e)

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

f)

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

33. For parts (a), (b), (c), (d), and (f) we have this table.

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

For part (e) we have this table.

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

35.

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

37.

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

39.

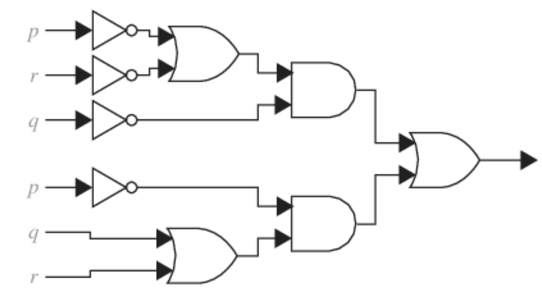
p	q	r	s	$p \leftrightarrow q$	$r \leftrightarrow s$	$(p \leftrightarrow q) \leftrightarrow (r \leftrightarrow s)$
T	T	T	T	T	T	T
T	T	T	F	T	F	F
T	T	F	T	T	F	F
T	T	F	F	T	T	T
T	F	T	T	F	T	F
T	F	T	F	F	F	T
T	F	F	T	F	F	T
T	F	F	F	F	T	F
F	T	T	T	F	T	F
F	T	T	F	F	F	T
F	T	F	T	F	F	T
F	T	F	F	F	T	F
F	F	T	T	T	T	T
F	F	T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

41. The first clause is true if and only if at least one of p, q, and r is true. The second clause is true if and only if at least one of the three variables is false. Therefore the entire statement is true if and only if there is at least one T and one F among the truth values of the variables, in other words, that they don't all have the same truth value. 43. **a)** Bitwise *OR* is 111 1111; bitwise *AND* is 000 0000; bitwise *XOR* is 111 1111. **b)** Bitwise *OR* is 1111 1010; bitwise *AND* is 1010 0000; bitwise *XOR* is 0101 1010. **c)** Bitwise *OR* is 10 0111 1001; bitwise *AND* is 00 0100 0000; bitwise *XOR* is 10 0011 1001. **d)** Bitwise *OR* is 11 1111 1111; bitwise *AND* is 00 0000 0000; bitwise *XOR* is 11 1111 1111. 45. 0.2, 0.6 47. 0.8, 0.6 49. **a)** The 99th statement is true and the rest are false. **b)** Statements 1 through 50 are all true and statements 51 through 100 are all false. **c)** This cannot happen; it is a paradox, showing that these cannot be statements.

Section 1.2

1. $e \rightarrow a$ 3. $g \rightarrow (r \wedge (\neg m) \wedge (\neg b))$ 5. $e \rightarrow (a \wedge (b \vee p) \wedge r)$ 7. **a)** $q \rightarrow p$ **b)** $q \wedge \neg p$ **c)** $q \rightarrow p$ **d)** $\neg q \rightarrow \neg p$ 9. Not consistent 11. Consistent 13. NEW **AND** JERSEY **AND** BEACHES, (JERSEY **AND** BEACHES) **NOT** NEW 15. "If I were to ask you whether the right branch leads to the ruins, would you answer yes?" 17 If the first professor did not want coffee, then he would know that the answer to the hostess's question was "no." Therefore the hostess and the remaining professors know that the first professor did want coffee. Similarly, the second professor must want coffee. When the third professor said "no," the hostess knows that the third professor does not want coffee. 19. *A* is a knight and *B* is a knave. 21. *A* is a knight and *B* is a knight. 23. *A* is a knave and *B* is a knight. 25. *A* is the knight, *B* is the spy, *C* is the knave. 27. *A* is the knight, *B* is the spy, *C* is the knave. 29. Any of the three can be the knight, any can be the spy, any can be the knave. 31. No solutions 33. In order of decreasing salary: Fred, Maggie, Janice 35. The detective can determine that the butler and cook are lying but cannot determine whether the gardener is telling the truth or whether the handyman is telling the truth. 37. The Japanese man owns the zebra, and the Norwegian drinks water. 39. One honest, 49 corrupt 41. **a)** $\neg(p \wedge (q \vee \neg r))$ **b)** $((\neg p) \wedge (\neg q)) \vee (p \wedge r)$

43.



Section 1.3

1. The equivalences follow by showing that the appropriate pairs of columns of this table agree.

p	$p \wedge \mathbf{T}$	$p \vee \mathbf{F}$	$p \wedge \mathbf{F}$	$p \vee \mathbf{T}$	$p \vee p$	$p \wedge p$
T	T	T	F	T	T	T
F	F	F	F	T	F	F

3. **a)**

p	q	$p \vee q$	$q \vee p$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

b)

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

5.

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

7. **a)** Jan is not rich, or Jan is not happy. **b)** Carlos will not bicycle tomorrow, and Carlos will not run tomorrow. **c)** Mei does not walk to class, and Mei does not take the bus to class. **d)** Ibrahim is not smart, or Ibrahim is not hard working.

9. **a)**

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

b)

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

c)

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

d)

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

e)

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

f)

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

11. In each case we will show that if the hypothesis is true, then the conclusion is also. **a)** If the hypothesis $p \wedge q$ is true, then by the definition of conjunction, the conclusion p must also be true. **b)** If the hypothesis p is true, by the definition of disjunction, the conclusion $p \vee q$ is also true. **c)** If the hypothesis $\neg p$ is true, that is, if p is false, then the conclusion $p \to q$ is true. **d)** If the hypothesis $p \wedge q$ is true, then both p and q are true, so the conclusion $p \to q$ is also true. **e)** If the hypothesis $\neg(p \to q)$ is true, then $p \to q$ is false, so the conclusion p is true (and q is false). **f)** If the hypothesis $\neg(p \to q)$ is true, then $p \to q$ is false, so p is true and q is false. Hence, the conclusion $\neg q$ is true. 13. That the fourth column of the truth table shown is identical to the first column proves part (a), and that the sixth column is identical to the first column proves part (b).

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

15. It is a tautology. 17. Each of these is true precisely when p and q have opposite truth values. 19. The proposition $\neg p \leftrightarrow q$ is true when $\neg p$ and q have the same truth values, which means that p and q have different truth values. Similarly, $p \leftrightarrow \neg q$ is true in exactly the same cases. Therefore, these two expressions are logically equivalent. 21. The proposition $\neg(p \leftrightarrow q)$ is true when $p \leftrightarrow q$ is false, which means that p and q have different truth values. Because this is precisely when $\neg p \leftrightarrow q$ is true, the two expressions are logically equivalent. 23. For $(p \to r) \wedge (q \to r)$ to be false, one of the two conditional statements must be false, which happens exactly when r is false and at least one of p and q is true. But these are precisely the cases in which $p \vee q$ is true and r is false, which is precisely when $(p \vee q) \to r$ is false. Because the two propositions are false in exactly the same situations, they are logically equivalent. 25. For $(p \to r) \vee (q \to r)$ to be false, both of the two conditional statements must be false, which happens exactly when r is false and both p and q are true. But this is precisely the case in which $p \wedge q$ is true and r is false, which is precisely when $(p \wedge q) \to r$ is false. Because the two propositions are false in exactly the same situations, they are logically equivalent. 27. This fact was observed in Section 1 when the biconditional was first defined. Each of these is true precisely when p and q have the same truth values. 29. The last column is all Ts.

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

31. These are not logically equivalent because when p, q, and r are all false, $(p \to q) \to r$ is false, but $p \to (q \to r)$ is true. 33. Many answers are possible. If we let r be true and p, q, and s be false, then $(p \to q) \to (r \to s)$ will be false, but $(p \to r) \to (q \to s)$ will be true. 35. **a)** $p \vee \neg q \vee \neg r$ **b)** $(p \vee q \vee r) \wedge s$ **c)** $(p \wedge \mathbf{T}) \vee (q \wedge \mathbf{F})$ 37. If we take duals twice, every $\vee$ changes to an $\wedge$ and then back to an $\vee$, every $\wedge$ changes to an $\vee$ and then back to an $\wedge$, every **T** changes to an **F** and then back to a **T**, every **F** changes to a **T** and then back to an **F**. Hence, $(s^*)^* = s$. 39. Let p and q be equivalent compound propositions involving only the operators $\wedge$, $\vee$, and $\neg$, and **T** and **F**. Note that $\neg p$ and $\neg q$ are also equivalent. Use De Morgan's laws as many times as necessary to push negations in as far as possible within these compound propositions, changing $\vee$s to $\wedge$s, and vice versa, and changing **T**s to **F**s, and vice versa. This shows that $\neg p$ and $\neg q$ are the same as p^* and q^* except that each atomic proposition p_i within them is replaced by its negation. From this we can conclude that p^* and q^* are equivalent because $\neg p$ and $\neg q$

are. 41. $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$ 43. Given a compound proposition p, form its truth table and then write down a proposition q in disjunctive normal form that is logically equivalent to p. Because q involves only $\neg$, $\wedge$, and $\vee$, this shows that these three operators form a functionally complete set. 45. By Exercise 43, given a compound proposition p, we can write down a proposition q that is logically equivalent to p and involves only $\neg$, $\wedge$, and $\vee$. By De Morgan's law we can eliminate all the $\wedge$'s by replacing each occurrence of $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ with $\neg(\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n)$. 47. $\neg(p \wedge q)$ is true when either p or q, or both, are false, and is false when both p and q are true. Because this was the definition of $p \mid q$, the two compound propositions are logically equivalent. 49. $\neg(p \vee q)$ is true when both p and q are false, and is false otherwise. Because this was the definition of $p \downarrow q$, the two are logically equivalent. 51. $((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$ 53. This follows immediately from the truth table or definition of $p \mid q$. 55. 16 57. If the database is open, then either the system is in its initial state or the monitor is put in a closed state. 59. All nine 61. **a)** Satisfiable **b)** Not satisfiable **c)** Not satisfiable 63. Use the same propositions as were given in the text for a 9×9 Sudoku puzzle, with the variables indexed from 1 to 4, instead of from 1 to 9, and with a similar change for the propositions for the 2×2 blocks: $\bigwedge_{r=0}^{1} \bigwedge_{s=0}^{1} \bigwedge_{n=1}^{4} \bigvee_{i=1}^{2} \bigvee_{j=1}^{2} p(2r+i, 2s+j, n)$ 65. $\bigvee_{i=1}^{9} p(i, j, n)$ asserts that column j contains the number n, so $\bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$ asserts that column j contains all 9 numbers; therefore $\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$ asserts that every column contains every number.

Section 1.4

1. **a)** T **b)** T **c)** F 3. **a)** T **b)** F **c)** F **d)** F 5. **a)** There is a student who spends more than 5 hours every weekday in class. **b)** Every student spends more than 5 hours every weekday in class. **c)** There is a student who does not spend more than 5 hours every weekday in class. **d)** No student spends more than 5 hours every weekday in class. 7. **a)** Every comedian is funny. **b)** Every person is a funny comedian. **c)** There exists a person such that if she or he is a comedian, then she or he is funny. **d)** Some comedians are funny. 9. **a)** $\exists x(P(x) \wedge Q(x))$ **b)** $\exists x(P(x) \wedge \neg Q(x))$ **c)** $\forall x(P(x) \vee Q(x))$ **d)** $\forall x \neg(P(x) \vee Q(x))$ 11. **a)** T **b)** T **c)** F **d)** F **e)** T **f)** F 13. **a)** T **b)** T **c)** T **d)** T 15. **a)** T **b)** F **c)** T **d)** F 17. **a)** $P(0) \vee P(1) \vee P(2) \vee P(3) \vee P(4)$ **b)** $P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge P(4)$ **c)** $\neg P(0) \vee \neg P(1) \vee \neg P(2) \vee \neg P(3) \vee \neg P(4)$ **d)** $\neg P(0) \wedge \neg P(1) \wedge \neg P(2) \wedge \neg P(3) \wedge \neg P(4)$ **e)** $\neg(P(0) \vee P(1) \vee P(2) \vee P(3) \vee P(4))$ **f)** $\neg(P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge P(4))$ 19. **a)** $P(1) \vee P(2) \vee P(3) \vee P(4) \vee P(5)$ **b)** $P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5)$ **c)** $\neg(P(1) \vee P(2) \vee P(3) \vee P(4) \vee P(5))$ **d)** $\neg(P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5))$ **e)** $(P(1) \wedge P(2) \wedge P(4) \wedge P(5)) \vee (\neg P(1) \vee \neg P(2) \vee \neg P(3) \vee \neg P(4) \vee \neg P(5))$ 21. Many answers are possible. **a)** All students in your discrete mathematics class; all students in the world **b)** All United States senators; all college football players **c)** George W. Bush and Jeb Bush; all politicians in the United States **d)** Bill Clinton and George W. Bush; all politicians in the United States 23. Let $C(x)$ be the propositional function "x is in your class." **a)** $\exists x H(x)$ and $\exists x(C(x) \wedge H(x))$, where $H(x)$ is "x can speak Hindi" **b)** $\forall x F(x)$ and $\forall x(C(x) \rightarrow F(x))$, where $F(x)$ is "x is friendly" **c)** $\exists x \neg B(x)$ and $\exists x(C(x) \wedge \neg B(x))$, where $B(x)$ is "x was born in California" **d)** $\exists x M(x)$ and $\exists x(C(x) \wedge M(x))$, where $M(x)$ is "x has been in a movie" **e)** $\forall x \neg L(x)$ and $\forall x(C(x) \rightarrow \neg L(x))$, where $L(x)$ is "x has taken a course in logic programming" 25. Let $P(x)$ be "x is perfect"; let $F(x)$ be "x is your friend"; and let the domain be all people. **a)** $\forall x \neg P(x)$ **b)** $\neg \forall x\, P(x)$ **c)** $\forall x(F(x) \rightarrow P(x))$ **d)** $\exists x(F(x) \wedge P(x))$ **e)** $\forall x(F(x) \wedge P(x))$ or $(\forall x\, F(x)) \wedge (\forall x\, P(x))$ **f)** $(\neg \forall x\, F(x)) \vee (\exists x \neg P(x))$ 27. Let $Y(x)$ be the propositional function that x is in your school or class, as appropriate. **a)** If we let $V(x)$ be "x has lived in Vietnam," then we have $\exists x V(x)$ if the domain is just your schoolmates, or $\exists x(Y(x) \wedge V(x))$ if the domain is all people. If we let $D(x, y)$ mean that person x has lived in country y, then we can rewrite this last one as $\exists x(Y(x) \wedge D(x, \text{Vietnam}))$. **b)** If we let $H(x)$ be "x can speak Hindi," 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 $S(x, y)$ mean that person x can speak language y, then we can rewrite this last one as $\exists x(Y(x) \wedge \neg S(x, \text{Hindi}))$. **c)** If we let $J(x)$, $P(x)$, and $C(x)$ be the propositional functions asserting x's knowledge of Java, Prolog, and C++, respectively, then we have $\exists x(J(x) \wedge P(x) \wedge C(x))$ if the domain is just your schoolmates, or $\exists x(Y(x) \wedge J(x) \wedge P(x) \wedge C(x))$ if the domain is all people. If we let $K(x, y)$ mean that person x knows programming language y, then we can rewrite this last one as $\exists x(Y(x) \wedge K(x, \text{Java}) \wedge K(x, \text{Prolog}) \wedge K(x, \text{C++}))$. **d)** If we let $T(x)$ be "x enjoys Thai food," then we have $\forall x\, T(x)$ if the domain is just your classmates, or $\forall x(Y(x) \rightarrow T(x))$ if the domain is all people. If we let $E(x, y)$ mean that person x enjoys food of type y, then we can rewrite this last one as $\forall x(Y(x) \rightarrow E(x, \text{Thai}))$. **e)** If we let $H(x)$ be "x plays hockey," then we have $\exists x \neg H(x)$ if the domain is just your classmates, or $\exists x(Y(x) \wedge \neg H(x))$ if the domain is all people. If we let $P(x, y)$ mean that person x plays game y, then we can rewrite this last one as $\exists x(Y(x) \wedge \neg P(x, \text{hockey}))$. 29. Let $T(x)$ mean that x is a tautology and $C(x)$ mean that x is a contradiction. **a)** $\exists x\, T(x)$ **b)** $\forall x(C(x) \rightarrow T(\neg x))$ **c)** $\exists x \exists y(\neg T(x) \wedge \neg C(x) \wedge \neg T(y) \wedge \neg C(y) \wedge T(x \vee y))$ **d)** $\forall x \forall y((T(x) \wedge T(y)) \rightarrow T(x \wedge y))$ 31. **a)** $Q(0,0,0) \wedge Q(0,1,0)$ **b)** $Q(0,1,1) \vee Q(1,1,1) \vee Q(2,1,1)$ **c)** $\neg Q(0,0,0) \vee \neg Q(0,0,1)$ **d)** $\neg Q(0,0,1) \vee \neg Q(1,0,1) \vee \neg Q(2,0,1)$ 33. **a)** Let $T(x)$ be the predicate that x can learn new tricks, and let the domain be old dogs. Original is $\exists x\, T(x)$. Negation is $\forall x \neg T(x)$: "No old dogs can learn new tricks." **b)** Let $C(x)$ be the predicate that x knows calculus, and let the domain be rabbits. Original is $\neg \exists x\, C(x)$.

Negation is $\exists x\, C(x)$: "There is a rabbit that knows calculus." **c)** Let $F(x)$ be the predicate that x can fly, and let the domain be birds. Original is $\forall x\ F(x)$. Negation is $\exists x\ \neg F(x)$: "There is a bird who cannot fly." **d)** Let $T(x)$ be the predicate that x can talk, and let the domain be dogs. Original is $\neg\exists x\ T(x)$. Negation is $\exists x\ T(x)$: "There is a dog that talks." **e)** Let $F(x)$ and $R(x)$ be the predicates that x knows French and knows Russian, respectively, and let the domain be people in this class. Original is $\neg\exists x(F(x) \wedge R(x))$. Negation is $\exists x(F(x) \wedge R(x))$: "There is someone in this class who knows French and Russian." **35. a)** There is no counterexample. **b)** $x = 0$ **c)** $x = 2$ **37. a)** $\forall x((F(x, 25{,}000) \vee S(x, 25)) \to E(x))$, where $E(x)$ is "Person x qualifies as an elite flyer in a given year," $F(x, y)$ is "Person x flies more than y miles in a given year," and $S(x, y)$ is "Person x takes more than y flights in a given year" **b)** $\forall x(((M(x) \wedge T(x, 3)) \vee (\neg M(x) \wedge T(x, 3.5))) \to Q(x))$, where $Q(x)$ is "Person x qualifies for the marathon," $M(x)$ is "Person x is a man," and $T(x, y)$ is "Person x has run the marathon in less than y hours" **c)** $M \to ((H(60) \vee (H(45) \wedge T)) \wedge \forall y\, G(\mathrm{B}, y))$, where M is the proposition "The student received a masters degree," $H(x)$ is "The student took at least x course hours," T is the proposition "The student wrote a thesis," and $G(x, y)$ is "The person got grade x or higher in course y" **d)** $\exists x\ ((T(x, 21) \wedge G(x, 4.0))$, where $T(x, y)$ is "Person x took more than y credit hours" and $G(x, p)$ is "Person x earned grade point average p" (we assume that we are talking about one given semester) **39. a)** If there is a printer that is both out of service and busy, then some job has been lost. **b)** If every printer is busy, then there is a job in the queue. **c)** If there is a job that is both queued and lost, then some printer is out of service. **d)** If every printer is busy and every job is queued, then some job is lost. **41. a)** $(\exists x\ F(x, 10)) \to \exists x\ S(x)$, where $F(x, y)$ is "Disk x has more than y kilobytes of free space," and $S(x)$ is "Mail message x can be saved" **b)** $(\exists x\ A(x)) \to \forall x(Q(x) \to T(x))$, where $A(x)$ is "Alert x is active," $Q(x)$ is "Message x is queued," and $T(x)$ is "Message x is transmitted" **c)** $\forall x((x \neq \text{main console}) \to T(x))$, where $T(x)$ is "The diagnostic monitor tracks the status of system x" **d)** $\forall x(\neg L(x) \to B(x))$, where $L(x)$ is "The host of the conference call put participant x on a special list" and $B(x)$ is "Participant x was billed" **43.** They are not equivalent. Let $P(x)$ be any propositional function that is sometimes true and sometimes false, and let $Q(x)$ be any propositional function that is always false. Then $\forall x(P(x) \to Q(x))$ is false but $\forall x\, P(x) \to \forall x\, Q(x)$ is true. **45.** Both statements are true precisely when at least one of $P(x)$ and $Q(x)$ is true for at least one value of x in the domain. **47. a)** If A is true, then both sides are logically equivalent to $\forall x\, P(x)$. If A is false, the left-hand side is clearly false. Furthermore, for every x, $P(x) \wedge A$ is false, so the right-hand side is false. Hence, the two sides are logically equivalent. **b)** If A is true, then both sides are logically equivalent to $\exists x\ P(x)$. If A is false, the left-hand side is clearly false. Furthermore, for every x, $P(x) \wedge A$ is false, so $\exists x(P(x) \wedge A)$ is false. Hence, the two sides are logically equivalent. **49.** We can establish these equivalences by arguing that one side is true if and only if the other side is true. **a)** Suppose that A is true. Then for each x, $P(x) \to A$ is true; therefore the left-hand side is always true in this case. By similar reasoning the right-hand side is always true in this case. Therefore, the two propositions are logically equivalent when A is true. On the other hand, suppose that A is false. There are two subcases. If $P(x)$ is false for every x, then $P(x) \to A$ is vacuously true, so the left-hand side is vacuously true. The same reasoning shows that the right-hand side is also true, because in this subcase $\exists x\, P(x)$ is false. For the second subcase, suppose that $P(x)$ is true for some x. Then for that x, $P(x) \to A$ is false, so the left-hand side is false. The right-hand side is also false, because in this subcase $\exists x\, P(x)$ is true but A is false. Thus in all cases, the two propositions have the same truth value. **b)** If A is true, then both sides are trivially true, because the conditional statements have true conclusions. If A is false, then there are two subcases. If $P(x)$ is false for some x, then $P(x) \to A$ is vacuously true for that x, so the left-hand side is true. The same reasoning shows that the right-hand side is true, because in this subcase $\forall x\, P(x)$ is false. For the second subcase, suppose that $P(x)$ is true for every x. Then for every x, $P(x) \to A$ is false, so the left-hand side is false (there is no x making the conditional statement true). The right-hand side is also false, because it is a conditional statement with a true hypothesis and a false conclusion. Thus in all cases, the two propositions have the same truth value. **51.** To show these are not logically equivalent, let $P(x)$ be the statement "x is positive," and let $Q(x)$ be the statement "x is negative" with domain the set of integers. Then $\exists x\ P(x) \wedge \exists x\ Q(x)$ is true, but $\exists x(P(x) \wedge Q(x))$ is false. **53. a)** True **b)** False, unless the domain consists of just one element **c)** True **55. a)** Yes **b)** No **c)** juana, kiko **d)** math273, cs301 **e)** juana, kiko **57.** `sibling(X,Y) :- mother(M,X), mother(M,Y), father(F,X), father(F,Y)` **59. a)** $\forall x(P(x) \to \neg Q(x))$ **b)** $\forall x(Q(x) \to R(x))$ **c)** $\forall x(P(x) \to \neg R(x))$ **d)** The conclusion does not follow. There may be vain professors, because the premises do not rule out the possibility that there are other vain people besides ignorant ones. **61. a)** $\forall x(P(x) \to \neg Q(x))$ **b)** $\forall x(R(x) \to \neg S(x))$ **c)** $\forall x(\neg Q(x) \to S(x))$ **d)** $\forall x(P(x) \to \neg R(x))$ **e)** The conclusion follows. Suppose x is a baby. Then by the first premise, x is illogical, so by the third premise, x is despised. The second premise says that if x could manage a crocodile, then x would not be despised. Therefore, x cannot manage a crocodile.

