B \wedge c \in C \,\}$ and $A(BC)$ equals the same set.

d) This is not true. Let $A = \{0\}$ and $B = \{1\}$. Then 01 is in the left-hand side but not the right-hand side.

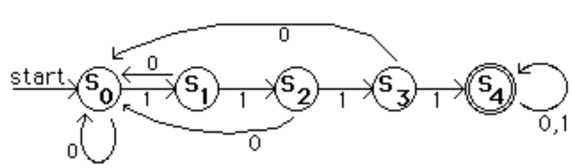
10. Clearly the strings generated by this regular expression have no 0 immediately preceding a 2. Conversely, we can take any string with this property and, by grouping the 2's together, view it as coming from this regular expression (we need to imagine a group of no 2's between every pair of consecutive 1's).

12. a) This regular expression is equivalent to $(\mathbf{0} \cup \mathbf{1})^*$, whose star height is 1. Clearly we cannot find an equivalent expression with star height 0.

b) It is always true that $(\mathbf{AB}^*)^*$ is equivalent to $\mathbf{A}^* \cup \mathbf{A}(\mathbf{A} \cup \mathbf{B})^*$. Thus we can replace the given expression (which has star height 3) by one with star height 2, namely $\mathbf{0}^* \cup \mathbf{0}(\mathbf{0} \cup \mathbf{01}^*\mathbf{0})^*$. Now since the substrings of consecutive 0's and 1's can be arbitrarily long, and yet not all strings are in the language (since each two maximal substrings of 1's must be separated by at least two 0's), it is not possible to reduce the star height to 1.

c) This regular expression is equivalent to $(\mathbf{0} \cup \mathbf{1})^*$, whose star height is 1. Clearly we cannot find an equivalent expression with star height 0.

14. We draw only the deterministic finite-state automaton for this problem. The finite-state machine with output is identical, except that the output is 1 if and only if the transition is to the final state in our picture. The idea here is simply that state s_i corresponds to having just seen i consecutive 1's.



16. If x is a string and s is a state, then $f(s,x)$ means the state that string x drives the machine to if the machine is currently in state s.

a) It is clear that by following the appropriate arrows, we can reach all the states except s_3 from state s_0; for example, $f(s_0, 01) = s_5$ and $f(s_0, \lambda) = s_0$. Clearly we cannot reach state s_3 from any other state.

b) Clearly only states s_2 and s_5 are reachable from state s_2.

c) A transient state s is one for which there is no path from s to itself. Clearly, once we leave state s_0 or s_1 or s_3 or s_6, we cannot return, so these are the transient states. Because of the loops, the other states are not transient. (Note, however, that a state does not need to have a loop at it in order to be nontransient.)

d) Clearly only s_4 and s_5 are the sinks, since the other states all have arrows leaving them.

18. a) To specify a deterministic automaton, we need to pick a start state (n ways to do this), we need to pick a set of final states (2^n ways to do this), and for each pair (state, input) (and there are nk such pairs) we need to choose a state for the transition (n^{nk} ways to do this). Therefore the answer is $n2^n n^{nk} = 2^n n^{nk+1}$.

b) This is the same as part **(a)**, except that we need to choose one of the 2^n subsets of states for each pair (state, input). Therefore the answer is $n2^n(2^n)^{nk} = n2^{n+kn^2}$.

20. No states are final, so no strings are accepted. Therefore the language recognized by this machine is $\emptyset$.

22. a) An even number (we assume that "positive even number" is implied here) of 1's is represented by $\mathbf{11(11)}^*$. An odd number of 0's is similarly represented by $\mathbf{0(00)}^*$. If we interpret "interspersed" in a positive sense (insisting that the string start and end with 1's), then our answer is

$$\mathbf{11(11)}^*(\mathbf{0(00)}^*\mathbf{11(11)}^*)^* .$$

b) This one is straightforward: $(\mathbf{1} \cup \mathbf{0})^*(\mathbf{00} \cup \mathbf{111})(\mathbf{1} \cup \mathbf{0})^*$.

c) The middle of this expression must be $(\mathbf{1}(\mathbf{0} \cup \mathbf{00}))^*$, so as to guarantee the desired interspersing. The beginning may allow up to two 0's, and the end may allow up to one 1. Therefore the answer is $(\emptyset^* \cup \mathbf{0} \cup \mathbf{00})(\mathbf{1}(\mathbf{0} \cup \mathbf{00}))^*(\emptyset^* \cup \mathbf{1})$.

24. It is clear from the definition of the sets generated by regular expressions that the union of two regular sets is regular. From Exercise 23 we know that the complement of a regular set is regular. Now $A \cap B = \overline{(\overline{A} \cup \overline{B})}$; therefore if A and B are regular, so is their intersection.

26. The proof is essentially identical to the solution of Exercise 24 in Section 13.4, since the gaps between successive powers of 2, like the gaps between successive squares, grow as the numbers get larger.

28. Suppose that there were a context-free grammar generating this set, and apply the analog of the pumping lemma to obtain strings u, v, w, x, and y such that not both v and x are empty and uv^iwx^iy is of the form $0^n1^n2^n$ for all i. Now if either v or x contains two or three different symbols, then uv^2wx^2y has the symbols out of order. Therefore at least one symbol (say the 0) is missing from vx. On the other hand at least one symbol (say the 1) appears in vx (since $vx \neq \lambda$). But then uv^iwx^iy must have more 1's than 0's for large i, a contradiction. Therefore there is no such context-free grammar.

30. The input will be a string of $n_1 + 1$ 1's, followed by an asterisk, followed by a string of $n_2 + 1$ 1's, with the tape head positioned at the leftmost 1 of the first argument. We want the machine to erase a 1 from the second argument for each 1 it finds in the first argument, leaving $n_2 - n_1$ 1's in the second string (also erasing the 1's in the first argument in the process), and then to replace the asterisk by a 1. If $n_2 < n_1$, however, we want the machine to halt with just one 1 on the tape (because the answer in that case is the number 0). We will adopt a recursive approach, in the sense that after one erasure, the problem becomes to compute $f(n_1 - 1, n_2 - 1)$, which will have the same answer.

In the Turing machine tuples that follows, the intent is that s_0 is the state in which we erase a 1 from n_1 (or notice that we are essentially finished); s_1 is the state in which we scan right to find the last 1 in n_2; s_2 is the state in which we erase a 1 from n_2 (or notice that $n_2 < n_1$); s_3 is the state in which we scan back to the starting point; s_4 is the clean-up state for handling the case $n_2 < n_1$, and s_5 is the halt state.

These tuples should accomplish the job: $(s_0, 1, s_1, B, R)$, $(s_0, *, s_5, 1, L)$, $(s_1, 1, s_1, 1, R)$, $(s_1, *, s_1, *, R)$, (s_1, B, s_2, B, L), $(s_2, 1, s_3, B, L)$, $(s_2, *, s_4, B, L)$, $(s_3, 1, s_3, 1, L)$, $(s_3, *, s_3, *, L)$, (s_3, B, s_0, B, R), $(s_4, 1, s_4, B, L)$, and $(s_4, B, s_5, 1, L)$.