Section 1.5

1. a) For every real number x there exists a real number y such that x is less than y. **b)** For every real number x and real number y, if x and y are both nonnegative, then their product is nonnegative. **c)** For every real number x and real number y, there exists a real number z such that $xy = z$. **3. a)** There is some student in your class who has sent a message to some student in your class. **b)** There is some student in your class who has sent a message to every student in your class. **c)** Every student in your class has sent a message to at least one student in your class. **d)** There is a student in your class who has been sent a message by every student in your class. **e)** Every student in your class has been sent a message from at least one student in your class. **f)** Every student in the class has sent a message to every student in the class. 5. **a)** Sarah Smith has visited www.att.com. **b)** At least one person has visited www.imdb.org. **c)** Jose Orez has visited at least one website. **d)** There is a website that both Ashok Puri and Cindy Yoon have visited. **e)** There is a person besides David Belcher who has visited all the websites that David Belcher has visited. **f)** There are two different people who have visited exactly the same websites. 7. **a)** Abdallah Hussein does not like Japanese cuisine. **b)** Some student at your school likes Korean cuisine, and everyone at your school likes Mexican cuisine. **c)** There is some cuisine that either Monique Arsenault or Jay Johnson likes. **d)** For every pair of distinct students at your school, there is some cuisine that at least one them does not like. **e)** There are two students at your school who like exactly the same set of cuisines. **f)** For every pair of students at your school, there is some cuisine about which they have the same opinion (either they both like it or they both do not like it). 9. **a)** $\forall x L(x, \text{Jerry})$ **b)** $\forall x \exists y L(x, y)$ **c)** $\exists y \forall x L(x, y)$ **d)** $\forall x \exists y \neg L(x, y)$ **e)** $\exists x \neg L(\text{Lydia}, x)$ **f)** $\exists x \forall y \neg L(y, x)$ **g)** $\exists x(\forall y L(y, x) \wedge \forall z((\forall w L(w, z)) \rightarrow z = x))$ **h)** $\exists x \exists y(x \neq y \wedge L(\text{Lynn}, x) \wedge L(\text{Lynn}, y) \wedge \forall z(L(\text{Lynn}, z) \rightarrow (z = x \vee z = y)))$ **i)** $\forall x L(x, x)$ **j)** $\exists x \forall y (L(x,y) \leftrightarrow x = y)$ 11. **a)** $A(\text{Lois, Professor Michaels})$ **b)** $\forall x(S(x) \rightarrow A(x, \text{Professor Gross}))$ **c)** $\forall x(F(x) \rightarrow (A(x, \text{Professor Miller}) \vee A(\text{Professor Miller}, x)))$ **d)** $\exists x(S(x) \wedge \forall y(F(y) \rightarrow \neg A(x, y)))$ **e)** $\exists x(F(x) \wedge \forall y(S(y) \rightarrow \neg A(y,x)))$ **f)** $\forall y(F(y) \rightarrow \exists x(S(x) \vee A(x,y)))$ **g)** $\exists x(F(x) \wedge \forall y((F(y) \wedge (y \neq x)) \rightarrow A(x,y)))$ **h)** $\exists x(S(x) \wedge \forall y(F(y) \rightarrow \neg A(y, x)))$ 13. **a)** $\neg M$ (Chou, Koko) **b)** $\neg M(\text{Arlene, Sarah}) \wedge \neg T(\text{Arlene, Sarah})$ **c)** $\neg M$ (Deborah, Jose) **d)** $\forall x M(x, \text{Ken})$ **e)** $\forall x \neg T(x, \text{Nina})$ **f)** $\forall x(T\text{-}x, \text{Avi}) \vee M(x, \text{Avi}))$ **g)** $\exists x \forall y(y \neq x \rightarrow M(x, y))$ **h)** $\exists x \forall y(y \neq x \rightarrow (M(x, y) \vee T(x, y)))$ **i)** $\exists x \exists y(x \neq y \wedge M(x, y) \wedge M(y, x))$ **j)** $\exists x M(x, x)$ **k)** $\exists x \forall y(x \neq y \rightarrow (\neg M(x, y) \wedge \neg T(y, x)))$ **l)** $\forall x(\exists y(x \neq y \wedge (M(y, x) \vee T(y, x))))$ **m)** $\exists x \exists y(x \neq y \wedge M(x, y) \wedge T(y, x))$ **n)** $\exists x \exists y(x \neq y \wedge \forall z((z \neq x \wedge z \neq y) \rightarrow (M(x, z) \vee M(y, z) \vee T(x, z) \vee T(y, z))))$ 15. **a)** $\forall x P(x)$, where $P(x)$ is "x needs a course in discrete mathematics" and the domain consists of all computer science students **b)** $\exists x P(x)$, where $P(x)$ is "x owns a personal computer" and the domain consists of all students in this class **c)** $\forall x \exists y P(x, y)$, where $P(x, y)$ is "x has taken y," the domain for x consists of all students in this class, and the domain for y consists of all computer science classes **d)** $\exists x \exists y P(x, y)$, where $P(x, y)$ and domains are the same as in part (c) **e)** $\forall x \forall y P(x, y)$, where $P(x, y)$ is "x has been in y," the domain for x consists of all students in this class, and the domain for y consists of all buildings on campus **f)** $\exists x \exists y \forall z(P(z, y) \rightarrow Q(x, z))$, where $P(z, y)$ is "z is in y" and $Q(x, z)$ is "x has been in z"; the domain for x consists of all students in the class, the domain for y consists of all buildings on campus, and the domain of z consists of all rooms. **g)** $\forall x \forall y \exists z(P(z, y) \wedge Q(x, z))$, with same environment as in part (f) 17. **a)** $\forall u \exists m(A(u, m) \wedge \forall n(n \neq m \rightarrow \neg A(u, n)))$, where $A(u, m)$ means that user u has access to mailbox m **b)** $\exists p \forall e(H(e) \wedge S(p, \text{running})) \rightarrow S$ (kernel, working correctly), where $H(e)$ means that error condition e is in effect and $S(x, y)$ means that the status of x is y **c)** $\forall u \forall s(E(s, .\text{edu}) \rightarrow A(u, s))$, where $E(s, x)$ means that website s has extension x, and $A(u, s)$ means that user u can access website s **d)** $\exists x \exists y(x \neq y \wedge \forall z((\forall s\, M(z,s)) \leftrightarrow (z = x \vee z = y)))$, where $M(a, b)$ means that system a monitors remote server b 19. **a)** $\forall x \forall y((x < 0) \wedge (y < 0) \rightarrow (x + y < 0))$ **b)** $\neg \forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow (x - y > 0))$ **c)** $\forall x \forall y\, (x^2 + y^2 \geq (x + y)^2)$ **d)** $\forall x \forall y\, (|xy| = |x||y|)$ 21. $\forall x \exists a \exists b \exists c \exists d\, ((x > 0) \rightarrow x = a^2 + b^2 + c^2 + d^2)$, where the domain consists of all integers 23. **a)** $\forall x\, \forall y\, ((x < 0) \wedge (y < 0) \rightarrow (xy > 0))$ **b)** $\forall x(x - x = 0)$ **c)** $\forall x \exists a \exists b(a \neq b \wedge \forall c(c^2 = x \leftrightarrow (c = a \vee c = b)))$ **d)** $\forall x((x < 0) \rightarrow \neg \exists y(x = y^2))$ 25. **a)** There is a multiplicative identity for the real numbers. **b)** The product of two negative real numbers is always a positive real number. **c)** There exist real numbers x and y such that x^2 exceeds y but x is less than y. **d)** The real numbers are closed under the operation of addition. 27. **a)** True **b)** True **c)** True **d)** True **e)** True **f)** False **g)** False **h)** True **i)** False 29. **a)** $P(1,1) \wedge P(1,2) \wedge P(1,3) \wedge P(2,1) \wedge P(2,2) \wedge P(2, 3) \wedge P(3, 1) \wedge P(3, 2) \wedge P(3, 3)$ **b)** $P(1, 1) \vee P(1, 2) \vee P(1, 3) \vee P(2, 1) \vee P(2, 2) \vee P(2, 3) \vee P(3,1) \vee P(3, 2) \vee P(3, 3)$ **c)** $(P(1, 1) \wedge P(1, 2) \wedge P(1, 3)) \vee (P(2, 1) \wedge P(2, 2) \wedge P(2, 3)) \vee (P(3, 1) \wedge P(3, 2) \wedge P(3, 3))$ **d)** $(P(1, 1) \vee P(2, 1) \vee P(3, 1)) \wedge (P(1, 2) \vee P(2, 2) \vee P(3, 2)) \wedge (P(1, 3) \vee P(2, 3) \vee P(3, 3))$ 31. **a)** $\exists x \forall y \exists z \neg T(x, y, z)$ **b)** $\exists x \forall y \neg P(x, y) \wedge \exists x \forall y \neg Q(x, y)$ **c)** $\exists x \forall y (\neg P(x, y) \vee \forall z \neg R(x, y, z))$ **d)** $\exists x \forall y(P(x, y) \wedge \neg Q(x, y))$ 33. **a)** $\exists x \exists y \neg P(x, y)$ **b)** $\exists y \forall x \neg P(x, y)$ **c)** $\exists y \exists x (\neg P(x, y) \wedge \neg Q(x, y))$ **d)** $(\forall x \forall y P(x, y)) \vee (\exists x \exists y \neg Q(x, y))$ **e)** $\exists x(\forall y \exists z \neg P(x,y,z) \vee \forall z \exists y \neg P(x, y, z))$ 35. Any domain with four or more members makes the statement true; any domain with three or fewer members makes the statement false. 37. **a)** There is someone in this class such that for every two different math courses, these are not the two and only two math courses this person has taken. **b)** Every person has either visited Libya or has not visited a country other than Libya. **c)** Someone has climbed every mountain in the Himalayas. **d)** There is someone who has neither been in a movie with Kevin Bacon nor has been in a movie with someone who has been in a movie with Kevin Bacon. 39. **a)** $x = 2, y = -2$ **b)** $x = -4$ **c)** $x = 17, y = -1$ 41. $\forall x\, \forall y\, \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$ 43. $\forall m \forall b(m \neq 0 \rightarrow \exists x(mx + b = 0 \wedge \forall w(mw + b = 0 \rightarrow w = x)))$ 45. **a)** True **b)** False **c)** True 47. $\neg(\exists x \forall y P(x, y)) \leftrightarrow \forall x(\neg \forall y P(x, y)) \leftrightarrow \forall x \exists y \neg P(x,y)$ 49. **a)** Suppose that $\forall x P(x) \wedge \exists x Q(x)$ is true. Then $P(x)$ is true for all x and there is an element y for which $Q(y)$ is true. Because $P(x) \wedge Q(y)$ is true for all x and there is a y for which $Q(y)$ is true, $\forall x \exists y (P(x) \wedge Q(y))$ is true. Conversely, suppose that the second proposition is true. Let x be an element in the domain. There is a y such that $Q(y)$ is true, so $\exists x Q(x)$ is true. Because $\forall x P(x)$ is also true, it follows that the first proposition is true. **b)** Suppose that $\forall x P(x) \vee \exists x Q(x)$ is true. Then either $P(x)$ is true for all x, or there exists a y for which $Q(y)$ is true. In the former case, $P(x) \vee Q(y)$ is true for all x, so $\forall x \exists y (P(x) \vee Q(y))$ is true. In the latter case, $Q(y)$ is true for a particular y, so $P(x) \vee Q(y)$ is true for all x and consequently $\forall x \exists y (P(x) \vee Q(y))$ is true. Conversely, suppose that the second proposition is true. If $P(x)$ is true for all x, then the first proposition is true. If not, $P(x)$ is false for some x, and for this x there must be a y such that $P(x) \vee Q(y)$ is true. Hence, $Q(y)$ must be true, so $\exists y Q(y)$ is true. It follows that the first proposition must hold. 51. We will show how an expression can be put into prenex normal form (PNF) if subexpressions in it can be put into PNF. Then, working from the inside out, any expression can be put in PNF. (To formalize the argument, it is necessary to use the method of structural induction that will be discussed in Section 5.3.) By Exercise 45 of Section 1.4, we can assume that the proposition uses only $\vee$ and $\neg$ as logical connectives. Now note that any proposition with no quantifiers is already in PNF. (This is the basis case of the argument.) Now suppose that the proposition is of the form $QxP(x)$, where Q is a quantifier. Because $P(x)$ is a shorter expression than the original proposition, we can put it into PNF. Then Qx followed by this PNF is again in PNF and is equivalent to the original proposition. Next, suppose that the proposition is of the form $\neg P$. If P is already in PNF, we slide the negation sign past all the quantifiers using the equivalences in Table 2 in Section 1.4. Finally, assume that proposition is of the form $P \vee Q$, where each of P and Q is in PNF. If only one of P and Q has quantifiers, then we can use Exercise 46 in Section 1.4 to bring the quantifier in front of both. If both P and Q have quantifiers, we can use Exercise 45 in Section 1.4, Exercise 48, or part (b) of Exercise 49 to rewrite $P \vee Q$ with two quantifiers preceding the disjunction of a proposition of the form $R \vee S$, and then put $R \vee S$ into PNF.

Section 1.6

1. Modus ponens; valid; the conclusion is true, because the hypotheses are true. 3. **a)** Addition **b)** Simplification **c)** Modus ponens **d)** Modus tollens **e)** Hypothetical syllogism 5. Let w be "Randy works hard," let d be "Randy is a dull boy," and let j be "Randy will get the job." The hypotheses are w, $w \rightarrow d$, and $d \rightarrow \neg j$. Using modus ponens and the first two hypotheses, d follows. Using modus ponens and the last hypothesis, $\neg j$, which is the desired conclusion, "Randy will not get the job," follows. 7. Universal instantiation is used to conclude that "If Socrates is a man, then Socrates is mortal." Modus ponens is then used to conclude that Socrates is mortal. 9. **a)** Valid conclusions are "I did not take Tuesday off," "I took Thursday off," "It rained on Thursday." **b)** "I did not eat spicy foods and it did not thunder" is a valid conclusion. **c)** "I am clever" is a valid conclusion. **d)** "Ralph is not a CS major" is a valid conclusion. **e)** "That you buy lots of stuff is good for the U.S. and is good for you" is a valid conclusion. **f)** "Mice gnaw their food" and "Rabbits are not rodents" are valid conclusions. 11. Suppose that $p_1, p_2, \ldots, p_n$ are true. We want to establish that $q \rightarrow r$ is true. If q is false, then we are done, vacuously. Otherwise, q is true, so by the validity of the given argument form (that whenever $p_1, p_2, \ldots, p_n, q$ are true, then r must be true), we know that r is true. 13. **a)** Let $c(x)$ be "x is in this class," $j(x)$ be "x knows how to write programs in JAVA," and $h(x)$ be "x can get a high-paying job." The premises are c(Doug), j(Doug), $\forall x (j(x) \rightarrow h(x))$. Using universal instantiation and the last premise, $j(\text{Doug}) \rightarrow h(\text{Doug})$ follows. Applying modus ponens to this conclusion and the second premise, h(Doug) follows. Using conjunction and the first premise, $c(\text{Doug}) \wedge h(\text{Doug})$ follows. Finally, using existential generalization, the desired conclusion, $\exists x (c(x) \wedge h(x))$ follows. **b)** Let $c(x)$ be "x is in this class," $w(x)$ be "x enjoys whale watching," and $p(x)$ be "x cares about ocean pollution." The premises are $\exists x (c(x) \wedge w(x))$ and $\forall x (w(x) \rightarrow p(x))$. From the first premise, $c(y) \wedge w(y)$ for a particular person y. Using simplification, $w(y)$ follows. Using the second premise and universal instantiation, $w(y) \rightarrow p(y)$ follows. Using modus ponens, $p(y)$ follows, and by conjunction, $c(y) \wedge p(y)$ follows. Finally, by existential generalization, the desired conclusion, $\exists x (c(x) \wedge p(x))$, follows. **c)** Let $c(x)$ be "x is in this class," $p(x)$ be "x owns a PC," and $w(x)$ be "x can use a word-processing program." The premises are c(Zeke), $\forall x (c(x) \rightarrow p(x))$, and $\forall x (p(x) \rightarrow w(x))$. Using the second premise and universal instantiation, $c(\text{Zeke}) \rightarrow p(\text{Zeke})$ follows. Using the first premise and modus ponens, p(Zeke) follows. Using the third premise and universal instantiation, $p(\text{Zeke}) \rightarrow w(\text{Zeke})$ follows. Finally, using modus ponens, w(Zeke), the desired conclusion, follows. **d)** Let $j(x)$ be "x is in New Jersey," $f(x)$ be "x lives within 50 miles of the ocean," and $s(x)$ be "x has seen the ocean." The premises are $\forall x (j(x) \rightarrow f(x))$ and $\exists x (j(x) \wedge \neg s(x))$. The second hypothesis and existential instantiation imply that $j(y) \wedge \neg s(y)$ for a particular person y. By simplification, $j(y)$ for this person y. Using universal instantiation and the first premise, $j(y) \rightarrow f(y)$, and by modus ponens, $f(y)$ follows. By simplification, $\neg s(y)$ follows from $j(y) \wedge \neg s(y)$. So $f(y) \wedge \neg s(y)$ follows by conjunction. Finally, the desired conclusion, $\exists x (f(x) \wedge \neg s(x))$, follows by existential generalization. 15. **a)** Correct, using universal instantiation and modus ponens **b)** Invalid; fallacy of affirming the conclusion **c)** Invalid; fallacy of denying the hypothesis **d)** Correct, using universal instantiation and modus tollens 17. We know that *some* x exists that makes

$H(x)$ true, but we cannot conclude that Lola is one such x. 19. **a)** Fallacy of affirming the conclusion **b)** Fallacy of begging the question **c)** Valid argument using modus tollens **d)** Fallacy of denying the hypothesis 21. By the second premise, there is some lion that does not drink coffee. Let Leo be such a creature. By simplification we know that Leo is a lion. By modus ponens we know from the first premise that Leo is fierce. Hence, Leo is fierce and does not drink coffee. By the definition of the existential quantifier, there exist fierce creatures that do not drink coffee, that is, some fierce creatures do not drink coffee. 23. The error occurs in step (5), because we cannot assume, as is being done here, that the c that makes P true is the same as the c that makes Q true. 25. We are given the premises $\forall x(P(x) \to Q(x))$ and $\neg Q(a)$. We want to show $\neg P(a)$. Suppose, to the contrary, that $\neg P(a)$ is not true. Then $P(a)$ is true. Therefore by universal modus ponens, we have $Q(a)$. But this contradicts the given premise $\neg Q(a)$. Therefore our supposition must have been wrong, and so $\neg P(a)$ is true, as desired.

27.

Step	**Reason**
1. $\forall x(P(x) \wedge R(x))$	Premise
2. $P(a) \wedge R(a)$	Universal instantiation from (1)
3. $P(a)$	Simplification from (2)
4. $\forall x(P(x) \to (Q(x) \wedge S(x)))$	Premise
5. $Q(a) \wedge S(a)$	Universal modus ponens from (3) and (4)
6. $S(a)$	Simplification from (5)
7. $R(a)$	Simplification from (2)
8. $R(a) \wedge S(a)$	Conjunction from (7) and (6)
9. $\forall x(R(x) \wedge S(x))$	Universal generalization from (5)

29.

Step	**Reason**
1. $\exists x \neg P(x)$	Premise
2. $\neg P(c)$	Existential instantiation from (1)
3. $\forall x(P(x) \vee Q(x))$	Premise
4. $P(c) \vee Q(c)$	Universal instantiation from (3)
5. $Q(c)$	Disjunctive syllogism from (4) and (2)
6. $\forall x(\neg Q(x) \vee S(x))$	Premise
7. $\neg Q(c) \vee S(c)$	Universal instantiation from (6)
8. $S(c)$	Disjunctive syllogism from (5) and (7)
9. $\forall x(R(x) \to \neg S(x))$	Premise
10. $R(c) \to \neg S(c)$	Universal instantiation from (9)
11. $\neg R(c)$	Modus tollens from (8) and (10)
12. $\exists x \neg R(x)$	Existential generalization from (11)

31. Let p be "It is raining"; let q be "Yvette has her umbrella"; let r be "Yvette gets wet." Assumptions are $\neg p \vee q$, $\neg q \vee \neg r$, and $p \vee \neg r$. Resolution on the first two gives $\neg p \vee \neg r$. Resolution on this and the third assumption gives $\neg r$, as desired. 33. Assume that this proposition is satisfiable. Using resolution on the first two clauses enables us to conclude $q \vee q$; in other words, we know that q has to be true. Using resolution on the last two clauses enables us to conclude $\neg q \vee \neg q$; in other words, we know that $\neg q$ has to be true. This is a contradiction. So this proposition is not satisfiable. 35. Valid

Section 1.7

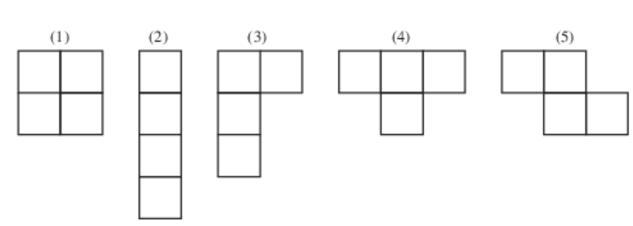
1. Let $n = 2k + 1$ and $m = 2l + 1$ be odd integers. Then $n+m = 2(k+l+1)$ is even. 3. Suppose that n is even. Then $n = 2k$ for some integer k. Therefore, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Because we have written n^2 as 2 times an integer, we conclude that n^2 is even. 5. Direct proof: Suppose that $m+n$ and $n+p$ are even. Then $m+n = 2s$ for some integer s and $n + p = 2t$ for some integer t. If we add these, we get $m + p + 2n = 2s + 2t$. Subtracting $2n$ from both sides and factoring, we have $m + p = 2s + 2t - 2n = 2(s + t - n)$. Because we have written $m + p$ as 2 times an integer, we conclude that $m + p$ is even. 7. Because n is odd, we can write $n = 2k + 1$ for some integer k. Then $(k+1)^2 - k^2 = k^2+2k+1-k^2 = 2k+1 = n$. 9. Suppose that r is rational and i is irrational and $s = r + i$ is rational. Then by Example 7, $s+(-r) = i$ is rational, which is a contradiction. 11. Because $\sqrt{2} \cdot \sqrt{2} = 2$ is rational and $\sqrt{2}$ is irrational, the product of two irrational numbers is not necessarily irrational. 13. Proof by contraposition: If $1/x$ were rational, then by definition $1/x = p/q$ for some integers p and q with $q \neq 0$. Because $1/x$ cannot be 0 (if it were, then we'd have the contradiction $1 = x \cdot 0$ by multiplying both sides by x), we know that $p \neq 0$. Now $x = 1/(1/x) = 1/(p/q) = q/p$ by the usual rules of algebra and arithmetic. Hence, x can be written as the quotient of two integers with the denominator nonzero. Thus by definition, x is rational. 15. Assume that it is not true that $x \geq 1$ or $y \geq 1$. Then $x < 1$ and $y < 1$. Adding these two inequalities, we obtain $x + y < 2$, which is the negation of $x + y \geq 2$. 17. **a)** Assume that n is odd, so $n = 2k+1$ for some integer k. Then $n^3+5 = 2(4k^3+6k^2+3k+3)$. Because $n^3 + 5$ is two times some integer, it is even. **b)** Suppose that $n^3 + 5$ is odd and n is odd. Because n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and then that n^3 is odd. But then $5 = (n^3 + 5) - n^3$ would have to be even because it is the difference of two odd numbers. Therefore, the supposition that $n^3 + 5$ and n were both odd is wrong. 19. The proposition is vacuously true because 0 is not a positive integer. Vacuous proof. 21. $P(1)$ is true because $(a + b)^1 = a + b \geq a^1 + b^1 = a + b$. Direct proof. 23. If we chose 9 or fewer days on each day of the week, this would account for at most $9 \cdot 7 = 63$ days. But we chose 64 days. This contradiction shows that at least 10 of the days we chose must be on the same day of the week. 25. Suppose by way of contradiction that a/b is a rational root, where a and b are integers and this fraction is in lowest terms (that is, a and b have no common divisor greater than 1). Plug this proposed root into the equation to obtain $a^3/b^3 + a/b + 1 = 0$. Multiply through by b^3 to obtain $a^3 + ab^2 + b^3 = 0$. If a and b are both odd, then the left-hand side is the sum of three odd numbers and therefore must be odd. If a is odd and b is even, then the left-hand side is odd + even + even, which is again odd. Similarly, if a is even and b is odd, then the left-hand

side is even + even + odd, which is again odd. Because the fraction a/b is in simplest terms, it cannot happen that both a and b are even. Thus in all cases, the left-hand side is odd, and therefore cannot equal 0. This contradiction shows that no such root exists. **27.** First, assume that n is odd, so that $n = 2k+1$ for some integer k. Then $5n+6 = 5(2k+1)+6 = 10k+11 = 2(5k+5)+1$. Hence, $5n+6$ is odd. To prove the converse, suppose that n is even, so that $n = 2k$ for some integer k. Then $5n+6 = 10k+6 = 2(5k+3)$, so $5n+6$ is even. Hence, n is odd if and only if $5n+6$ is odd. **29.** This proposition is true. Suppose that m is neither 1 nor -1. Then mn has a factor m larger than 1. On the other hand, $mn = 1$, and 1 has no such factor. Hence, $m = 1$ or $m = -1$. In the first case $n = 1$, and in the second case $n = -1$, because $n = 1/m$. **31.** We prove that all these are equivalent to x being even. If x is even, then $x = 2k$ for some integer k. Therefore $3x+2 = 3\cdot 2k+2 = 6k+2 = 2(3k+1)$, which is even, because it has been written in the form $2t$, where $t = 3k+1$. Similarly, $x+5 = 2k+5 = 2k+4+1 = 2(k+2)+1$, so $x+5$ is odd; and $x^2 = (2k)^2 = 2(2k^2)$, so x^2 is even. For the converses, we will use a proof by contraposition. So assume that x is not even; thus x is odd and we can write $x = 2k+1$ for some integer k. Then $3x+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1$, which is odd (i.e., not even), because it has been written in the form $2t+1$, where $t = 3k+2$. Similarly, $x+5 = 2k+1+5 = 2(k+3)$, so $x+5$ is even (i.e., not odd). That x^2 is odd was already proved in Example 1. **33.** We give proofs by contraposition of $(i) \to (ii)$, $(ii) \to (i)$, $(i) \to (iii)$, and $(iii) \to (i)$. For the first of these, suppose that $3x+2$ is rational, namely, equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x = ((p/q)-2)/3 = (p-2q)/(3q)$, where $3q \neq 0$. This shows that x is rational. For the second conditional statement, suppose that x is rational, namely, equal to p/q for some integers p and q with $q \neq 0$. Then we can write $3x+2 = (3p+2q)/q$, where $q \neq 0$. This shows that $3x+2$ is rational. For the third conditional statement, suppose that $x/2$ is rational, namely, equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x = 2p/q$, where $q \neq 0$. This shows that x is rational. And for the fourth conditional statement, suppose that x is rational, namely, equal to p/q for some integers p and q with $q \neq 0$. Then we can write $x/2 = p/(2q)$, where $2q \neq 0$. This shows that $x/2$ is rational. **35.** No **37.** Suppose that $p_1 \to p_4 \to p_2 \to p_5 \to p_3 \to p_1$. To prove that one of these propositions implies any of the others, just use hypothetical syllogism repeatedly. **39.** We will give a proof by contradiction. Suppose that $a_1, a_2, \ldots, a_n$ are all less than A, where A is the average of these numbers. Then $a_1 + a_2 + \cdots + a_n < nA$. Dividing both sides by n shows that $A = (a_1 + a_2 + \cdots + a_n)/n < A$, which is a contradiction. **41.** We will show that the four statements are equivalent by showing that (i) implies (ii), (ii) implies (iii), (iii) implies (iv), and (iv) implies (i). First, assume that n is even. Then $n = 2k$ for some integer k. Then $n+1 = 2k+1$, so $n+1$ is odd. This shows that (i) implies (ii). Next, suppose that $n+1$ is odd, so $n+1 = 2k+1$ for some integer k. Then $3n+1 = 2n+(n+1) = 2(n+k)+1$, which shows that $3n+1$ is odd, showing that (ii) implies (iii). Next, suppose that $3n+1$ is odd, so $3n+1 = 2k+1$ for some integer k. Then $3n = (2k+1)-1 = 2k$, so $3n$ is even. This shows that (iii) implies (iv). Finally, suppose that n is not even. Then n is odd, so $n = 2k+1$ for some integer k. Then $3n = 3(2k+1) = 6k+3 = 2(3k+1)+1$, so $3n$ is odd. This completes a proof by contraposition that (iv) implies (i).

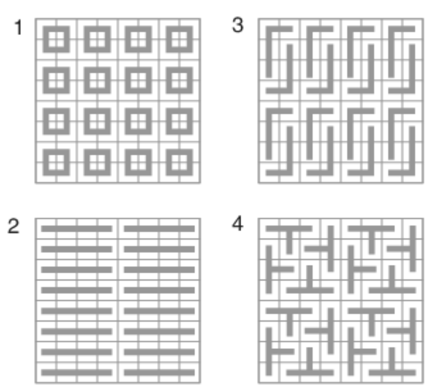
Section 1.8

1. $1^2+1 = 2 \geq 2 = 2^1$; $2^2+1 = 5 \geq 4 = 2^2$; $3^2+1 = 10 \geq 8 = 2^3$; $4^2+1 = 17 \geq 16 = 2^4$ **3.** If $x \leq y$, then $\max(x, y) + \min(x, y) = y + x = x + y$. If $x \geq y$, then $\max(x, y) + \min(x, y) = x + y$. Because these are the only two cases, the equality always holds. **5.** Because $|x-y| = |y-x|$, the values of x and y are interchangeable. Therefore, without loss of generality, we can assume that $x \geq y$. Then $(x+y-(x-y))/2 = (x+y-x+y)/2 = 2y/2 = y = \min(x, y)$. Similarly, $(x+y+(x-y))/2 = (x+y+x-y)/2 = 2x/2 = x = \max(x, y)$. **7.** There are four cases. *Case 1:* $x \geq 0$ and $y \geq 0$. Then $|x|+|y| = x+y = |x+y|$. *Case 2:* $x < 0$ and $y < 0$. Then $|x|+|y| = -x+(-y) = -(x+y) = |x+y|$ because $x+y < 0$. *Case 3:* $x \geq 0$ and $y < 0$. Then $|x|+|y| = x+(-y)$. If $x \geq -y$, then $|x+y| = x+y$. But because $y < 0$, $-y > y$, so $|x|+|y| = x+(-y) > x+y = |x+y|$. If $x < -y$, then $|x+y| = -(x+y) = -x+(-y)$. But because $x \geq 0$, $x \geq -x$, so $|x|+|y| = x+(-y) \geq -x+(-y) = |x+y|$. *Case 4:* $x < 0$ and $y \geq 0$. Identical to Case 3 with the roles of x and y reversed. **9.** 10,001, 10,002, ..., 10,100 are all nonsquares, because $100^2 = 10{,}000$ and $101^2 = 10{,}201$; constructive. **11.** $8 = 2^3$ and $9 = 3^2$ **13.** Let $x = 2$ and $y = \sqrt{2}$. If $x^y = 2^{\sqrt{2}}$ is irrational, we are done. If not, then let $x = 2^{\sqrt{2}}$ and $y = \sqrt{2}/4$. Then $x^y = (2^{\sqrt{2}})^{\sqrt{2}/4} = 2^{\sqrt{2}\cdot(\sqrt{2})/4} = 2^{1/2} = \sqrt{2}$. **15. a)** This statement asserts the existence of x with a certain property. If we let $y = x$, then we see that $P(x)$ is true. If y is anything other than x, then $P(x)$ is not true. Thus, x is the unique element that makes P true. **b)** The first clause here says that there is an element that makes P true. The second clause says that whenever two elements both make P true, they are in fact the same element. Together these say that P is satisfied by exactly one element. **c)** This statement asserts the existence of an x that makes P true and has the further property that whenever we find an element that makes P true, that element is x. In other words, x is the unique element that makes P true. **17.** The equation $|a-c| = |b-c|$ is equivalent to the disjunction of two equations: $a-c = b-c$ or $a-c = -b+c$. The first of these is equivalent to $a = b$, which contradicts the assumptions made in this problem, so the original equation is equivalent to $a-c = -b+c$. By adding $b+c$ to both sides and dividing by 2, we see that this equation is equivalent to $c = (a+b)/2$. Thus, there is a unique solution. Furthermore, this c is an integer, because the sum of the odd integers a and b is even. **19.** We are being asked to solve $n = (k - 2) + (k + 3)$ for k. Using the usual, reversible, rules of algebra, we see that this equation is equivalent to $k = (n - 1)/2$. In other words, this is the one and only value of k that makes our equation true. Because n is odd, $n - 1$ is even, so k is an integer. **21.** If x is itself an integer, then we can take $n = x$ and $\epsilon = 0$. No other solution is possible in this case, because if the integer n is greater than x, then n is at least $x + 1$, which would make $\epsilon \geq 1$. If x is not an integer, then round it up to the next integer, and call that integer n. Let $\epsilon = n - x$. Clearly $0 \leq \epsilon < 1$; this is the only ϵ that will work with this n, and n cannot be any larger, because ϵ is constrained to be less than 1. **23.** The harmonic mean of distinct positive real numbers x and y is always less than their geometric mean. To prove $2xy/(x + y) < \sqrt{xy}$, multiply both sides by $(x + y)/(2\sqrt{xy})$ to obtain the equivalent inequality $\sqrt{xy} < (x + y)/2$, which is proved in Example 14. **25.** The parity (oddness or evenness) of the sum of the numbers written on the board never changes, because $j + k$ and $|j - k|$ have the same parity (and at each step we reduce the sum by $j + k$ but increase it by $|j - k|$). Therefore the integer at the end of the process must have the same parity as $1 + 2 + \cdots + (2n) = n(2n + 1)$, which is odd because n is odd. **27.** Without loss of generality we can assume that n is nonnegative, because the fourth power of an integer and the fourth power of its negative are the same. We divide an arbitrary positive integer n by 10, obtaining a quotient k and remainder l, whence $n = 10k + l$, and l is an integer between 0 and 9, inclusive. Then we compute n^4 in each of these 10 cases. We get the following values, where X is some integer that is a multiple of 10, whose exact value we do not care about. $(10k + 0)^4 = 10{,}000k^4 = 10{,}000k^4 + 0$, $(10k + 1)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 1$, $(10k + 2)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 16$, $(10k + 3)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 81$, $(10k + 4)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 256$, $(10k + 5)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 625$, $(10k + 6)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 1296$, $(10k + 7)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 2401$, $(10k + 8)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 4096$, $(10k + 9)^4 = 10{,}000k^4 + X \cdot k^3 + X \cdot k^2 + X \cdot k + 6561$. Because each coefficient indicated by X is a multiple of 10, the corresponding term has no effect on the ones digit of the answer. Therefore the ones digits are 0, 1, 6, 1, 6, 5, 6, 1, 6, 1, respectively, so it is always a 0, 1, 5, or 6. **29.** Because $n^3 > 100$ for all $n > 4$, we need only note that $n = 1$, $n = 2$, $n = 3$, and $n = 4$ do not satisfy $n^2 + n^3 = 100$. **31.** Because $5^4 = 625$, both x and y must be less than 5. Then $x^4 + y^4 \leq 4^4 + 4^4 = 512 < 625$. **33.** If it is not true that $a \leq \sqrt[3]{n}$, $b \leq \sqrt[3]{n}$, or $c \leq \sqrt[3]{n}$, then $a > \sqrt[3]{n}$, $b > \sqrt[3]{n}$, and $c > \sqrt[3]{n}$. Multiplying these inequalities of positive numbers together we obtain $abc < (\sqrt[3]{n})^3 = n$, which implies the negation of our hypothesis that $n = abc$. **35.** By finding a common denominator, we can assume that the given rational numbers are a/b and c/b, where b is a positive integer and a and c are integers with $a < c$. In particular, $(a + 1)/b \leq c/b$. Thus, $x = (a + \frac{1}{2}\sqrt{2})/b$ is between the two given rational numbers, because $0 < \sqrt{2} < 2$. Furthermore, x is irrational, because if x were rational, then $2(bx - a) = \sqrt{2}$ would be as well, in violation of Example 10 in Section 1.7. **37. a)** Without loss of generality, we can assume that the x sequence is already sorted into nondecreasing order, because we can relabel the indices. There are only a finite number of possible orderings for the y sequence, so if we can show that we can increase the sum (or at least keep it the same) whenever we find y_i and y_j that are out of order (i.e., $i < j$ but $y_i > y_j$) by switching them, then we will have shown that the sum is largest when the y sequence is in nondecreasing order. Indeed, if we perform the swap, then we have added $x_i y_j + x_j y_i$ to the sum and subtracted $x_i y_i + x_j y_j$. The net effect is to have added $x_i y_j + x_j y_i - x_i y_i - x_j y_j = (x_j - x_i)(y_i - y_j)$, which is nonnegative by our ordering assumptions. **b)** Similar to part (a) **39. a)** $6 \to 3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$ **b)** $7 \to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$ **c)** $17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$ **d)** $21 \to 64 \to 32 \to 16 \to 8 \to 4 \to 2 \to 1$ **41.** Without loss of generality, assume that the upper left and upper right corners of the board are removed. Place three dominoes horizontally to fill the remaining portion of the first row, and fill each of the other seven rows with four horizontal dominoes. **43.** Because there is an even number of squares in all, either there is an even number of squares in each row or there is an even number of squares in each column. In the former case, tile the board in the obvious way by placing the dominoes horizontally, and in the latter case, tile the board in the obvious way by placing the dominoes vertically. **45.** We can rotate the board if necessary to make the removed squares be 1 and 16. Square 2 must be covered by a domino. If that domino is placed to cover squares 2 and 6, then the following domino placements are forced in succession: 5-9, 13-14, and 10-11, at which point there is no way to cover square 15. Otherwise, square 2 must be covered by a domino placed at 2-3. Then the following domino placements are forced: 4-8, 11-12, 6-7, 5-9, and 10-14, and again there is no way to cover square 15. **47.** Remove the two black squares adjacent to a white corner, and remove two white squares other than that corner. Then no domino can cover that white corner.

49. a)



b) The picture shows tilings for the first four patterns.



To show that pattern 5 cannot tile the checkerboard, label the squares from 1 to 64, one row at a time from the top, from left to right in each row. Thus, square 1 is the upper left corner, and square 64 is the lower right. Suppose we did have a tiling. By symmetry and without loss of generality, we may suppose that the tile is positioned in the upper left corner, covering squares 1, 2, 10, and 11. This forces a tile to be adjacent to it on the right, covering squares 3, 4, 12, and 13. Continue in this manner and we are forced to have a tile covering squares 6, 7, 15, and 16. This makes it impossible to cover square 8. Thus, no tiling is possible.

Supplementary Exercises

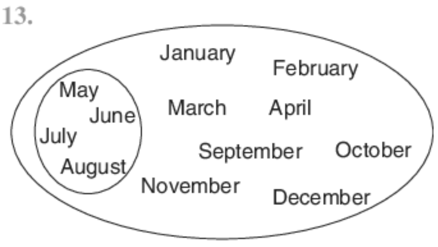
1. a) $q \to p$ **b)** $q \land p$ **c)** $\neg q \lor \neg p$ **d)** $q \leftrightarrow p$ **3. a)** The proposition cannot be false unless $\neg p$ is false, so p is true. If p is true and q is true, then $\neg q \land (p \to q)$ is false, so the conditional statement is true. If p is true and q is false, then $p \to q$ is false, so $\neg q \land (p \to q)$ is false and the conditional statement is true. **b)** The proposition cannot be false unless q is false. If q is false and p is true, then $(p \lor q) \land \neg p$ is false, and the conditional statement is true. If q is false and p is false, then $(p \lor q) \land \neg p$ is false, and the conditional statement is true. **5.** $\neg q \to \neg p$; $p \to q$; $\neg p \to \neg q$ **7.** $(p \land q \land r \land \neg s) \lor (p \land q \land \neg r \land s) \lor (p \land \neg q \land r \land s) \lor (\neg p \land q \land r \land s)$ **9.** Translating these statements into symbols, using the obvious letters, we have $\neg t \to \neg g$, $\neg g \to \neg q$, $r \to q$, and $\neg t \land r$. Assume the statements are consistent. The fourth statement tells us that $\neg t$ must be true. Therefore by modus ponens with the first statement, we know that $\neg g$ is true, hence (from the second statement), that $\neg q$ is true. Also, the fourth statement tells us that r must be true, and so again modus ponens (third statement) makes q true. This is a contradiction: $q \land \neg q$. Thus the statements are inconsistent. **11.** Reject-accept-reject-accept, accept-accept-accept-accept, accept-accept-reject-accept, reject-reject-reject-reject, reject-reject-accept-reject, and reject-accept-accept-accept **13.** Aaron is a knave and Crystal is a knight; it cannot be determined what Bohan is. **15.** Brenda **17.** The premises cannot both be true, because they are contradictory. Therefore it is (vacuously) true that whenever all the premises are true, the conclusion is also true, which by definition makes this a valid argument. Because the premises are not both true, we cannot conclude that the conclusion is true. **19.** Use the same propositions as were given in Section 1.3 for a 9×9 Sudoku puzzle, with the variables indexed from 1 to 16, instead of from 1 to 9, and with a similar change for the propositions for the 4×4 blocks: $\bigwedge_{r=0}^{3} \bigwedge_{s=0}^{3} \bigwedge_{n=1}^{16} \bigvee_{i=1}^{4} \bigvee_{j=1}^{4} p(4r+i, 4s+j, n)$. **21. a)** F **b)** T **c)** F **d)** T **e)** F **f)** T **23.** Many answers are possible. One example is United States senators. **25.** $\forall x \exists y \exists z\, (y \neq z \land \forall w (P(w, x) \leftrightarrow (w = y \lor w = z)))$ **27. a)** $\neg \exists x P(x)$ **b)** $\exists x (P(x) \land \forall y (P(y) \to y = x))$ **c)** $\exists x_1 \exists x_2 (P(x_1) \land P(x_2) \land x_1 \neq x_2 \land \forall y (P(y) \to (y = x_1 \lor y = x_2)))$ **d)** $\exists x_1 \exists x_2 \exists x_3 (P(x_1) \land P(x_2) \land P(x_3) \land x_1 \neq x_2 \land x_1 \neq x_3 \land x_2 \neq x_3 \land \forall y (P(y) \to (y = x_1 \lor y = x_2 \lor y = x_3)))$ **29.** Suppose that $\exists x (P(x) \to Q(x))$ is true. Then either $Q(x_0)$ is true for some x_0, in which case $\forall x P(x) \to \exists x\, Q(x)$ is true; or $P(x_0)$ is false for some x_0, in which case $\forall x P(x) \to \exists x Q(x)$ is true. Conversely, suppose that $\exists x (P(x) \to Q(x))$ is false. That means that $\forall x (P(x) \land \neg Q(x))$ is true, which implies $\forall x P(x)$ and $\forall x (\neg Q(x))$. This latter proposition is equivalent to $\neg \exists x Q(x)$. Thus, $\forall x P(x) \to \exists x Q(x)$ is false. **31.** No **33.** $\forall x\, \forall z\, \exists y\, T(x, y, z)$, where $T(x, y, z)$ is the statement that student x has taken class y in department z, where the domains are the set of students in the class, the set of courses at this university, and the set of departments in the school of mathematical sciences **35.** $\exists! x \exists! y\, T(x, y)$ and $\exists x \forall z ((\exists y \forall w (T(z, w) \leftrightarrow w = y)) \leftrightarrow z = x)$, where $T(x, y)$ means that student x has taken class y and the domain is all students in this class **37.** $P(a) \to Q(a)$ and $Q(a) \to R(a)$ by universal instantiation; then $\neg Q(a)$ by modus tollens and $\neg P(a)$ by modus tollens **39.** We give a proof by contraposition and show that if $\sqrt{x}$ is rational, then x is rational, assuming throughout that $x \geq 0$. Suppose that $\sqrt{x} = p/q$ is rational, $q \neq 0$. Then $x = (\sqrt{x})^2 = p^2/q^2$ is also rational (q^2 is again nonzero). **41.** We can give a constructive proof by letting $m = 10^{500} + 1$. Then $m^2 = (10^{500}+1)^2 > (10^{500})^2 = 10^{1000}$. **43.** 23 cannot be written as the sum of eight cubes. **45.** 223 cannot be written as the sum of 36 fifth powers.

CHAPTER 2

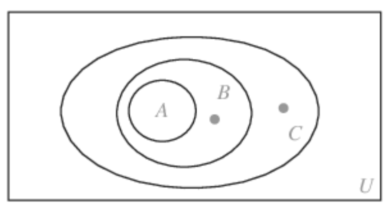
Section 2.1

1. a) $\{-1, 1\}$ **b)** $\{1,2,3,4,5,6,7,8,9,10,11\}$ **c)** $\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}$ **d)** $\emptyset$ **3. a)** The first is a subset of the second, but the second is not a subset of the first. **b)** Neither is a subset of the other. **c)** The first is a subset of the second, but the second is not a subset of the first. **5. a)** Yes **b)** No **c)** No **7. a)** Yes **b)** No **c)** Yes **d)** No **e)** No **f)** No **9. a)** False **b)** False **c)** False **d)** True **e)** False **f)** False **g)** True **11. a)** True **b)** True **c)** False **d)** True **e)** True **f)** False

13.



15. The dots in certain regions indicate that those regions are not empty.



17. Suppose that $x \in A$. Because $A \subseteq B$, this implies that $x \in B$. Because $B \subseteq C$, we see that $x \in C$. Because $x \in A$ implies that $x \in C$, it follows that $A \subseteq C$. 19. **a)** 1 **b)** 1 **c)** 2 **d)** 3 21. **a)** $\{\emptyset, \{a\}\}$ **b)** $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ **c)** $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ 23. **a)** 8 **b)** 16 **c)** 2 25. For the "if" part, given $A \subseteq B$, we want to show that that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, i.e., if $C \subseteq A$ then $C \subseteq B$. But this follows directly from Exercise 17. For the "only if" part, given that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we want to show that $A \subseteq B$. Suppose $a \in A$. Then $\{a\} \subseteq A$, so $\{a\} \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, it follows that $\{a\} \in \mathcal{P}(B)$, which means that $\{a\} \subseteq B$. But this implies $a \in B$, as desired. 27. **a)** $\{(a, y), (b, y), (c, y), (d, y), (a, z), (b, z), (c, z), (d, z)\}$ **b)** $\{(y, a), (y, b), (y, c), (y, d), (z, a), (z, b), (z, c), (z, d)\}$ 29. The set of triples (a, b, c), where a is an airline and b and c are cities. A useful subset of this set is the set of triples (a, b, c) for which a flies between b and c. 31. $\emptyset \times A = \{(x, y) \mid x \in \emptyset \text{ and } y \in A\} = \emptyset = \{(x, y) \mid x \in A \text{ and } y \in \emptyset\} = A \times \emptyset$ 33. **a)** $\{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (1, 3), (3, 0), (3, 1), (3, 3)\}$ **b)** $\{(1, 1), (1, 2), (1, a), (1, b), (2, 1), (2, 2), (2, a), (2, b), (a, 1), (a, 2), (a, a), (a, b), (b, 1), (b, 2), (b, a), (b, b)\}$ 35. mn 37. m^n 39. The elements of $A \times B \times C$ consist of 3-tuples (a, b, c), where $a \in A$, $b \in B$, and $c \in C$, whereas the elements of $(A \times B) \times C$ look like $((a, b), c)$—ordered pairs, the first coordinate of which is again an ordered pair. 41. **a)** The square of a real number is never -1. True **b)** There exists an integer whose square is 2. False **c)** The square of every integer is positive. False **d)** There is a real number equal to its own square. True 43. **a)** $\{-1, 0, 1\}$ **b)** $\mathbf{Z} - \{0, 1\}$ **c)** $\emptyset$ 45. We must show that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ if and only if $a = c$ and $b = d$. The "if" part is immediate. So assume these two sets are equal. First, consider the case when $a \neq b$. Then $\{\{a\}, \{a, b\}\}$ contains exactly two elements, one of which contains one element. Thus, $\{\{c\}, \{c, d\}\}$ must have the same property, so $c \neq d$ and $\{c\}$ is the element containing exactly one element. Hence, $\{a\} = \{c\}$, which implies that $a = c$. Also, the two-element sets $\{a, b\}$ and $\{c, d\}$ must be equal. Because $a = c$ and $a \neq b$, it follows that $b = d$. Second, suppose that $a = b$. Then $\{\{a\}, \{a, b\}\} = \{\{a\}\}$, a set with one element. Hence, $\{\{c\}, \{c, d\}\}$ has only one element, which can happen only when $c = d$, and the set is $\{\{c\}\}$. It then follows that $a = c$ and $b = d$. 47. Let $S = \{a_1, a_2, \ldots, a_n\}$. Represent each subset of S with a bit string of length n, where the ith bit is 1 if and only if $a_i \in S$. To generate all subsets of S, list all 2^n bit strings of length n (for instance, in increasing order), and write down the corresponding subsets.

Section 2.2

1. **a)** The set of students who live within one mile of school and walk to classes **b)** The set of students who live within one mile of school or walk to classes (or do both) **c)** The set of students who live within one mile of school but do not walk to classes **d)** The set of students who walk to classes but live more than one mile away from school 3. **a)** $\{0,1,2,3,4,5,6\}$ **b)** $\{3\}$ **c)** $\{1, 2, 4, 5\}$ **d)** $\{0, 6\}$ 5. $\overline{\overline{A}} = \{x \mid \neg(x \in \overline{A})\} = \{x \mid \neg(\neg x \in A)\} = \{x \mid x \in A\} = A$ 7. **a)** $A \cup U = \{x \mid x \in A \vee x \in U\} = \{x \mid x \in A \vee \mathbf{T}\} = \{x \mid \mathbf{T}\} = U$ **b)** $A \cap \emptyset = \{x \mid x \in A \wedge x \in \emptyset\} = \{x \mid x \in A \wedge \mathbf{F}\} = \{x \mid \mathbf{F}\} = \emptyset$ 9. **a)** $A \cup \overline{A} = \{x \mid x \in A \vee x \notin A\} = U$ **b)** $A \cap \overline{A} = \{x \mid x \in A \wedge x \notin A\} = \emptyset$ 11. **a)** $A \cup B = \{x \mid x \in A \vee x \in B\} = \{x \mid x \in B \vee x \in A\} = B \cup A$ **b)** $A \cap B = \{x \mid x \in A \wedge x \in B\} = \{x \mid x \in B \wedge x \in A\} = B \cap A$ 13. Suppose $x \in A \cap (A \cup B)$. Then $x \in A$ and $x \in A \cup B$ by the definition of intersection. Because $x \in A$, 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, $x \in A \cup B$ as well. Therefore $x \in A \cap (A \cup B)$ by the definition of intersection, so the right-hand side is a subset of the left-hand side. 15. **a)** $x \in \overline{A \cup B} \equiv x \notin A \cup B \equiv \neg(x \in A \vee x \in B) \equiv \neg(x \in A) \wedge \neg(x \in B) \equiv x \notin A \wedge x \notin B \equiv x \in \overline{A} \wedge x \in \overline{B} \equiv x \in \overline{A} \cap \overline{B}$

b)

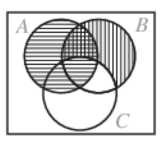
A	B	$A \cup B$	$\overline{A \cup B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cap \overline{B}$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

17. **a)** $x \in \overline{A \cap B \cap C} \equiv x \notin A \cap B \cap C \equiv x \notin A \vee x \notin B \vee x \notin C \equiv x \in \overline{A} \vee x \in \overline{B} \vee x \in \overline{C} \equiv x \in \overline{A} \cup \overline{B} \cup \overline{C}$

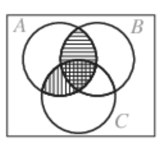
b)

A	B	C	$A \cap B \cap C$	$\overline{A \cap B \cap C}$	$\overline{A}$	$\overline{B}$	$\overline{C}$	$\overline{A} \cup \overline{B} \cup \overline{C}$
1	1	1	1	0	0	0	0	0
1	1	0	0	1	0	0	1	1
1	0	1	0	1	0	1	0	1
1	0	0	0	1	0	1	1	1
0	1	1	0	1	1	0	0	1
0	1	0	0	1	1	0	1	1
0	0	1	0	1	1	1	0	1
0	0	0	0	1	1	1	1	1

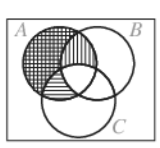
19. **a)** Both sides equal $\{x \mid x \in A \wedge x \notin B\}$. **b)** $A = A \cap U = A \cap (B \cup \overline{B}) = (A \cap B) \cup (A \cap \overline{B})$ 21. $x \in A \cup (B \cup C) \equiv (x \in A) \vee (x \in (B \cup C)) \equiv (x \in A) \vee (x \in B \vee x \in C) \equiv (x \in A \vee x \in B) \vee (x \in C) \equiv x \in (A \cup B) \cup C$ 23. $x \in A \cup (B \cap C) \equiv (x \in A) \vee (x \in (B \cap C)) \equiv (x \in A) \vee (x \in B \wedge x \in C) \equiv (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \equiv x \in (A \cup B) \cap (A \cup C)$ 25. **a)** $\{4,6\}$ **b)** $\{0,1,2,3,4,5,6,7,8,9,10\}$ **c)** $\{4, 5, 6, 8, 10\}$ **d)** $\{0,2,4, 5,6,7,8,9,10\}$ 27. **a)** The double-shaded portion is the desired set.



b) The desired set is the entire shaded portion.



c) The desired set is the entire shaded portion.



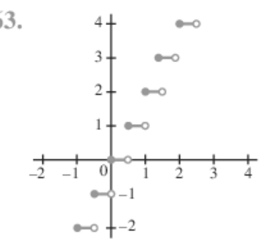
29. **a)** $B \subseteq A$ **b)** $A \subseteq B$ **c)** $A \cap B = \emptyset$ **d)** Nothing, because this is always true **e)** $A = B$ 31. $A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B) \equiv \forall x(x \notin B \rightarrow x \notin A) \equiv \forall x(x \in \overline{B} \rightarrow x \in \overline{A}) \equiv \overline{B} \subseteq \overline{A}$ 33. The set of students who are computer science majors but not mathematics majors or who are mathematics majors but not computer science majors 35. An element is in $(A \cup B) - (A \cap B)$ if it is in the union of A and B but not in the intersection of A and B, which means that it is in either A or B but not in both A and B. This is exactly what it means for an element to belong to $A \oplus B$. 37. **a)** $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$ **b)** $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$ **c)** $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \overline{A} = \overline{A}$ **d)** $A \oplus \overline{A} = (A - \overline{A}) \cup (\overline{A} - A) = A \cup \overline{A} = U$ 39. $B = \emptyset$ 41. Yes 43. Yes 45. If $A \cup B$ were finite, then it would have n elements for some natural number n. But A already has more than n elements, because it is infinite, and $A \cup B$ has all the elements that A has, so $A \cup B$ has more than n elements. This contradiction shows that $A \cup B$ must be infinite. 47. **a)** $\{1, 2, 3, \ldots, n\}$ **b)** $\{1\}$ 49. **a)** A_n **b)** $\{0, 1\}$ 51. **a)** $\mathbf{Z}$, $\{-1, 0, 1\}$ **b)** $\mathbf{Z} - \{0\}$, $\emptyset$ **c)** $\mathbf{R}$, $[-1, 1]$ **d)** $[1, \infty)$, $\emptyset$ 53. **a)** $\{1, 2, 3, 4, 7, 8, 9, 10\}$ **b)** $\{2, 4, 5, 6, 7\}$ **c)** $\{1, 10\}$ 55. The bit in the ith position of the bit string of the difference of two sets is 1 if the ith bit of the first string is 1 and the ith bit of the second string is 0, and is 0 otherwise. 57. **a)** 11 1110 0000 0000 0000 0000 0000 $\vee$ 01 1100 1000 0000 0100 0101 0000 = 11 1110 1000 0000 0100 0101 0000, representing $\{a, b, c, d, e, g, p, t, v\}$ **b)** 11 1110 0000 0000 0000 0000 0000 $\wedge$ 01 1100 1000 0000 0100 0101 0000 = 01 1100 0000 0000 0000 0000 0000, representing $\{b, c, d\}$ **c)** (11 1110 0000 0000 0000 0000 0000 $\vee$ 00 0110 0110 0001 1000 0110 0110) $\wedge$ (01 1100 1000 0000 0100 0101 0000 $\vee$ 00 1010 0010 0000 1000 0010 0111) = 11 1110 0110 0001 1000 0110 0110 $\wedge$ 01 1110 1010 0000 1100 0111 0111 = 01 1110 0010 0000 1000 0110 0110, representing $\{b, c, d, e, i, o, t, u, x, y\}$ **d)** 11 1110 0000 0000 0000 0000 0000 $\vee$ 01 1100 1000 0000 0100 0101 0000 $\vee$ 00 1010 0010 0000 1000 0010 0111 $\vee$ 00 0110 0110 0001 1000 0110 0110 = 11 1110 1110 0001 1100 0111 0111, representing $\{a,b,c,d,e,g,h,i,n,o,p,t,u,v,x,y,z\}$ 59. **a)** $\{1, 2, 3, \{1, 2, 3\}\}$ **b)** $\{\emptyset\}$ **c)** $\{\emptyset, \{\emptyset\}\}$ **d)** $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ 61. **a)** $\{3 \cdot a,\ 3 \cdot b,\ 1 \cdot c,\ 4 \cdot d\}$ **b)** $\{2 \cdot a,\ 2 \cdot b\}$ **c)** $\{1 \cdot a,\ 1 \cdot c\}$ **d)** $\{1 \cdot b,\ 4 \cdot d\}$ **e)** $\{5 \cdot a,\ 5 \cdot b,\ 1 \cdot c, 4 \cdot d\}$ 63. $\overline{F}$ = {0.4 Alice, 0.1 Brian, 0.6 Fred, 0.9 Oscar, 0.5 Rita}, $\overline{R}$ = {0.6 Alice, 0.2 Brian, 0.8 Fred, 0.1 Oscar, 0.3 Rita} 65. {0.4 Alice, 0.8 Brian, 0.2 Fred, 0.1 Oscar, 0.5 Rita}

Section 2.3

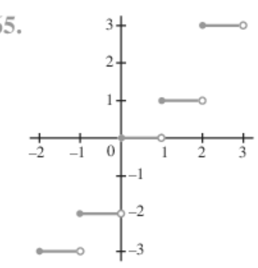
1. **a)** $f(0)$ is not defined. **b)** $f(x)$ is not defined for $x < 0$. **c)** $f(x)$ is not well-defined because there are two distinct values assigned to each x. 3. **a)** Not a function **b)** A function **c)** Not a function 5. **a)** Domain the set of bit strings; range the set of integers **b)** Domain the set of bit strings; range the set of even nonnegative integers **c)** Domain the set of bit strings; range the set of nonnegative integers not exceeding 7 **d)** Domain the set of positive integers; range the set of squares of positive integers $= \{1, 4, 9, 16, \ldots\}$ 7. **a)** Domain $\mathbf{Z}^+ \times \mathbf{Z}^+$; range $\mathbf{Z}^+$ **b)** Domain $\mathbf{Z}^+$; range $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ **c)** Domain the set of bit strings; range $\mathbf{N}$ **d)** Domain the set of bit strings; range $\mathbf{N}$ 9. **a)** 1 **b)** 0 **c)** 0 **d)** -1 **e)** 3 **f)** -1 **g)** 2 **h)** 1 11. Only the function in part (a) 13. Only the functions in parts (a) and (d) 15. **a)** Onto **b)** Not onto **c)** Onto **d)** Not onto **e)** Onto 17. **a)** Depends on whether teachers share offices **b)** One-to-one assuming only one teacher per bus **c)** Most likely not one-to-one, especially if salary is set by a collective bargaining agreement **d)** One-to-one 19. Answers will vary. **a)** Set of offices at the school; probably not onto **b)** Set of buses going on the trip; onto, assuming every bus gets a teacher chaperone **c)** Set of real numbers; not onto **d)** Set of strings of nine digits with hyphens after third and fifth digits; not onto 21. **a)** The function $f(x)$ with $f(x) = 3x + 1$ when $x \geq 0$ and $f(x) = -3x + 2$ when $x < 0$ **b)** $f(x) = |x| + 1$ **c)** The function $f(x)$ with $f(x) = 2x + 1$ when $x \geq 0$ and $f(x) = -2x$ when $x < 0$ **d)** $f(x) = x^2 + 1$ 23. **a)** Yes **b)** No **c)** Yes **d)** No 25. Suppose that f is strictly decreasing. This means that $f(x) > f(y)$ whenever $x < y$. To show that g is strictly increasing, suppose that $x < y$. Then $g(x) = 1/f(x) < 1/f(y) = g(y)$. Conversely, suppose that g is strictly increasing. This means that $g(x) < g(y)$ whenever $x < y$. To show that f is strictly decreasing, suppose that $x < y$. Then $f(x) = 1/g(x) > 1/g(y) = f(y)$. 27. **a)** Let f be a given strictly decreasing function from $\mathbf{R}$ to itself. If

$a < b$, then $f(a) > f(b)$; if $a > b$, then $f(a) < f(b)$. Thus if $a \neq b$, then $f(a) \neq f(b)$. **b)** Answers will vary; for example, $f(x) = 0$ for $x < 0$ and $f(x) = -x$ for $x \geq 0$. **29.** The function is not one-to-one, so it is not invertible. On the restricted domain, the function is the identity function on the nonnegative real numbers, $f(x) = x$, so it is its own inverse. **31. a)** $f(S) = \{0, 1, 3\}$ **b)** $f(S) = \{0, 1, 3, 5, 8\}$ **c)** $f(S) = \{0, 8, 16, 40\}$ **d)** $f(S) = \{1, 12, 33, 65\}$ **33. a)** Let x and y be distinct elements of A. Because g is one-to-one, $g(x)$ and $g(y)$ are distinct elements of B. Because f is one-to-one, $f(g(x)) = (f \circ g)(x)$ and $f(g(y)) = (f \circ g)(y)$ are distinct elements of C. Hence, $f \circ g$ is one-to-one. **b)** Let $y \in C$. Because f is onto, $y = f(b)$ for some $b \in B$. Now because g is onto, $b = g(x)$ for some $x \in A$. Hence, $y = f(b) = f(g(x)) = (f \circ g)(x)$. It follows that $f \circ g$ is onto. **35.** No. For example, suppose that $A = \{a\}$, $B = \{b, c\}$, and $C = \{d\}$. Let $g(a) = b$, $f(b) = d$, and $f(c) = d$. Then f and $f \circ g$ are onto, but g is not. **37.** $(f + g)(x) = x^2 + x + 3$, $(fg)(x) = x^3 + 2x^2 + x + 2$ **39.** f is one-to-one because $f(x_1) = f(x_2) \rightarrow ax_1 + b = ax_2 + b \rightarrow ax_1 = ax_2 \rightarrow x_1 = x_2$. f is onto because $f((y-b)/a) = y$. $f^{-1}(y) = (y-b)/a$. **41. a)** $A = B = \mathbf{R}$, $S = \{x \mid x > 0\}$, $T = \{x \mid x < 0\}$, $f(x) = x^2$ **b)** It suffices to show that $f(S) \cap f(T) \subseteq f(S \cap T)$. Let $y \in B$ be an element of $f(S) \cap f(T)$. Then $y \in f(S)$, so $y = f(x_1)$ for some $x_1 \in S$. Similarly, $y = f(x_2)$ for some $x_2 \in T$. Because f is one-to-one, it follows that $x_1 = x_2$. Therefore $x_1 \in S \cap T$, so $y \in f(S \cap T)$. **43. a)** $\{x \mid 0 \leq x < 1\}$ **b)** $\{x \mid -1 \leq x < 2\}$ **c)** $\emptyset$ **45.** $f^{-1}(\overline{S}) = \{x \in A \mid f(x) \notin S\} = \overline{\{x \in A \mid f(x) \in S\}} = \overline{f^{-1}(S)}$ **47.** Let $x = \lfloor x \rfloor + \epsilon$, where ϵ is a real number with $0 \leq \epsilon < 1$. If $\epsilon < \frac{1}{2}$, then $\lfloor x \rfloor - 1 < x - \frac{1}{2} < \lfloor x \rfloor$, so $\lceil x - \frac{1}{2} \rceil = \lfloor x \rfloor$ and this is the integer closest to x. If $\epsilon > \frac{1}{2}$, then $\lfloor x \rfloor < x - \frac{1}{2} < \lfloor x \rfloor + 1$, so $\lceil x - \frac{1}{2} \rceil = \lfloor x \rfloor + 1$ and this is the integer closest to x. If $\epsilon = \frac{1}{2}$, then $\lceil x - \frac{1}{2} \rceil = \lfloor x \rfloor$, which is the smaller of the two integers that surround x and are the same distance from x. **49.** Write the real number x as $\lfloor x \rfloor + \epsilon$, where ϵ is a real number with $0 \leq \epsilon < 1$. Because $\epsilon = x - \lfloor x \rfloor$, it follows that $0 \leq -\lfloor x \rfloor < 1$. The first two inequalities, $x - 1 < \lfloor x \rfloor$ and $\lfloor x \rfloor \leq x$, follow directly. For the other two inequalities, write $x = \lceil x \rceil - \epsilon'$, where $0 \leq \epsilon' < 1$. Then $0 \leq \lceil x \rceil - x < 1$, and the desired inequality follows. **51. a)** If $x < n$, because $\lfloor x \rfloor \leq x$, it follows that $\lfloor x \rfloor < n$. Suppose that $x \geq n$. By the definition of the floor function, it follows that $\lfloor x \rfloor \geq n$. This means that if $\lfloor x \rfloor < n$, then $x < n$. **b)** If $n < x$, then because $x \leq \lceil x \rceil$, it follows that $n \leq \lceil x \rceil$. Suppose that $n \geq x$. By the definition of the ceiling function, it follows that $\lceil x \rceil \leq n$. This means that if $n < \lceil x \rceil$, then $n < x$. **53.** If n is even, then $n = 2k$ for some integer k. Thus, $\lfloor n/2 \rfloor = \lfloor k \rfloor = k = n/2$. If n is odd, then $n = 2k + 1$ for some integer k. Thus, $\lfloor n/2 \rfloor = \lfloor k + \frac{1}{2} \rfloor = k = (n-1)/2$. **55.** Assume that $x \geq 0$. The left-hand side is $\lceil -x \rceil$ and the right-hand side is $-\lfloor x \rfloor$. If x is an integer, then both sides equal $-x$. Otherwise, let $x = n + \epsilon$, where n is a natural number and ϵ is a real number with $0 \leq \epsilon < 1$. Then $\lceil -x \rceil = \lceil -n - \epsilon \rceil = -n$ and $-\lfloor x \rfloor = -\lfloor n + \epsilon \rfloor = -n$ also. When $x < 0$, the equation also holds because it can be obtained by substituting $-x$ for x. **57.** $\lceil b \rceil - \lfloor a \rfloor - 1$ **59. a)** 1 **b)** 3 **c)** 126 **d)** 3600 **61. a)** 100 **b)** 256 **c)** 1030 **d)** 30,200

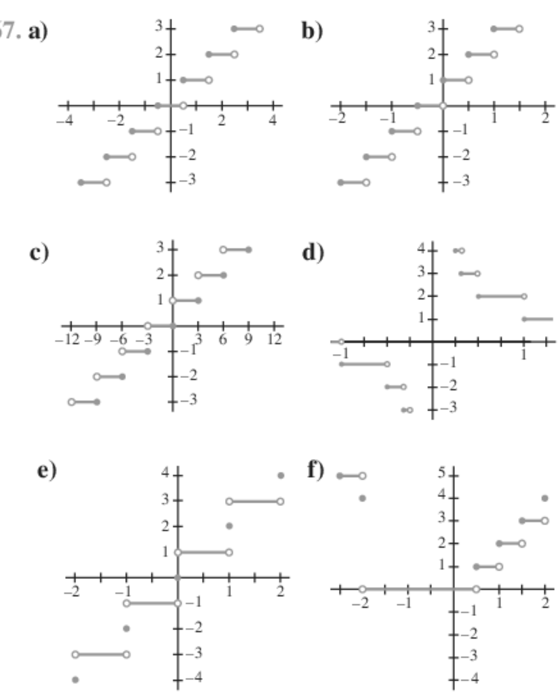
63.



65.



67.



g) See part (a). **69.** $f^{-1}(y) = (y-1)^{1/3}$ **71. a)** $f_{A \cap B}(x) = 1 \leftrightarrow x \in A \cap B \leftrightarrow x \in A$ and $x \in B \leftrightarrow f_A(x) = 1$ and $f_B(x) = 1 \leftrightarrow f_A(x)f_B(x) = 1$ **b)** $f_{A \cup B}(x) = 1 \leftrightarrow x \in A \cup B \leftrightarrow x \in A$ or $x \in B \leftrightarrow f_A(x) = 1$ or $f_B(x) = 1 \leftrightarrow f_A(x) + f_B(x) - f_A(x)f_B(x) = 1$ **c)** $f_{\overline{A}}(x) = 1 \leftrightarrow x \in \overline{A} \leftrightarrow x \notin A \leftrightarrow f_A(x) = 0 \leftrightarrow 1 - f_A(x) = 1$ **d)** $f_{A \oplus B}(x) = 1 \leftrightarrow x \in A \oplus B \leftrightarrow (x \in A$ and $x \notin B)$ or $(x \notin A$ and $x \in B) \leftrightarrow f_A(x) + f_B(x) - 2f_A(x)f_B(x) = 1$ **73. a)** True; because $\lfloor x \rfloor$ is already an integer, $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$. **b)** False; $x = \frac{1}{2}$ is a counterexample. **c)** True; if x or y is an integer, then by property 4b in Table 1, the difference is 0. If neither x nor y is an integer, then $x = n + \epsilon$ and $y = m + \delta$, where n and m are integers and ϵ and δ are positive real numbers less than 1. Then $m + n < x + y < m + n + 2$, so $\lceil x + y \rceil$ is either $m + n + 1$ or $m + n + 2$. Therefore, the given expression is either $(n + 1) + (m + 1) - (m + n + 1) = 1$ or $(n + 1) + (m + 1) - (m + n + 2) = 0$, as desired. **d)** False; $x = \frac{1}{4}$ and $y = 3$ is a counterexample. **e)** False; $x = \frac{1}{2}$ is a counterexample. 75. **a)** If x is a positive integer, then the two sides are equal. So suppose that $x = n^2 + m + \epsilon$, where n^2 is the largest perfect square less than x, m is a nonnegative integer, and $0 < \epsilon \le 1$. Then both $\sqrt{x}$ and $\sqrt{\lfloor x \rfloor} = \sqrt{n^2 + m}$ are between n and $n + 1$, so both sides equal n. **b)** If x is a positive integer, then the two sides are equal. So suppose that $x = n^2 - m - \epsilon$, where n^2 is the smallest perfect square greater than x, m is a nonnegative integer, and ϵ is a real number with $0 < \epsilon \le 1$. Then both $\sqrt{x}$ and $\sqrt{\lceil x \rceil} = \sqrt{n^2 - m}$ are between $n - 1$ and n. Therefore, both sides of the equation equal n. 77. **a)** Domain is $\mathbf{Z}$; codomain is $\mathbf{R}$; domain of definition is the set of nonzero integers; the set of values for which f is undefined is $\{0\}$; not a total function. **b)** Domain is $\mathbf{Z}$; codomain is $\mathbf{Z}$; domain of definition is $\mathbf{Z}$; set of values for which f is undefined is $\emptyset$; total function. **c)** Domain is $\mathbf{Z} \times \mathbf{Z}$; codomain is $\mathbf{Q}$; domain of definition is $\mathbf{Z} \times (\mathbf{Z} - \{0\})$; set of values for which f is undefined is $\mathbf{Z} \times \{0\}$; not a total function. **d)** Domain is $\mathbf{Z} \times \mathbf{Z}$; codomain is $\mathbf{Z}$; domain of definition is $\mathbf{Z} \times \mathbf{Z}$; set of values for which f is undefined is $\emptyset$; total function. **e)** Domain is $\mathbf{Z} \times \mathbf{Z}$; codomain is $\mathbf{Z}$; domain of definitions is $\{(m, n) \mid m > n\}$; set of values for which f is undefined is $\{(m, n) \mid m \le n\}$; not a total function. 79. **a)** By definition, to say that S has cardinality m is to say that S has exactly m distinct elements. Therefore we can assign the first object to 1, the second to 2, and so on. This provides the one-to-one correspondence. **b)** By part (a), there is a bijection f from S to $\{1, 2, \ldots, m\}$ and a bijection g from T to $\{1, 2, \ldots, m\}$. Then the composition $g^{-1} \circ f$ is the desired bijection from S to T.

Section 2.4

1. **a)** 3 **b)** −1 **c)** 787 **d)** 2639 3. **a)** $a_0 = 2, a_1 = 3, a_2 = 5, a_3 = 9$ **b)** $a_0 = 1, a_1 = 4, a_2 = 27, a_3 = 256$ **c)** $a_0 = 0, a_1 = 0, a_2 = 1, a_3 = 1$ **d)** $a_0 = 0, a_1 = 1, a_2 = 2, a_3 = 3$ 5. **a)** 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 **b)** 1, 1, 1, 2, 2, 2, 3, 3, 3, 4 **c)** 1, 1, 3, 3, 5, 5, 7, 7, 9, 9 **d)** −1, −2, −2, 8, 88, 656, 4912, 40064, 362368, 3627776 **e)** 3, 6, 12, 24, 48, 96, 192, 384, 768, 1536 **f)** 2, 4, 6, 10, 16, 26, 42, 68, 110, 178 **g)** 1, 2, 2, 3, 3, 3, 3, 4, 4, 4 **h)** 3, 3, 5, 4, 4, 3, 5, 5, 4, 3 7. Each term could be twice the previous term; the nth term could be obtained from the previous term by adding $n - 1$; the terms could be the positive integers that are not multiples of 3; there are infinitely many other possibilities. 9. **a)** 2, 12, 72, 432, 2592 **b)** 2, 4, 16, 256, 65,536 **c)** 1, 2, 5, 11, 26 **d)** 1, 1, 6, 27, 204 **e)** 1, 2, 0, 1, 3 11. **a)** 6, 17, 49, 143, 421 **b)** $49 = 5 \cdot 17 - 6 \cdot 6$, $143 = 5 \cdot 49 - 6 \cdot 17$, $421 = 5 \cdot 143 - 6 \cdot 49$ **c)** $5a_{n-1} - 6a_{n-2} = 5(2^{n-1} + 5 \cdot 3^{n-1}) - 6(2^{n-2} + 5 \cdot 3^{n-2}) = 2^{n-2}(10 - 6) + 3^{n-2}(75 - 30) = 2^{n-2} \cdot 4 + 3^{n-2} \cdot 9 \cdot 5 = 2^n + 3^n \cdot 5 = a_n$ 13. **a)** Yes **b)** No **c)** No **d)** Yes **e)** Yes **f)** Yes **g)** No **h)** No 15. **a)** $a_{n-1} + 2a_{n-2} + 2n - 9 = -(n - 1) + 2 + 2[-(n - 2) + 2] + 2n - 9 = -n + 2 = a_n$ **b)** $a_{n-1} + 2a_{n-2} + 2n - 9 = 5(-1)^{n-1} - (n - 1) + 2 + 2[5(-1)^{n-2} - (n - 2) + 2] + 2n - 9 = 5(-1)^{n-2}(-1 + 2) - n + 2 = a_n$ **c)** $a_{n-1} + 2a_{n-2} + 2n - 9 = 3(-1)^{n-1} + 2^{n-1} - (n - 1) + 2 + 2[3(-1)^{n-2} + 2^{n-2} - (n - 2) + 2] + 2n - 9 = 3(-1)^{n-2}(-1 + 2) + 2^{n-2}(2 + 2) - n + 2 = a_n$ **d)** $a_{n-1} + 2a_{n-2} + 2n - 9 = 7 \cdot 2^{n-1} - (n - 1) + 2 + 2[7 \cdot 2^{n-2} - (n - 2) + 2] + 2n - 9 = 2^{n-2}(7 \cdot 2 + 2 \cdot 7) - n + 2 = a_n$ 17. **a)** $a_n = 2 \cdot 3^n$ **b)** $a_n = 2n + 3$ **c)** $a_n = 1 + n(n + 1)/2$ **d)** $a_n = n^2 + 4n + 4$ **e)** $a_n = 1$ **f)** $a_n = (3^{n+1} - 1)/2$ **g)** $a_n = 5n!$ **h)** $a_n = 2^n n!$ 19. **a)** $a_n = 3a_{n-1}$ **b)** 5,904,900 21. **a)** $a_n = n + a_{n-1}$, $a_0 = 0$ **b)** $a_{12} = 78$ **c)** $a_n = n(n + 1)/2$ 23. $B(k) = [1 + (0.07/12)]B(k - 1) - 100$, with $B(0) = 5000$ 25. **a)** One 1 and one 0, followed by two 1s and two 0s, followed by three 1s and three 0s, and so on; 1, 1, 1 **b)** The positive integers are listed in increasing order with each even positive integer listed twice; 9, 10, 10. **c)** The terms in odd-numbered locations are the successive powers of 2; the terms in even-numbered locations are all 0; 32, 0, 64. **d)** $a_n = 3 \cdot 2^{n-1}$; 384, 768, 1536 **e)** $a_n = 15 - 7(n - 1) = 22 - 7n$; −34, −41, −48 **f)** $a_n = (n^2 + n + 4)/2$; 57, 68, 80 **g)** $a_n = 2n^3$; 1024, 1458, 2000 **h)** $a_n = n! + 1$; 362881, 3628801, 39916801 27. Among the integers $1, 2, \ldots, a_n$, where a_n is the nth positive integer not a perfect square, the nonsquares are $a_1, a_2, \ldots, a_n$ and the squares are $1^2, 2^2, \ldots, k^2$, where k is the integer with $k^2 < n + k < (k + 1)^2$. Consequently, $a_n = n + k$, where $k^2 < a_n < (k + 1)^2$. To find k, first note that $k^2 < n + k < (k + 1)^2$, so $k^2 + 1 \le n + k \le (k + 1)^2 - 1$. Hence, $(k - \frac{1}{2})^2 + \frac{3}{4} = k^2 - k + 1 \le n \le k^2 + k = (k + \frac{1}{2})^2 - \frac{1}{4}$. It follows that $k - \frac{1}{2} < \sqrt{n} < k + \frac{1}{2}$, so $k = \{\sqrt{n}\}$ and $a_n = n + k = n + \{\sqrt{n}\}$. 29. **a)** 20 **b)** 11 **c)** 30 **d)** 511 31. **a)** 1533 **b)** 510 **c)** 4923 **d)** 9842 33. **a)** 21 **b)** 78 **c)** 18 **d)** 18 35. $\sum_{j=1}^{n}(a_j - a_{j-1}) = a_n - a_0$ 37. **a)** n^2 **b)** $n(n + 1)/2$ 39. 15150 41. $\frac{n(n+1)(2n+1)}{3} + \frac{n(n+1)}{2} + (n + 1)(m - (n + 1)^2 + 1)$, where $n = \lfloor \sqrt{m} \rfloor - 1$ 43. **a)** 0 **b)** 1680 **c)** 1 **d)** 1024 45. 34

Section 2.5

1. **a)** Countably infinite, −1, −2, −3, −4, ... **b)** Countably infinite, 0, 2, −2, 4, −4, ... **c)** Countably infinite, 99, 98, 97, ... **d)** Uncountable **e)** Finite **f)** Countably infinite, 0, 7, −7, 14, −14, ... 3. **a)** Countable: match n with the string of n 1s. **b)** Countable. To find a correspondence, follow the path in Example 4, but omit fractions in the top three rows (as well as continuing to omit fractions not in lowest terms). **c)** Uncountable **d)** Uncountable 5. Suppose m new guests arrive at the fully occupied hotel. Move the guest in Room n to Room $m + n$ for $n = 1, 2, 3, \ldots$; then the new guests can occupy rooms 1 to m. 7. For $n = 1, 2, 3, \ldots$, put

the guest currently in Room $2n$ into Room n, and the guest currently in Room $2n - 1$ into Room n of the new building. **9.** Move the guess currently Room i to Room $2i + 1$ for $i = 1, 2, 3, \ldots$. Put the jth guest from the kth bus into Room $2^k(2j + 1)$. **11.** **a)** $A = [1, 2]$ (closed interval of real numbers from 1 to 2), $B = [3, 4]$ **b)** $A = [1, 2] \cup \mathbf{Z}^+$, $B = [3, 4] \cup \mathbf{Z}^+$ **c)** $A = [1, 3]$, $B = [2, 4]$ **13.** Suppose that A is countable. Then either A has cardinality n for some nonnegative integer n, in which case there is a one-to-one function from A to a subset of $\mathbf{Z}^+$ (the range is the first n positive integers), or there exists a one-to-one correspondence f from A to $\mathbf{Z}^+$; in either case we have satisfied Definition 2. Conversely, suppose that $|A| \le |\mathbf{Z}^+|$. By definition, this means that there is a one-to-one function from A to $\mathbf{Z}^+$, so A has the same cardinality as a subset of $\mathbf{Z}^+$ (namely the range of that function). By Exercise 16 we conclude that A is countable. **15.** Assume that B is countable. Then the elements of B can be listed as $b_1, b_2, b_3, \ldots$. Because A is a subset of B, taking the subsequence of $\{b_n\}$ that contains the terms that are in A gives a listing of the elements of A. Because A is uncountable, this is impossible. **17.** Assume that $A - B$ is countable. Then, because $A = (A - B) \cup (A \cap B)$, the elements of A can be listed in a sequence by alternating elements of $A - B$ and elements of $A \cap B$. This contradicts the uncountability of A. **19.** We are given bijections f from A to B and g from C to D. Then the function from $A \times C$ to $B \times D$ that sends (a, c) to $(f(a), g(c))$ is a bijection. **21.** By the definition of $|A| \le |B|$, there is a one-to-one function $f : A \to B$. Similarly, there is a one-to-one function $g : B \to C$. By Exercise 33 in Section 2.3, the composition $g \circ f : A \to C$ is one-to-one. Therefore by definition $|A| \le |C|$. **23.** Using the Axiom of Choice from set theory, choose distinct elements $a_1, a_2, a_3, \ldots$ of A one at a time (this is possible because A is infinite). The resulting set $\{a_1, a_2, a_3, \ldots\}$ is the desired infinite subset of A. **25.** The set of finite strings of characters over a finite alphabet is countably infinite, because we can list these strings in alphabetical order by length. Therefore the infinite set S can be identified with an infinite subset of this countable set, which by Exercise 16 is also countably infinite. **27.** Suppose that $A_1, A_2, A_3, \ldots$ are countable sets. Because A_i is countable, we can list its elements in a sequence as $a_{i1}, a_{i2}, a_{i3}, \ldots$. The elements of the set $\bigcup_{i=1}^{n} A_i$ can be listed by listing all terms a_{ij} with $i + j = 2$, then all terms a_{ij} with $i + j = 3$, then all terms a_{ij} with $i + j = 4$, and so on. **29.** There are a finite number of bit strings of length m, namely, 2^m. The set of all bit, strings is the union of the sets of bit strings of length m for $m = 0, 1, 2, \ldots$. Because the union of a countable number of countable sets is countable (see Exercise 27), there are a countable number of bit strings. **31.** It is clear from the formula that the range of values the function takes on for a fixed value of $m + n$, say $m + n = x$, is $(x - 2)(x - 1)/2 + 1$ through $(x - 2)(x - 1)/2 + (x - 1)$, because m can assume the values $1, 2, 3, \ldots, (x - 1)$ under these conditions, and the first term in the formula is a fixed positive integer when $m + n$ is fixed. To show that this function is one-to-one and onto, we merely need to show that the range of values for $x + 1$ picks up precisely where the range of values for x left off, i.e., that $f(x - 1, 1) + 1 = f(1, x)$. We have $f(x - 1, 1) + 1 = \frac{(x-2)(x-1)}{2} + (x - 1) + 1 = \frac{x^2 - x + 2}{2} = \frac{(x-1)x}{2} + 1 = f(1, x)$. **33.** By the Schröder-Bernstein theorem, it suffices to find one-to-one functions $f : (0, 1) \to [0, 1]$ and $g : [0, 1] \to (0, 1)$. Let $f(x) = x$ and $g(x) = (x + 1)/3$. **35.** Each element A of the power set of the set of positive integers (i.e., $A \subseteq \mathbf{Z}^+$) can be represented uniquely by the bit string $a_1a_2a_3\ldots$, where $a_i = 1$ if $i \in A$ and $a_i = 0$ if $i \notin A$. Assume there were a one-to-one correspondence $f : \mathbf{Z}^+ \to \mathcal{P}(\mathbf{Z}^+)$. Form a new bit string $s = s_1s_2s_3\ldots$ by setting s_i to be 1 minus the ith bit of $f(i)$. Then because s differs in the i bit from $f(i)$, s is not in the range of f, a contradiction. **37.** For any finite alphabet there are a finite number of strings of length n, whenever n is a positive integer. It follows by the result of Exercise 27 that there are only a countable number of strings from any given finite alphabet. Because the set of all computer programs in a particular language is a subset of the set of all strings of a finite alphabet, which is a countable set by the result from Exercise 16, it is itself a countable set. **39.** Exercise 37 shows that there are only a countable number of computer programs. Consequently, there are only a countable number of computable functions. Because, as Exercise 38 shows, there are an uncountable number of functions, not all functions are computable.

Section 2.6

1. **a)** 3×4 **b)** $\begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}$ **c)** $\begin{bmatrix} 2 & 0 & 4 & 6 \end{bmatrix}$ **d)** 1 **e)** $\begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ 1 & 4 & 3 \\ 3 & 6 & 7 \end{bmatrix}$ **3.** **a)** $\begin{bmatrix} 1 & 11 \\ 2 & 18 \end{bmatrix}$ **b)** $\begin{bmatrix} 2 & -2 & -3 \\ 1 & 0 & 2 \\ 9 & -4 & 4 \end{bmatrix}$ **c)** $\begin{bmatrix} -4 & 15 & -4 & 1 \\ -3 & 10 & 2 & -3 \\ 0 & 2 & -8 & 6 \\ 1 & -8 & 18 & -13 \end{bmatrix}$ **5.** $\begin{bmatrix} 9/5 & -6/5 \\ -1/5 & 4/5 \end{bmatrix}$ **7.** $\mathbf{0} + \mathbf{A} = [0 + a_{ij}] = [a_{ij} + 0] = \mathbf{0} + \mathbf{A}$ **9.** $\mathbf{A} + (\mathbf{B} + \mathbf{C}) = [a_{ij} + (b_{ij} + c_{ij})] = [(a_{ij} + b_{ij}) + c_{ij}] = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$ **11.** The number of rows of $\mathbf{A}$ equals the number of columns of $\mathbf{B}$, and the number of columns of $\mathbf{A}$ equals the number of rows of $\mathbf{B}$. **13.** $\mathbf{A}(\mathbf{BC}) = \left[\sum_q a_{iq}\left(\sum_r b_{qr}c_{rl}\right)\right] = \left[\sum_q \sum_r a_{iq}b_{qr}c_{rl}\right] = \left[\sum_r \sum_q a_{iq}b_{qr}c_{rl}\right] = \left[\sum_r \left(\sum_q a_{iq}b_{qr}\right)c_{rl}\right] = (\mathbf{AB})\mathbf{C}$ **15.** $\mathbf{A}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ **17.** **a)** Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$. Then $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$. We have $(\mathbf{A} + \mathbf{B})^t = [a_{ji} + b_{ji}] = [a_{ji}] + [b_{ji}] = \mathbf{A}^t + \mathbf{B}^t$. **b)** Using the same notation as in part (a), we have $\mathbf{B}^t\mathbf{A}^t =$

$\left[\sum_q b_{qi}a_{jq}\right] = \left[\sum_q a_{jq}b_{qi}\right] = (\mathbf{AB})^t$, because the (i, j)th entry is the (j, i)th entry of $\mathbf{AB}$. **19.** The result follows because $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = (ad - bc)\mathbf{I}_2 = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. **21.** $\mathbf{A}^n(\mathbf{A}^{-1})^n = \mathbf{A}(\mathbf{A}\cdots(\mathbf{A}(\mathbf{A}\mathbf{A}^{-1})\mathbf{A}^{-1})\cdots\mathbf{A}^{-1})\mathbf{A}^{-1}$ by the associative law. Because $\mathbf{AA}^{-1} = \mathbf{I}$, working from the inside shows that $\mathbf{A}^n(\mathbf{A}^{-1})^n = \mathbf{I}$. Similarly $(\mathbf{A}^{-1})^n\mathbf{A}^n = \mathbf{I}$. Therefore $(\mathbf{A}^n)^{-1} = (\mathbf{A}^{-1})^n$. **23.** The (i, j)th entry of $\mathbf{A} + \mathbf{A}^t$ is $a_{ij} + a_{ji}$, which equals $a_{ji} + a_{ij}$, the (j, i)th entry of $\mathbf{A} + \mathbf{A}^t$, so by definition $\mathbf{A} + \mathbf{A}^t$ is symmetric. **25.** $x_1 = 1$, $x_2 = -1$, $x_3 = -2$

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

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

31. a) $\mathbf{A} \vee \mathbf{B} = [a_{ij} \vee b_{ij}] = [b_{ij} \vee a_{ij}] = \mathbf{B} \vee \mathbf{A}$ **b)** $\mathbf{A} \wedge \mathbf{B} = [a_{ij} \wedge b_{ij}] = [b_{ij} \wedge a_{ij}] = \mathbf{B} \wedge \mathbf{A}$ **33. a)** $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = [a_{ij}] \vee [b_{ij} \wedge c_{ij}] = [a_{ij} \vee (b_{ij} \wedge c_{ij})] = [(a_{ij} \vee b_{ij}) \wedge (a_{ij} \vee c_{ij})] = [a_{ij} \vee b_{ij}] \wedge [a_{ij} \vee c_{ij}] = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$ **b)** $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = [a_{ij}] \wedge [b_{ij} \vee c_{ij}] = [a_{ij} \wedge (b_{ij} \vee c_{ij})] = [(a_{ij} \wedge b_{ij}) \vee (a_{ij} \wedge c_{ij})] = [a_{ij} \wedge b_{ij}] \vee [a_{ij} \wedge c_{ij}] = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$ **35.** $\mathbf{A} \odot (\mathbf{B} \odot \mathbf{C}) = \left[\bigvee_q a_{iq} \wedge \left(\bigvee_r (b_{qr} \wedge c_{rl})\right)\right] = \left[\bigvee_q \bigvee_r (a_{iq} \wedge b_{qr} \wedge c_{rl})\right] = \left[\bigvee_r \bigvee_q (a_{iq} \wedge b_{qr} \wedge c_{rl})\right] = \left[\bigvee_r \left(\bigvee_q (a_{iq} \wedge b_{qr})\right) \wedge c_{rl}\right] = (\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C}$

Supplementary Exercises

1. a) $\overline{A}$ **b)** $A \cap B$ **c)** $A - B$ **d)** $\overline{A} \cap \overline{B}$ **e)** $A \oplus B$ **3.** Yes **5.** $A - (A - B) = A - (A \cap \overline{B}) = A \cap \overline{(A \cap \overline{B})} = A \cap (\overline{A} \cup B) = (A \cap \overline{A}) \cup (A \cap B) = \emptyset \cup (A \cap B) = A \cap B$ **7.** Let $A = \{1\}$, $B = \emptyset$, $C = \{1\}$. Then $(A - B) - C = \emptyset$, but $A - (B - C) = \{1\}$. **9.** No. For example, let $A = B = \{a, b\}$, $C = \emptyset$, and $D = \{a\}$. Then $(A - B) - (C - D) = \emptyset - \emptyset = \emptyset$, but $(A - C) - (B - D) = \{a, b\} - \{b\} = \{a\}$. **11. a)** $|\emptyset| \le |A \cap B| \le |A| \le |A \cup B| \le |U|$ **b)** $|\emptyset| \le |A - B| \le |A \oplus B| \le |A \cup B| \le |A| + |B|$ **13. a)** Yes, no **b)** Yes, no **c)** f has inverse with $f^{-1}(a) = 3$, $f^{-1}(b) = 4$, $f^{-1}(c) = 2$, $f^{-1}(d) = 1$; g has no inverse. **15.** If f is one-to-one, then f provides a bijection between S and $f(S)$, so they have the same cardinality. If f is not one-to-one, then there exist elements x and y in S such that $f(x) = f(y)$. Let $S = \{x, y\}$. Then $|S| = 2$ but $|f(S)| = 1$. **17.** Let $x \in A$. Then $S_f(\{x\}) = \{f(y) \mid y \in \{x\}\} = \{f(x)\}$. By the same reasoning, $S_g(\{x\}) = \{g(x)\}$. Because $S_f = S_g$, we can conclude that $\{f(x)\} = \{g(x)\}$, and so necessarily $f(x) = g(x)$. **19.** The equation is true if and only if the sum of the fractional parts of x and y is less than 1. **21.** The equation is true if and only if either both x and y are integers, or x is not an integer but the sum of the fractional parts of x and y is less than or equal to 1. **23.** If x is an integer, then $\lfloor x \rfloor + \lfloor m - x \rfloor = x + m - x = m$. Otherwise, write x in terms of its integer and fractional parts: $x = n + \epsilon$, where $n = \lfloor x \rfloor$ and $0 < \epsilon < 1$. In this case $\lfloor x \rfloor + \lfloor m - x \rfloor = \lfloor n + \epsilon \rfloor + \lfloor m - n - \epsilon \rfloor = n + m - n - 1 = m - 1$. **25.** Write $n = 2k + 1$ for some integer k. Then $n^2 = 4k^2 + 4k + 1$, so $n^2/4 = k^2 + k + \frac{1}{4}$. Therefore, $\lceil n^2/4 \rceil = k^2 + k + 1$. But $(n^2 + 3)/4 = (4k^2 + 4k + 1 + 3)/4 = k^2 + k + 1$. **27.** Let $x = n + (r/m) + \epsilon$, where n is an integer, r is a nonnegative integer less than m, and ϵ is a real number with $0 \le \epsilon < 1/m$. The left-hand side is $\lfloor nm + r + m\epsilon \rfloor = nm + r$. On the right-hand side, the terms $\lfloor x \rfloor$ through $\lfloor x + (m + r - 1)/m \rfloor$ are all just n and the terms from $\lfloor x + (m - r)/m \rfloor$ on are all $n + 1$. Therefore, the right-hand side is $(m - r)n + r(n + 1) = nm + r$, as well. **29.** 101 **31.** $a_1 = 1$; $a_{2n+1} = n \cdot a_{2n}$ for all $n > 0$; and $a_{2n} = n + a_{2n-1}$ for all $n > 0$. The next four terms are 5346, 5353, 37471, and 37479. **33.** If each $f^{-1}(j)$ is countable, then $S = f^{-1}(1) \cup f^{-1}(2) \cup \cdots$ is the countable union of countable sets and is therefore countable by Exercise 27 in Section 2.5. **35.** Because there is a one-to-one correspondence between $\mathbf{R}$ and the open interval $(0, 1)$ (given by $f(x) = 2\arctan(x)/\pi$), it suffices to shows that $|(0, 1) \times (0, 1)| = |(0, 1)|$. By the Schröder-Bernstein theorem it suffices to find injective functions $f : (0, 1) \to (0, 1) \times (0, 1)$ and $g : (0, 1) \times (0, 1) \to (0, 1)$. Let $f(x) = (x, \frac{1}{2})$. For g we follow the hint. Suppose $(x, y) \in (0, 1) \times (0, 1)$, and represent x and y with their decimal expansions $x = 0.x_1x_2x_3\ldots$ and $y = 0.y_1y_2y_3\ldots$, never choosing the expansion of any number that ends in an infinite string of 9s. Let $g(x, y)$ be the decimal expansion obtained by interweaving these two strings, namely $0.x_1y_1x_2y_2x_3y_3\ldots$. **37.** $\mathbf{A}^{4n} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{A}^{4n+1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\mathbf{A}^{4n+2} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $\mathbf{A}^{4n+3} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, for $n \ge 0$ **39.** Suppose that $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Let $\mathbf{B} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Because $\mathbf{AB} = \mathbf{BA}$, it follows that $c = 0$ and $a = d$. Let $\mathbf{B} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. Because $\mathbf{AB} = \mathbf{BA}$, it follows that $b = 0$. Hence, $\mathbf{A} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = a\mathbf{I}$. **41. a)** Let $\mathbf{A} \odot \mathbf{0} = [b_{ij}]$. Then $b_{ij} = (a_{i1} \wedge 0) \vee \cdots \vee (a_{ip} \wedge 0) = 0$. Hence, $\mathbf{A} \odot \mathbf{0} = \mathbf{0}$. Similarly $\mathbf{0} \odot \mathbf{A} = 0$. **b)** $\mathbf{A} \vee \mathbf{0} = [a_{ij} \vee 0] = [a_{ij}] = \mathbf{A}$. Hence $\mathbf{A} \vee \mathbf{0} = \mathbf{A}$. Similarly $\mathbf{0} \vee \mathbf{A} = \mathbf{A}$. **c)** $\mathbf{A} \wedge \mathbf{0} = [a_{ij} \wedge 0] = [0] = \mathbf{0}$. Hence $\mathbf{A} \wedge \mathbf{0} = \mathbf{0}$. Similarly $\mathbf{0} \wedge \mathbf{A} = \mathbf{0}$.

CHAPTER 3

Section 3.1

1. $max := 1$, $i := 2$, $max := 8$, $i := 3$, $max := 12$, $i := 4$, $i := 5$, $i := 6$, $i := 7$, $max := 14$, $i := 8$, $i := 9$, $i := 10$, $i := 11$

3. **procedure** *AddUp*($a_1, \ldots, a_n$: integers)
   $sum := a_1$
   for $i := 2$ **to** n
      $sum := sum + a_i$
   return *sum*

5. **procedure** *duplicates*($a_1, a_2, \ldots, a_n$: integers in nondecreasing order)
   $k := 0$ {this counts the duplicates}
   $j := 2$
   while $j \le n$
     if $a_j = a_{j-1}$ **then**
       $k := k + 1$
       $c_k := a_j$
       while $j \le n$ and $a_j = c_k$
         $j := j + 1$
     $j := j + 1$
   $\{c_1, c_2, \ldots, c_k$ is the desired list$\}$

7. **procedure** *last even location*($a_1, a_2, \ldots, a_n$: integers)
   $k := 0$
   for $i := 1$ **to** n
     if a_i is even **then** $k := i$
   return k $\{k = 0$ if there are no evens$\}$

9. **procedure** *palindrome check*($a_1 a_2 \ldots a_n$: string)
   $answer :=$ **true**
   for $i := 1$ **to** $\lfloor n/2 \rfloor$
     if $a_i \ne a_{n+1-i}$ **then** $answer :=$ **false**
   return *answer*

11. **procedure** *interchange*(x, y: real numbers)
    $z := x$
    $x := y$
    $y := z$

The minimum number of assignments needed is three.

13. Linear search: $i := 1$, $i := 2$, $i := 3$, $i := 4$, $i := 5$, $i := 6$, $i := 7$, $location := 7$; binary search: $i := 1$, $j := 8$, $m := 4$, $i := 5$, $m := 6$, $i := 7$, $m := 7$, $j := 7$, $location := 7$

15. **procedure** *insert*($x, a_1, a_2, \ldots, a_n$: integers)
    {the list is in order: $a_1 \le a_2 \le \cdots \le a_n$}
    $a_{n+1} := x + 1$
    $i := 1$
    while $x > a_i$
      $i := i + 1$
    for $j := 0$ **to** $n - i$
      $a_{n-j+1} := a_{n-j}$
    $a_i := x$
    {x has been inserted into correct position}

17. **procedure** *first largest*($a_1, \ldots, a_n$: integers)
    $max := a_1$
    $location := 1$
    for $i := 2$ **to** n
      if $max < a_i$ **then**
        $max := a_i$
        $location := i$
    return *location*

19. **procedure** *mean-median-max-min*(a, b, c: integers)
    $mean := (a + b + c)/3$
    {the six different orderings of a, b, c with respect to $\ge$ will be handled separately}
    if $a \ge b$ **then**
      if $b \ge c$ **then** $median := b$; $max := a$; $min := c$
      $\vdots$
    (The rest of the algorithm is similar.)

21. **procedure** *first-three*($a_1, a_2, \ldots, a_n$: integers)
    if $a_1 > a_2$ **then** interchange a_1 and a_2
    if $a_2 > a_3$ **then** interchange a_2 and a_3
    if $a_1 > a_2$ **then** interchange a_1 and a_2

23. **procedure** *onto*(f: function from A to B where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$, $a_1, \ldots, a_n$, $b_1, \ldots, b_m$ are integers)
    for $i := 1$ **to** m
      $hit(b_i) := 0$
    $count := 0$
    for $j := 1$ **to** n
      if $hit(f(a_j)) = 0$ **then**
        $hit(f(a_j)) := 1$
        $count := count + 1$
    if $count = m$ **then return true else return false**

25. **procedure** *ones*(a: bit string, $a = a_1 a_2 \ldots a_n$)
    $count := 0$
    for $i := 1$ **to** n
      if $a_i := 1$ **then**
        $count := count + 1$
    return *count*

27. **procedure** *ternary search*(s: integer, $a_1, a_2, \ldots, a_n$: increasing integers)
    $i := 1$
    $j := n$
    while $i < j - 1$
      $l := \lfloor (i + j)/3 \rfloor$
      $u := \lfloor 2(i + j)/3 \rfloor$
      if $x > a_u$ **then** $i := u + 1$
      else if $x > a_l$ **then**
        $i := l + 1$
        $j := u$
      else $j := l$
    if $x = a_i$ **then** $location := i$
    else if $x = a_j$ **then** $location := j$

```
    else location := 0
    return location {0 if not found}
```

29.
```
procedure find a mode(a_1, a_2, ..., a_n: nondecreasing
    integers)
modecount := 0
i := 1
while i ≤ n
  value := a_i
  count := 1
  while i ≤ n and a_i = value
    count := count + 1
    i := i + 1
  if count > modecount then
    modecount := count
    mode := value
return mode
```

31.
```
procedure find duplicate(a_1, a_2, ..., a_n: integers)
location := 0
i := 2
while i ≤ n and location = 0
  j := 1
  while j < i and location = 0
    if a_i = a_j then location := i
    else j := j + 1
  i := i + 1
return location
{location is the subscript of the first value that
 repeats a previous value in the sequence}
```

33.
```
procedure find decrease(a_1, a_2, ..., a_n: positive
    integers)
location := 0
i := 2
while i ≤ n and location = 0
  if a_i < a_{i-1} then location := i
  else i := i + 1
return location
{location is the subscript of the first value less than
 the immediately preceding one}
```

35. At the end of the first pass: 1, 3, 5, 4, 7; at the end of the second pass: 1, 3, 4, 5, 7; at the end of the third pass: 1, 3, 4, 5, 7; at the end of the fourth pass: 1, 3, 4, 5, 7

37.
```
procedure better bubblesort(a_1, ..., a_n: integers)
i := 1; done := false
while i < n and done = false
  done := true
  for j := 1 to n − i
    if a_j > a_{j+1} then
      interchange a_j and a_{j+1}
      done := false
  i := i + 1
{a_1, ..., a_n is in increasing order}
```

39. At the end of the first, second, and third passes: 1, 3, 5, 7, 4; at the end of the fourth pass: 1, 3, 4, 5, 7 **41. a)** 1, 5, 4, 3, 2; 1, 2, 4, 3, 5; 1, 2, 3, 4, 5; 1, 2, 3, 4, 5 **b)** 1, 4, 3, 2, 5; 1, 2, 3, 4, 5; 1, 2, 3, 4, 5; 1, 2, 3, 4, 5 **c)** 1, 2, 3, 4, 5; 1, 2, 3, 4, 5; 1, 2, 3, 4, 5; 1, 2, 3, 4, 5 **43.** We carry out the linear search algorithm given as Algorithm 2 in this section, except that we replace $x \neq a_i$ by $x < a_i$, and we replace the **else** clause with **else** *location* $:= n + 1$. **45.** $2 + 3 + 4 + \cdots + n = (n^2 + n - 2)/2$ **47.** Find the location for the 2 in the list 3 (one comparison), and insert it in front of the 3, so the list now reads 2, 3, 4, 5, 1, 6. Find the location for the 4 (compare it to the 2 and then the 3), and insert it, leaving 2, 3, 4, 5, 1, 6. Find the location for the 5 (compare it to the 3 and then the 4), and insert it, leaving 2, 3, 4, 5, 1, 6. Find the location for the 1 (compare it to the 3 and then the 2 and then the 2 again), and insert it, leaving 1, 2, 3, 4, 5, 6. Find the location for the 6 (compare it to the 3 and then the 4 and then the 5), and insert it, giving the final answer 1, 2, 3, 4, 5, 6.

49.
```
procedure binary insertion sort(a_1, a_2, ..., a_n:
    real numbers with n ≥ 2)
for j := 2 to n
  {binary search for insertion location i}
  left := 1
  right := j − 1
  while left < right
    middle := ⌊(left + right)/2⌋
    if a_j > a_middle then left := middle + 1
    else right := middle
  if a_j < a_left then i := left else i := left + 1
  {insert a_j in location i by moving a_i through a_{j−1}
     toward back of list}
  m := a_j
  for k := 0 to j − i − 1
    a_{j−k} := a_{j−k−1}
  a_i := m
{a_1, a_2, ..., a_n are sorted}
```

51. The variation from Exercise 50 **53. a)** Two quarters, one penny **b)** Two quarters, one dime, one nickel, four pennies **c)** A three quarters, one penny **d)** Two quarters, one dime **55.** Greedy algorithm uses fewest coins in parts (a), (c), and (d). **a)** Two quarters, one penny **b)** Two quarters, one dime, nine pennies **c)** Three quarters, one penny **d)** Two quarters, one dime **57.** The 9:00–9:45 talk, the 9:50–10:15 talk, the 10:15–10:45 talk, the 11:00–11:15 talk **59. a)** Order the talks by starting time. Number the lecture halls 1, 2, 3, and so on. For each talk, assign it to lowest numbered lecture hall that is currently available. **b)** If this algorithm uses n lecture halls, then at the point the nth hall was first assigned, it *had* to be used (otherwise a lower-numbered hall would have been assigned), which means that n talks were going on simultaneously (this talk just assigned and the $n - 1$ talks currently in halls 1 through $n - 1$). **61.** Here we assume that the men are the suitors and the women the suitees.

```
procedure stable(M_1, M_2, ..., M_s, W_1, W_2, ..., W_s:
    preference lists)
for i := 1 to s
  mark man i as rejected
for i := 1 to s
  set man i's rejection list to be empty
for j := 1 to s
```

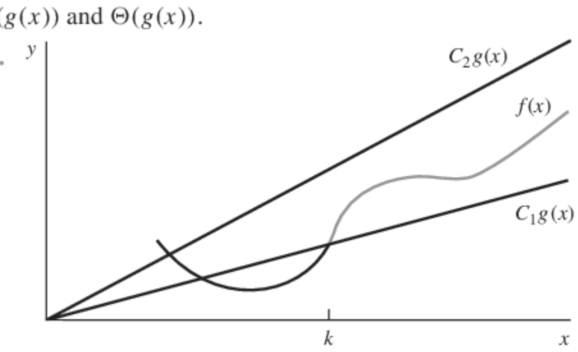
```
    set woman j's proposal list to be empty
while rejected men remain
    for i := 1 to s
        if man i is marked rejected then add i to the
        proposal list for the woman j who ranks highest
        on his preference list but does not appear on his
        rejection list, and mark i as not rejected
    for j := 1 to s
        if woman j's proposal list is nonempty then
        remove from j's proposal list all men i
        except the man i_0 who ranks highest on her
        preference list, and for each such man i mark
        him as rejected and add j to his rejection list
for j := 1 to s
    match j with the one man on j's proposal list
{This matching is stable.}
```

63. If the assignment is not stable, then there is a man m and a woman w such that m prefers w to the woman w' with whom he is matched, and w prefers m to the man with whom she is matched. But m must have proposed to w before he proposed to w', because he prefers the former. Because m did not end up matched with w, she must have rejected him. Women reject a suitor only when they get a better proposal, and they eventually get matched with a pending suitor, so the woman with whom w is matched must be better in her eyes than m, contradicting our original assumption. Therefore the marriage is stable. 65. Run the two programs on their inputs concurrently and report which one halts.

Section 3.2

1. The choices of C and k are not unique. **a)** $C = 1, k = 10$ **b)** $C = 4, k = 7$ **c)** No **d)** $C = 5, k = 1$ **e)** $C = 1, k = 0$ **f)** $C = 1, k = 2$ 3. $x^4 + 9x^3 + 4x + 7 \le 4x^4$ for all $x > 9$; witnesses $C = 4, k = 9$ 5. $(x^2+1)/(x+1) = x - 1 + 2/(x+1) < x$ for all $x > 1$; witnesses $C = 1, k = 1$ 7. The choices of C and k are not unique. **a)** $n = 3, C = 3, k = 1$ **b)** $n = 3, C = 4, k = 1$ **c)** $n = 1, C = 2, k = 1$ **d)** $n = 0, C = 2, k = 1$ 9. $x^2 + 4x + 17 \le 3x^3$ for all $x > 17$, so $x^2 + 4x + 17$ is $O(x^3)$, with witnesses $C = 3, k = 17$. However, if x^3 were $O(x^2 + 4x + 17)$, then $x^3 \le C(x^2 + 4x + 17) \le 3Cx^2$ for some C, for all sufficiently large x, which implies that $x \le 3C$ for all sufficiently large x, which is impossible. Hence, x^3 is not $O(x^2 + 4x + 17)$. 11. $3x^4 + 1 \le 4x^4 = 8(x^4/2)$ for all $x > 1$, so $3x^4 + 1$ is $O(x^4/2)$, with witnesses $C = 8, k = 1$. Also $x^4/2 \le 3x^4 + 1$ for all $x > 0$, so $x^4/2$ is $O(3x^4 + 1)$, with witnesses $C = 1, k = 0$. 13. Because $2^n \le 3^n$ for all $n > 0$, it follows that 2^n is $O(3^n)$, with witnesses $C = 1, k = 0$. However, if 3^n were $O(2^n)$, then for some C, $3^n \le C \cdot 2^n$ for all sufficiently large n. This says that $C \ge (3/2)^n$ for all sufficiently large n, which is impossible. Hence, 3^n is not $O(2^n)$. 15. All functions for which there exist real numbers k and C with $|f(x)| \le C$ for $x > k$. These are the functions $f(x)$ that are bounded for all sufficiently large x. 17. There are constants C_1, C_2, k_1, and k_2 such that $|f(x)| \le C_1|g(x)|$ for all $x > k_1$ and $|g(x)| \le C_2|h(x)|$ for all $x > k_2$. Hence, for $x > \max(k_1, k_2)$ it follows that $|f(x)| \le C_1|g(x)| \le C_1C_2|h(x)|$. This shows that $f(x)$ is $O(h(x))$. 19. 2^{n+1} is $O(2^n)$; 2^{2n} is not. 21. $1000 \log n$, $\sqrt{n}$, $n \log n$, $n^2/1000000$, 2^n, 3^n, $2n!$ 23. The algorithm that uses $n \log n$ operations 25. **a)** $O(n^3)$ **b)** $O(n^5)$ **c)** $O(n^3 \cdot n!)$ 27. **a)** $O(n^2 \log n)$ **b)** $O(n^2(\log n)^2)$ **c)** $O(n^{2^n})$ 29. **a)** Neither $\Theta(x^2)$ nor $\Omega(x^2)$ **b)** $\Theta(x^2)$ and $\Omega(x^2)$ **c)** Neither $\Theta(x^2)$ nor $\Omega(x^2)$ **d)** $\Omega(x^2)$, but not $\Theta(x^2)$ **e)** $\Omega(x^2)$, but not $\Theta(x^2)$ **f)** $\Omega(x^2)$ and $\Theta(x^2)$ 31. If $f(x)$ is $\Theta(g(x))$, then there exist constants C_1 and C_2 with $C_1|g(x)| \le |f(x)| \le C_2|g(x)|$. It follows that $|f(x)| \le C_2|g(x)|$ and $|g(x)| \le (1/C_1)|f(x)|$ for $x > k$. Thus, $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$. Conversely, suppose that $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$. Then there are constants C_1, C_2, k_1, and k_2 such that $|f(x)| \le C_1|g(x)|$ for $x > k_1$ and $|g(x)| \le C_2|f(x)|$ for $x > k_2$. We can assume that $C_2 > 0$ (we can always make C_2 larger). Then we have $(1/C_2)|g(x)| \le |f(x)| \le C_1|g(x)|$ for $x > \max(k_1, k_2)$. Hence, $f(x)$ is $\Theta(g(x))$. 33. If $f(x)$ is $\Theta(g(x))$, then $f(x)$ is both $O(g(x))$ and $\Omega(g(x))$. Hence, there are positive constants C_1, k_1, C_2, and k_2 such that $|f(x)| \le C_2|g(x)|$ for all $x > k_2$ and $|f(x)| \ge C_1|g(x)|$ for all $x > k_1$. It follows that $C_1|g(x)| \le |f(x)| \le C_2|g(x)|$ whenever $x > k$, where $k = \max(k_1, k_2)$. Conversely, if there are positive constants C_1, C_2, and k such that $C_1|g(x)| \le |f(x)| \le C_2|g(x)|$ for $x > k$, then taking $k_1 = k_2 = k$ shows that $f(x)$ is both $O(g(x))$ and $\Theta(g(x))$.

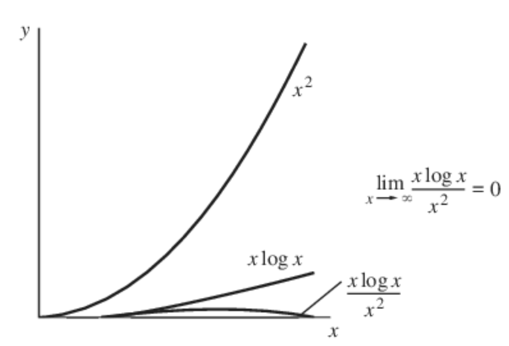
35.



37. If $f(x)$ is $\Theta(1)$, then $|f(x)|$ is bounded between positive constants C_1 and C_2. In other words, $f(x)$ cannot grow larger than a fixed bound or smaller than the negative of this bound and must not get closer to 0 than some fixed bound. 39. Because $f(x)$ is $O(g(x))$, there are constants C and k such that $|f(x)| \le C|g(x)|$ for $x > k$. Hence, $|f^n(x)| \le C^n|g^n(x)|$ for $x > k$, so $f^n(x)$ is $O(g^n(x))$ by taking the constant to be C^n. 41. Because $f(x)$ and $g(x)$ are increasing and unbounded, we can assume $f(x) \ge 1$ and $g(x) \ge 1$ for sufficiently large x. There are constants C and k with $f(x) \le Cg(x)$ for $x > k$. This implies that $\log f(x) \le \log C + \log g(x) < 2 \log g(x)$ for sufficiently large x. Hence, $\log f(x)$ is $O(\log g(x))$. 43. By definition there are positive constraints C_1, C_1', C_2, C_2', k_1, k_1', k_2, and k_2' such that $f_1(x) \ge C_1|g(x)|$ for all $x > k_1$, $f_1(x) \le C_1'|g(x)|$ for all $x > k_1'$, $f_2(x) \ge C_2|g(x)|$ for all $x > k_2$, and $f_2(x) \le C_2'|g(x)|$ for all $x > k_2'$. Adding the first and third inequalities shows that $f_1(x) + f_2(x) \ge (C_1 + C_2)|g(x)|$ for all $x > k$ where

$k = \max(k_1, k_2)$. Adding the second and fourth inequalities shows that $f_1(x) + f_2(x) \le (C_1' + C_2')|g(x)|$ for all $x > k'$ where $k' = \max(k_1', k_2')$. Hence, $f_1(x) + f_2(x)$ is $\Theta(g(x))$. This is no longer true if f_1 and f_2 can assume negative values. **45.** This is false. Let $f_1 = x^2 + 2x$, $f_2(x) = x^2 + x$, and $g(x) = x^2$. Then $f_1(x)$ and $f_2(x)$ are both $O(g(x))$, but $(f_1 - f_2)(x)$ is not. **47.** Take $f(n)$ to be the function with $f(n) = n$ if n is an odd positive integer and $f(n) = 1$ if n is an even positive integer and $g(n)$ to be the function with $g(n) = 1$ if n is an odd positive integer and $g(n) = n$ if n is an even positive integer. **49.** There are positive constants $C_1, C_2, C_1', C_2', k_1, k_1', k_2$, and k_2' such that $|f_1(x)| \ge C_1|g_1(x)|$ for all $x > k_1$, $|f_1(x)| \le C_1'|g_1(x)|$ for all $x \ge k_1'$, $|f_2(x)| > C_2|g_2(x)|$ for all $x > k_2$, and $|f_2(x)| \le C_2'|g_2(x)|$ for all $x > k_2'$. Because f_2 and g_2 are never zero, the last two inequalities can be rewritten as $|1/f_2(x)| \le (1/C_2)|1/g_2(x)|$ for all $x > k_2$ and $|1/f_2(x)| \ge (1/C_2')|1/g_2(x)|$ for all $x > k_2'$. Multiplying the first and rewritten fourth inequalities shows that $|f_1(x)/f_2(x)| \ge (C_1/C_2')|g_1(x)/g_2(x)|$ for all $x > \max(k_1, k_2')$, and multiplying the second and rewritten third inequalities gives $|f_1(x)/f_2(x)| \le (C_1'/C_2)|g_1(x)/g_2(x)|$ for all $x > \max(k_1', k_2)$. It follows that f_1/f_2 is big-Theta of g_1/g_2. **51.** There exist positive constants C_1, C_2, k_1, k_2, k_1', k_2' such that $|f(x, y)| \le C_1|g(x, y)|$ for all $x > k_1$ and $y > k_2$ and $|f(x, y)| \ge C_2|g(x, y)|$ for all $x > k_1'$ and $y > k_2'$. **53.** $(x^2 + xy + x \log y)^3 < (3x^2y^3) = 27x^6y^3$ for $x > 1$ and $y > 1$, because $x^2 < x^2y$, $xy < x^2y$, and $x \log y < x^2y$. Hence, $(x^2 + xy + x \log y)^3$ is $O(x^6y^3)$. **55.** For all positive real numbers x and y, $\lfloor xy \rfloor \le xy$. Hence, $\lfloor xy \rfloor$ is $O(xy)$ from the definition, taking $C = 1$ and $k_1 = k_2 = 0$. **57.** Clearly $n^d < n^c$ for all $n \ge 2$; therefore n^d is $O(n^c)$. The ratio $n^d/n^c = n^{d-c}$ is unbounded so there is no constant C such that $n^d \le Cn^c$ for large n. **59.** If f and g are positive-valued functions such that $\lim_{n\to\infty} f(x)/g(x) = C < \infty$, then $f(x) < (C+1)g(x)$ for large enough x, so $f(n)$ is $O(g(n))$. If that limit is ∞, then clearly $f(n)$ is not $O(g(n))$. Here repeated applications of L'Hôpital's rule shows that $\lim_{x\to\infty} x^d/b^x = 0$ and $\lim_{x\to\infty} b^x/x^d = \infty$. **61. a)** $\lim_{x\to\infty} x^2/x^3 = \lim_{x\to\infty} 1/x = 0$ **b)** $\lim_{x\to\infty} \frac{x \log x}{x^2} = \lim_{x\to\infty} \frac{\log x}{x} = \lim_{x\to\infty} \frac{1}{x \ln 2} = 0$ (using L'Hôpital's rule) **c)** $\lim_{x\to\infty} \frac{x^2}{2^x} = \lim_{x\to\infty} \frac{2x}{2^x \cdot \ln 2} = \lim_{x\to\infty} \frac{2}{2^x \cdot (\ln 2)^2} = 0$ (using L'Hôpital's rule) **d)** $\lim_{x\to\infty} \frac{x^2+x+1}{x^2} = \lim_{x\to\infty} \left(1 + \frac{1}{x} + \frac{1}{x^2}\right) = 1 \ne 0$

63.



65. No. Take $f(x) = 1/x^2$ and $g(x) = 1/x$. **67. a)** Because $\lim_{x\to\infty} f(x)/g(x) = 0$, $|f(x)|/|g(x)| < 1$ for sufficiently large x. Hence, $|f(x)| < |g(x)|$ for $x > k$ for some constant k. Therefore, $f(x)$ is $O(g(x))$. **b)** Let $f(x) = g(x) = x$. Then $f(x)$ is $O(g(x))$, but $f(x)$ is not $o(g(x))$ because $f(x)/g(x) = 1$. **69.** Because $f_2(x)$ is $o(g(x))$, from Exercise 67(a) it follows that $f_2(x)$ is $O(g(x))$. By Corollary 1, we have $f_1(x) + f_2(x)$ is $O(g(x))$. **71.** We can easily show that $(n-i)(i+1) \ge n$ for $i = 0, 1, \ldots, n-1$. Hence, $(n!)^2 = (n \cdot 1)((n-1) \cdot 2) \cdot ((n-2) \cdot 3) \cdots (2 \cdot (n-1)) \cdot (1 \cdot n) \ge n^n$. Therefore, $2 \log n! \ge n \log n$. **73.** Compute that $\log 5! \approx 6.9$ and $(5 \log 5)/4 \approx 2.9$, so the inequality holds for $n = 5$. Assume $n \ge 6$. Because $n!$ is the product of all the integers from n down to 1, we have $n! > n(n-1)(n-2)\cdots\lceil n/2 \rceil$ (because at least the term 2 is missing). Note that there are more than $n/2$ terms in this product, and each term is at least as big as $n/2$. Therefore the product is greater than $(n/2)^{(n/2)}$. Taking the log of both sides of the inequality, we have $\log n! > \log\left(\frac{n}{2}\right)^{n/2} = \frac{n}{2}\log\frac{n}{2} = \frac{n}{2}(\log n - 1) > (n \log n)/4$, because $n > 4$ implies $\log n - 1 > (\log n)/2$. **75.** All are not asymptotic.

Section 3.3

1. $O(1)$ **3.** $O(n^2)$ **5.** $2n - 1$ **7.** Linear **9.** $O(n)$
11. a) procedure *disjointpair*$(S_1, S_2, \ldots, S_n$: subsets of $\{1, 2, \ldots, n\})$

answer := **false**
for $i := 1$ **to** n
  for $j := i + 1$ **to** n
    disjoint := **true**
    for $k := 1$ **to** n
      if $k \in S_i$ and $k \in S_j$ **then** *disjoint* := **false**
    if *disjoint* **then** *answer* := **true**
return *answer*

b) $O(n^3)$ **13. a)** *power* := 1, y := 1; i := 1, *power* := 2, $y := 3$; $i := 2$, *power* := 4, y := 15 **b)** $2n$ multiplications and n additions **15. a)** $2^{10^9} \approx 10^{3 \times 10^8}$ **b)** 10^9 **c)** 3.96×10^7 **d)** 3.16×10^4 **e)** 29 **f)** 12 **17. a)** $2^{2^{60 \cdot 10^{12}}}$ **b)** $2^{60 \cdot 10^{12}}$ **c)** $\lfloor 2^{\sqrt{60 \cdot 10^6}} \rfloor \approx 2 \times 10^{2331768}$ **d)** 60,000,000 **e)** 7,745,966 **f)** 45 **g)** 6 **19. a)** 36 years **b)** 13 days **c)** 19 minutes **21. a)** Less than 1 millisecond more **b)** 100 milliseconds more **c)** $2n + 1$ milliseconds more **d)** $3n^2 + 3n + 1$ milliseconds more **e)** Twice as much time **f)** 2^{2n+1} times as many milliseconds **g)** $n + 1$ times as many milliseconds **23.** The average number of comparisons is $(3n + 4)/2$. **25.** $O(\log n)$ **27.** $O(n)$ **29.** $O(n^2)$ **31.** $O(n)$ **33.** $O(n)$ **35.** $O(\log n)$ comparisons; $O(n^2)$ swaps **37.** $O(n^2 2^n)$ **39. a)** doubles **b)** increases by 1 **41.** Use Algorithm 1, where **A** and **B** are now $n \times n$ upper triangular matrices, by replacing m by n in line 1, and having q iterate only from i to j, rather than from 1 to k. **43.** $n(n+1)(n+2)/6$ **45.** $\mathbf{A}((\mathbf{BC})\mathbf{D})$

Supplementary Exercises

1. a)

```
procedure last max(a_1, ..., a_n: integers)
max := a_1
last := 1
i := 2
while i ≤ n
  if a_i ≥ max then
    max := a_i
    last := i
  i := i + 1
return last
```

b) $2n - 1 = O(n)$ comparisons

3. a)

```
procedure pair zeros(b_1 b_2 ... b_n: bit string, n ≥ 2)
x := b_1
y := b_2
k := 2
while k < n and (x ≠ 0 or y ≠ 0)
  k := k + 1
  x := y
  y := b_k
if x = 0 and y = 0 then print "YES"
else print "NO"
```

b) $O(n)$

5. a) and **b)**

```
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}
```

c) $2n - 2$

7. Before any comparisons are done, there is a possibility that each element could be the maximum and a possibility that it could be the minimum. This means that there are $2n$ different possibilities, and $2n - 2$ of them have to be eliminated through comparisons of elements, because we need to find the unique maximum and the unique minimum. We classify comparisons of two elements as "virgin" or "nonvirgin," depending on whether or not both elements being compared have been in any previous comparison. A virgin comparison eliminates the possibility that the larger one is the minimum and that the smaller one is the maximum; thus each virgin comparison eliminates two possibilities, but it clearly cannot do more. A nonvirgin comparison must be between two elements that are still in the running to be the maximum or two elements that are still in the running to be the minimum, and at least one of these elements must *not* be in the running for the other category. For example, we might be comparing x and y, where all we know is that x has been eliminated as the minimum. If we find that $x > y$ in this case, then only one possibility has been ruled out—we now know that y is not the maximum. Thus in the worst case, a nonvirgin comparison eliminates only one possibility. (The cases of other nonvirgin comparisons are similar.) Now there are at most $\lfloor n/2 \rfloor$ comparisons of elements that have not been compared before, each removing two possibilities; they remove $2\lfloor n/2 \rfloor$ possibilities altogether. Therefore we need $2n - 2 - 2\lfloor n/2 \rfloor$ more comparisons that, as we have argued, can remove only one possibility each, in order to find the answers in the worst case, because $2n - 2$ possibilities have to be eliminated. This gives us a total of $2n - 2 - 2\lfloor n/2 \rfloor + \lfloor n/2 \rfloor$ comparisons in all. But $2n - 2 - 2\lfloor n/2 \rfloor + \lfloor n/2 \rfloor = 2n - 2 - \lfloor n/2 \rfloor = 2n - 2 + \lceil -n/2 \rceil = \lceil 2n - n/2 \rceil - 2 = \lceil 3n/2 \rceil - 2$, as desired. **9.** The following algorithm has worst-case complexity $O(n^4)$.

```
procedure equal sums(a_1, a_2, ..., a_n)
for i := 1 to n
  for j := i + 1 to n {since we want i < j}
    for k := 1 to n
      for l := k + 1 to n {since we want k < l}
        if a_i + a_j = a_k + a_l and (i, j) ≠ (k, l)
          then output these pairs
```

11. At end of first pass: 3, 1, 4, 5, 2, 6; at end of second pass: 1, 3, 2, 4, 5, 6; at end of third pass: 1, 2, 3, 4, 5, 6; fourth pass finds nothing to exchange and algorithm terminates **13.** There are possibly as many as n passes through the list, and each pass uses $O(n)$ comparisons. Thus there are $O(n^2)$ comparisons in all. **15.** Because $\log n < n$, we have $(n \log n + n^2)^3 \le (n^2 + n^2)^3 \le (2n^2)^3 = 8n^6$ for all $n > 0$. This proves that $(n \log n + n^2)^3$ is $O(n^6)$, with witnesses $C = 8$ and $k = 0$. **17.** $O(x^2 2^x)$ **19.** Note that $\frac{n!}{2^n} = \frac{n}{2} \cdot \frac{n-1}{2} \cdots \frac{3}{2} \cdot \frac{2}{2} \cdot \frac{1}{2} > \frac{n}{2} \cdot 1 \cdot 1 \cdots 1 \cdot \frac{1}{2} = \frac{n}{4}$. **21.** All of these functions are of the same order. **23.** 2^{107} **25.** $(\log n)^2$, $2^{\sqrt{\log_2 n}}$, $n(\log n)^{1001}$, $n^{1.0001}$, 1.0001^n, n^n **27.** For example, $f(n) = n^{2\lfloor n/2 \rfloor + 1}$ and $g(n) = n^{2\lceil n/2 \rceil}$

29. a)

```
procedure brute(a_1, a_2, ..., a_n : integers)
  for i := 1 to n − 1
    for j := i + 1 to n
      for k := 1 to n
        if a_i + a_j = a_k then return true else return false
```

b) $O(n^3)$

31. For m_1: w_1 and w_2; for m_2: w_1 and w_3; for m_3: w_2 and w_3; for w_1: m_1 and m_2; for w_2: m_1 and m_3; for w_3: m_2 and m_3 **33.** A matching in which each woman is assigned her valid partner ranking highest on her preference list is female optimal; a matching in which each man is assigned his valid partner ranking lowest on his preference list is male pessimal. **35. a)** Modify the preamble to Exercise 60 in Section 3.1 so that there are s men $m_1, m_2, \ldots, m_s$ and t women $w_1, w_2, \ldots, w_t$. A matching will contain $\min(s, t)$ marriages. The definition of "stable marriage" is the same, with the understanding that each person prefers any mate to being unmatched. **b)** Create $|s - t|$ fictitious people (men or women, whichever is in shorter supply) so that the number of men and the number of women become the same, and put these fictitious people at the bottom of everyone's preference lists. **c)** This follows immediately from Exercise 63 in Section 3.1. 37. 5; 15 39. The first situation in Exercise 37 41. **a)** For each subset S of $\{1, 2, \ldots, n\}$, compute $\sum_{j\in S} w_j$. Keep track of the subset giving the largest such sum that is less than or equal to W, and return that subset as the output of the algorithm. **b)** The food pack and the portable stove 43. **a)** The makespan is always at least as large as the load on the processor assigned to do the lengthiest job, which must be at least $\max_{j=1,2,\ldots,n} t_j$. Therefore the minimum makespan satisfies this inequality. **b)** The total amount of time the processors need to spend working on the jobs (the total load) is $\sum_{j=1}^{n} t_j$. Therefore the average load per processor is $\frac{1}{p}\sum_{j=1}^{n} t_j$. The maximum load cannot be any smaller than the average, so the minimum makespan is always at least this large. 45. Processor 1: jobs 1, 4; processor 2: job 2; processor 3: jobs 3, 5

CHAPTER 4

Section 4.1

1. **a)** Yes **b)** No **c)** Yes **d)** No 3. Suppose that $a \mid b$. Then there exists an integer k such that $ka = b$. Because $a(ck) = bc$ it follows that $a \mid bc$. 5. If $a \mid b$ and $b \mid a$, there are integers c and d such that $b = ac$ and $a = bd$. Hence, $a = acd$. Because $a \neq 0$ it follows that $cd = 1$. Thus either $c = d = 1$ or $c = d = -1$. Hence, either $a = b$ or $a = -b$. 7. Because $ac \mid bc$ there is an integer k such that $ack = bc$. Hence, $ak = b$, so $a \mid b$. 9. **a)** 2, 5 **b)** -11, 10 **c)** 34, 7 **d)** 77, 0 **e)** 0, 0 **f)** 0, 3 **g)** -1, 2 **h)** 4, 0 11. **a)** 7:00 **b)** 8:00 **c)** 10:00 13. **a)** 10 **b)** 8 **c)** 0 **d)** 9 **e)** 6 **f)** 11 15. If $a \textbf{ mod } m = b \textbf{ mod } m$, then a and b have the same remainder when divided by m. Hence, $a = q_1m + r$ and $b = q_2m + r$, where $0 \le r < m$. It follows that $a - b = (q_1 - q_2)m$, so $m \mid (a - b)$. It follows that $a \equiv b \pmod{m}$. 17. There is some b with $(b-1)k < n \le bk$. Hence, $(b-1)k \le n-1 < bk$. Divide by k to obtain $b - 1 < n/k \le b$ and $b - 1 \le (n-1)/k < b$. Hence, $\lceil n/k \rceil = b$ and $\lfloor (n-1)/k \rfloor = b - 1$. 19. $x \textbf{ mod } m$ if $x \textbf{ mod } m \le \lceil m/2 \rceil$ and $(x \textbf{ mod } m) - m$ if $x \textbf{ mod } m > \lceil m/2 \rceil$ 21. **a)** 1 **b)** 2 **c)** 3 **d)** 9 23. **a)** 1, 109 **b)** 40, 89 **c)** -31, 222 **d)** -21, 38259 25. **a)** -15 **b)** -7 **c)** 140 27. $-1, -26, -51, -76$, 24, 49, 74, 99 29. **a)** No **b)** No **c)** Yes **d)** No 31. **a)** 13 **a)** 6 33. **a)** 9 **b)** 4 **c)** 25 **d)** 0 35. Let $m = tn$. Because $a \equiv b \pmod{m}$ there exists an integer s such that $a = b + sm$. Hence, $a = b + (st)n$, so $a \equiv b \pmod{n}$. 37. **a)** Let $m = c = 2$, $a = 0$, and $b = 1$. Then $0 = ac \equiv bc = 2 \pmod{2}$, but $0 = a \not\equiv b = 1 \pmod{2}$. **b)** Let $m = 5$, $a = b = 3$, $c = 1$, and $d = 6$. Then $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$, but $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod{5}$. 39. By Exercise 38 the sum of two squares must be either $0 + 0 = 0$, $0 + 1 = 1$, or $1 + 1 = 2$, modulo 4, never 3, and therefore not of the form $4k + 3$. 41. Because $a \equiv b \pmod{m}$, there exists an integer s such that $a = b + sm$, so $a - b = sm$. Then $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$, $k \ge 2$, is also a multiple of m. It follows that $a^k \equiv b^k \pmod{m}$. 43. To prove closure, note that $a \cdot_m b = (a \cdot b) \textbf{ mod } m$, which by definition is an element of $\mathbf{Z}_m$. Multiplication is associative because $(a \cdot_m b) \cdot_m c$ and $a \cdot_m (b \cdot_m c)$ both equal $(a \cdot b \cdot c) \textbf{ mod } m$ and multiplication of integers is associative. Similarly, multiplication in $\mathbf{Z}_m$ is commutative because multiplication in $\mathbf{Z}$ is commutative, and 1 is the multiplicative identity for $\mathbf{Z}_m$ because 1 is the multiplicative identity for $\mathbf{Z}$. 45. $0 +_5 0 = 0$, $0 +_5 1 = 1$, $0 +_5 2 = 2$, $0 +_5 3 = 3$, $0 +_5 4 = 4$; $1 +_5 1 = 2$, $1 +_5 2 = 3$, $1 +_5 3 = 4$, $1 +_5 4 = 0$; $2 +_5 2 = 4$, $2 +_5 3 = 0$, $2 +_5 4 = 1$; $3 +_5 3 = 1$, $3 +_5 4 = 2$; $4 +_4 4 = 3$ and $0 \cdot_5 0 = 0$, $0 \cdot_5 1 = 0$, $0 \cdot_5 2 = 0$, $0 \cdot_5 3 = 0$, $0 \cdot_5 4 = 0$; $1 \cdot_5 1 = 1$, $1 \cdot_5 2 = 2$, $1 \cdot_5 3 = 3$, $1 \cdot_5 4 = 4$; $2 \cdot_5 2 = 4$, $2 \cdot_5 3 = 1$, $2 \cdot_5 4 = 3$; $3 \cdot_5 3 = 4$, $3 \cdot_5 4 = 2$; $4 \cdot_5 4 = 1$ 47. f is onto but not one-to-one (unless $d = 1$); g is neither.

Section 4.2

1. **a)** 1110 0111 **b)** 1 0001 1011 0100 **c)** 1 0111 11010110 1100 3. **a)** 31 **b)** 513 **c)** 341 **d)** 26,896 5. **a)** 1 0111 1010 **b)** 11 1000 0100 **c)** 1 0001 0011 **d)** 101 0000 1111 7. **a)** 1000 0000 1110 **b)** 1 0011 0101 1010 1011 **c)** 10101011 1011 1010 **d)** 1101 1110 1111 1010 11001110 1101 9. 1010 1011 1100 1101 1110 1111 11. $(\mathrm{B7B})_{16}$ 13. Adding up to three leading 0s if necessary, write the binary expansion as $(\ldots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 2^4b_{10} + 2^5b_{11} + 2^6b_{12} + 2^7b_{13} + 2^8b_{20} + 2^9b_{21} + 2^{10}b_{22} + 2^{11}b_{23} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13}) \cdot 2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23}) \cdot 2^8 + \cdots$. Now $(b_{i3}b_{i2}b_{i1}b_{i0})_2$ translates into the hexadecimal digit h_i. So our number is $h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots = h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots$, which is the hexadecimal expansion $(\ldots h_1h_1h_0)_{16}$. 15 Adding up to two leading 0s if necessary, write the binary expansion as $(\ldots b_{22}b_{21}b_{20}b_{12}b_{11}b_{10}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 2^3b_{10} + 2^4b_{11} + 2^5b_{12} + 2^6b_{20} + 2^7b_{21} + 2^8b_{22} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + (b_{10} + 2b_{11} + 4b_{12}) \cdot 2^3 + (b_{20} + 2b_{21} + 4b_{22}) \cdot 2^6 + \cdots$. Now $(b_{i2}b_{i1}b_{i0})_2$ translates into the octal digit h_i. So our number is $h_0 + h_1 \cdot 2^3 + h_2 \cdot 2^6 + \cdots = h_0 + h_1 \cdot 8 + h_2 \cdot 8^2 + \cdots$, which is the octal expansion $(\ldots h_1h_1h_0)_8$. 17. 1 1101 1100 1010 1101 0001, $(1273)_8$ 19. Convert the given octal numeral to binary, then convert from binary to hexadecimal using Example 7. 21. **a)** 1011 1110, 10 0001 0000 0001 **b)** 1 1010 1100, 1011 0000 0111 0011 **c)** 100 1001 1010, 101 0010 1001 0110 0000 **d)** 110 0000 0000, 1000 0000 0001 1111 1111 23. **a)** 1132, 144,305 **b)** 6273, 2,134,272 **c)** 2110, 1,107,667 **d)** 57,777, 237,326,216 25. 436 27. 27 29. The binary expansion of the integer is the unique such sum. 31. Let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_{10}$. Then $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0 \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod{3}$, because

$10^j \equiv 1 \pmod 3)$) for all nonnegative integers j. It follows that $3 \mid a$ if and only if 3 divides the sum of the decimal digits of a. 33. Let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$. Then $a = a_0 + 2a_1 + 2^2a_2 + \cdots + 2^{n-1}a_{n-1} \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pm a_{n-1} \pmod 3$. It follows that a is divisible by 3 if and only if the sum of the binary digits in the even-numbered positions minus the sum of the binary digits in the odd-numbered positions is divisible by 3. 35. **a)** -6 **b)** 13 **c)** -14 **d)** 0 37. The one's complement of the sum is found by adding the one's complements of the two integers except that a carry in the leading bit is used as a carry to the last bit of the sum. 39. If $m \geq 0$, then the leading bit a_{n-1} of the one's complement expansion of m is 0 and the formula reads $m = \sum_{i=0}^{n-2} a_i 2^i$. This is correct because the right-hand side is the binary expansion of m. When m is negative, the leading bit a_{n-1} of the one's complement expansion of m is 1. The remaining $n-1$ bits can be obtained by subtracting $-m$ from $111\ldots1$ (where there are $n-1$ 1s), because subtracting a bit from 1 is the same as complementing it. Hence, the bit string $a_{n-2}\ldots a_0$ is the binary expansion of $(2^{n-1}-1)-(-m)$. Solving the equation $(2^{n-1}-1)-(-m) = \sum_{i=0}^{n-2} a_i 2^i$ for m gives the desired equation because $a_{n-1} = 1$. 41. **a)** -7 **b)** 13 **c)** -15 **d)** -1 43. To obtain the two's complement representation of the sum of two integers, add their two's complement representations (as binary integers are added) and ignore any carry out of the leftmost column. However, the answer is invalid if an overflow has occurred. This happens when the leftmost digits in the two's complement representation of the two terms agree and the leftmost digit of the answer differs. 45. If $m \geq 0$, then the leading bit a_{n-1} is 0 and the formula reads $m = \sum_{i=0}^{n-2} a_i 2^i$. This is correct because the right-hand side is the binary expansion of m. If $m < 0$, its two's complement expansion has 1 as its leading bit and the remaining $n-1$ bits are the binary expansion of $2^{n-1}-(-m)$. This means that $(2^{n-1})-(-m) = \sum_{i=0}^{n-2} a_i 2^i$. Solving for m gives the desired equation because $a_{n-1} = 1$. 47. $4n$

49.
```
procedure Cantor(x: positive integer)
  n := 1; f := 1
  while (n + 1) · f ≤ x
    n := n + 1
    f := f · n
  y := x
  while n > 0
    a_n := ⌊y/f⌋
    y := y − a_n · f
    f := f/n
    n := n − 1
  {x = a_n n! + a_{n−1}(n − 1)! + ··· + a_1 1!}
```

51. First step: $c = 0$, $d = 0$, $s_0 = 1$; second step: $c = 0$, $d = 1$, $s_1 = 0$; third step: $c = 1$, $d = 1$, $s_2 = 0$; fourth step: $c = 1$, $d = 1$, $s_3 = 0$; fifth step: $c = 1$, $d = 1$, $s_4 = 1$; sixth step: $c = 1$, $s_5 = 1$

53.
```
procedure subtract(a, b: positive integers, a > b,
    a = (a_{n−1}a_{n−2} ... a_1a_0)_2,
    b = (b_{n−1}b_{n−2} ... b_1b_0)_2)
  B := 0 {B is the borrow}
  for j := 0 to n − 1
    if a_j ≥ b_j + B then
      s_j := a_j − b_j − B
      B := 0
    else
      s_j := a_j + 2 − b_j − B
      B := 1
  {(s_{n−1}s_{n−2} ... s_1s_0)_2 is the difference}
```

55.
```
procedure compare(a, b: positive integers,
    a = (a_n a_{n−1} ... a_1a_0)_2,
    b = (b_n b_{n−1} ... b_1b_0)_2)
  k := n
  while a_k = b_k and k > 0
    k := k − 1
  if a_k = b_k then print "a equals b"
  if a_k > b_k then print "a is greater than b"
  if a_k < b_k then print "a is less than b"
```

57. $O(\log n)$ 59. The only time-consuming part of the algorithm is the **while** loop, which is iterated q times. The work done inside is a subtraction of integers no bigger than a, which has $\log a$ bits. The result now follows from Example 9.

Section 4.3

1. 29, 71, 97 prime; 21, 111, 143 not prime 3. **a)** $2^3 \cdot 11$ **b)** $2 \cdot 3^2 \cdot 7$ **c)** 3^6 **d)** $7 \cdot 11 \cdot 13$ **e)** $11 \cdot 101$ **f)** $2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$ 5. $2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

7.
```
procedure primetester(n : integer greater than 1)
  isprime := true
  d := 2
  while isprime and d ≤ √n
    if n mod d = 0 then isprime := false
    else d := d + 1
  return isprime
```

9. Write $n = rs$, where $r > 1$ and $s > 1$. Then $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + (2^r)^{s-3} + \cdots + 1)$. The first factor is at least $2^2 - 1 = 3$ and the second factor is at least $2^2 + 1 = 5$. This provides a factoring of $2^n - 1$ into two factors greater than 1, so $2^n - 1$ is composite. 11. Suppose that $\log_2 3 = a/b$ where $a, b \in \mathbf{Z}^+$ and $b \neq 0$. Then $2^{a/b} = 3$, so $2^a = 3^b$. This violates the fundamental theorem of arithmetic. Hence, $\log_2 3$ is irrational. 13. 3, 5, and 7 are primes of the desired form. 15. 1, 7, 11, 13, 17, 19, 23, 29 17. **a)** Yes **b)** No **c)** Yes **d)** Yes 19. Suppose that n is not prime, so that $n = ab$, where a and b are integers greater than 1. Because $a > 1$, by the identity in the hint, $2^a - 1$ is a factor of $2^n - 1$ that is greater than 1, and the second

factor in this identity is also greater than 1. Hence, $2^n - 1$ is not prime. **21. a)** 2 **b)** 4 **c)** 12 **23.** $\phi(p^k) = p^k - p^{k-1}$ **25. a)** $3^5 \cdot 5^3$ **b)** 1 **c)** 23^{17} **d)** $41 \cdot 43 \cdot 53$ **e)** 1 **f)** 1111 **27. a)** $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$ **b)** $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$ **c)** 23^{31} **d)** $41 \cdot 43 \cdot 53$ **e)** $2^{12}3^{13}5^{17}7^{21}$ **f)** Undefined **29.** gcd (92928, 123552) = 1056; lcm(92928, 123552) = 10,872,576; both products are 11,481,440,256. **31.** Because $\min(x, y) + \max(x, y) = x + y$, the exponent of p_i in the prime factorization of $\gcd(a, b) \cdot \operatorname{lcm}(a, b)$ is the sum of the exponents of p_i in the prime factorizations of a and b. **33. a)** 6 **b)** 3 **c)** 11 **d)** 3 **e)** 40 **f)** 12 **35.** 9 **37.** By Exercise 36 it follows that $\gcd(2^b - 1, (2^a - 1) \textbf{ mod } (2^b - 1)) = \gcd(2^b - 1, 2^{a \textbf{ mod } b} - 1)$. Because the exponents involved in the calculation are b and a **mod** b, the same as the quantities involved in computing $\gcd(a, b)$, the steps used by the Euclidean algorithm to compute $\gcd(2^a - 1, 2^b - 1)$ run in parallel to those used to compute $\gcd(a, b)$ and show that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. **39. a)** $1 = (-1) \cdot 10 + 1 \cdot 11$ **b)** $1 = 21 \cdot 21 + (-10) \cdot 44$ **c)** $12 = (-1) \cdot 36 + 48$ **d)** $1 = 13 \cdot 55 + (-21) \cdot 34$ **e)** $3 = 11 \cdot 213 + (-20) \cdot 117$ **f)** $223 = 1 \cdot 0 + 1 \cdot 223$ **g)** $1 = 37 \cdot 2347 + (-706) \cdot 123$ **h)** $2 = 1128 \cdot 3454 + (-835) \cdot 4666$ **i)** $1 = 2468 \cdot 9999 + (-2221) \cdot 11111$ **41.** $(-3) \cdot 26 + 1 \cdot 91 = 13$ **43.** $34 \cdot 144 + (-55) \cdot 89 = 1$

45.
```
procedure extended Euclidean(a, b: positive integers)
  x := a
  y := b
  oldolds := 1
  olds := 0
  oldoldt := 0
  oldt := 1
  while y ≠ 0
    q := x div y
    r := x mod y
    x := y
    y := r
    s := oldolds − q · olds
    t := oldoldt − q · oldt
    oldolds := olds
    oldoldt := oldt
    olds := s
    oldt := t
  {gcd(a, b) is x, and (oldolds)a + (oldoldt)b = x}
```

47. a) $a_n = 1$ if n is prime and $a_n = 0$ otherwise. **b)** a_n is the smallest prime factor of n with $a_1 = 1$. **c)** a_n is the number of positive divisors of n. **d)** $a_n = 1$ if n has no divisors that are perfect squares greater than 1 and $a_n = 0$ otherwise. **e)** a_n is the largest prime less than or equal to n. **f)** a_n is the product of the first $n - 1$ primes. **49.** Because every second integer is divisible by 2, the product is divisible by 2. Because every third integer is divisible by 3, the product is divisible by 3. Therefore the product has both 2 and 3 in its prime factorization and is therefore divisible by $3 \cdot 2 = 6$. **51.** $n = 1601$ is a counterexample. **53** Setting $k = a + b + 1$ will produce the composite number $a(a + b + 1) + b = a^2 + ab + a + b = (a + 1)(a + b)$. **55.** Suppose that there are only finitely many primes of the form $4k + 3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on. Let $Q = 4q_1q_2 \cdots q_n - 1$. Note that Q is of the form $4k + 3$ (where $k = q_1q_2 \cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed. If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Because all odd primes are either of the form $4k + 1$ or of the form $4k + 3$, and the product of primes of the form $4k + 1$ is also of this form (because $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$), there must be a factor of Q of the form $4k + 3$ different from the primes we listed. **57.** Given a positive integer x, we show that there is exactly one positive rational number m/n (in lowest terms) such that $K(m/n) = x$. From the prime factorization of x, read off the m and n such that $K(m/n) = x$. The primes that occur to even powers are the primes that occur in the prime factorization of m, with the exponents being half the corresponding exponents in x; and the primes that occur to odd powers are the primes that occur in the prime factorization of n, with the exponents being half of one more than the exponents in x.

Section 4.4

1. $15 \cdot 7 = 105 \equiv 1 \pmod{26}$ **3.** 7 **5. a)** 7 **b)** 52 **c)** 34 **d)** 73 **7.** Suppose that b and c are both inverses of a modulo m. Then $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Hence, $ba \equiv ca \pmod{m}$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \pmod{m}$. **9.** 8 **11. a)** 67 **b)** 88 **c)** 146 **13.** 3 and 6 **15.** Let $m' = m/\gcd(c, m)$. Because all the common factors of m and c are divided out of m to obtain m', it follows that m' and c are relatively prime. Because m divides $ac - bc = (a - b)c$, it follows that m' divides $(a - b)c$. By Lemma 3 in Section 4.3, we see that m' divides $a - b$, so $a \equiv b \pmod{m'}$. **17.** Suppose that $x^2 \equiv 1 \pmod{p}$. Then p divides $x^2 - 1 = (x + 1)(x - 1)$. By Lemma 2 it follows that $p \mid x + 1$ or $p \mid x - 1$, so $x \equiv -1 \pmod{p}$ or $x \equiv 1 \pmod{p}$. **19. a)** Suppose that $ia \equiv ja \pmod{p}$, where $1 \leq i < j < p$. Then p divides $ja - ia = a(j - i)$. By Theorem 1, because a is not divisible by p, p divides $j - i$, which is impossible because $j - i$ is a positive integer less than p. **b)** By part (a), because no two of $a, 2a, \ldots, (p - 1)a$ are congruent modulo p, each must be congruent to a different number from 1 to $p - 1$. It follows that $a \cdot 2a \cdot 3a \cdot \cdots \cdot (p - 1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p - 1) \pmod{p}$. It follows that $(p - 1)! \cdot a^{p-1} \equiv p - 1 \pmod{p}$. **c)** By Wilson's theorem and part (b), if p does not divide a, it follows that $(-1) \cdot a^{p-1} \equiv -1 \pmod{p}$. Hence, $a^{p-1} \equiv 1 \pmod{p}$. **d)** If $p \mid a$, then $p \mid a^p$. Hence, $a^p \equiv a \equiv 0 \pmod{p}$. If p does not divide a, then $a^{p-1} \equiv a \pmod{p}$, by part (c). Multiplying both sides of this congruence by a gives $a^p \equiv a \pmod{p}$. **21.** All integers of the form $323 + 330k$, where k is an integer **23.** All integers of the form $53 + 60k$, where k is an integer

25.

```
procedure chinese(m1, m2, ..., mn : relatively
        prime positive integers ; a1, a2, ..., an : integers)
m := 1
for k := 1 to n
    m := m · mk
for k := 1 to n
    Mk := m/mk
    yk := Mk^(-1) mod mk
x := 0
for k := 1 to n
    x := x + ak Mk yk
while x ≥ m
    x := x − m
return x {the smallest solution to the system
        {x ≡ ak (mod mk), k = 1, 2, ..., n }}
```

27. All integers of the form $16 + 252k$, where k is an integer **29.** Suppose that p is a prime appearing in the prime factorization of $m_1 m_2 \cdots m_n$. Because the m_is are relatively prime, p is a factor of exactly one of the m_is, say m_j. Because m_j divides $a - b$, it follows that $a - b$ has the factor p in its prime factorization to a power at least as large as the power to which it appears in the prime factorization of m_j. It follows that $m_1 m_2 \cdots m_n$ divides $a - b$, so $a \equiv b \pmod{m_1 m_2 \cdots m_n}$. **31.** $x \equiv 1 \pmod{6}$ **33.** 7 **35.** $a^{p-2} \cdot a = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$ **37.** **a)** By Fermat's little theorem, we have $2^{10} \equiv 1 \pmod{11}$. Hence, $2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{11}$. **b)** Because $32 \equiv 1 \pmod{31}$, it follows that $2^{340} = (2^5)^{68} = 32^{68} \equiv 1^{68} = 1 \pmod{31}$. **c)** Because 11 and 31 are relatively prime, and $11 \cdot 31 = 341$, it follows by parts (a) and (b) and Exercise 29 that $2^{340} \equiv 1 \pmod{341}$. **39.** **a)** 3, 4, 8 **b)** 983 **41.** Suppose that q is an odd prime with $q \mid 2^p - 1$. By Fermat's little theorem, $q \mid 2^{q-1} - 1$. From Exercise 37 in Section 4.3, $\gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p,q-1)} - 1$. Because q is a common divisor of $2^p - 1$ and $2^{q-1} - 1$, $\gcd(2^p - 1, 2^{q-1} - 1) > 1$. Hence, $\gcd(p, q-1) = p$, because the only other possibility, namely, $\gcd(p, q-1) = 1$, gives us $\gcd(2^p - 1, 2^{q-1} - 1) = 1$. Hence, $p \mid q - 1$, and therefore there is a positive integer m such that $q - 1 = mp$. Because q is odd, m must be even, say, $m = 2k$, and so every prime divisor of $2^p - 1$ is of the form $2kp + 1$. Furthermore, the product of numbers of this form is also of this form. Therefore, all divisors of $2^p - 1$ are of this form. **43.** M_{11} is not prime; M_{17} is prime. **45.** First, $2047 = 23 \cdot 89$ is composite. Write $2047 - 1 = 2046 = 2 \cdot 1023$, so $s = 1$ and $t = 1023$ in the definition. Then $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1^{93} = 1 \pmod{2047}$, as desired. **47.** We must show that $b^{2820} \equiv 1 \pmod{2821}$ for all b relatively prime to 2821. Note that $2821 = 7 \cdot 13 \cdot 31$, and if $\gcd(b, 2821) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 31) = 1$. Using Fermat's little theorem we find that $b^6 \equiv 1 \pmod{7}$, $b^{12} \equiv 1 \pmod{13}$, and $b^{30} \equiv 1 \pmod{31}$. It follows that $b^{2820} \equiv (b^6)^{470} \equiv 1 \pmod{7}$, $b^{2820} \equiv (b^{12})^{235} \equiv 1 \pmod{13}$, and $b^{2820} \equiv (b^{30})^{94} \equiv 1 \pmod{31}$. By Exercise 29 (or the Chinese remainder theorem) it follows that $b^{2820} \equiv 1 \pmod{2821}$, as desired. **49.** **a)** If we multiply out this expression, we get $n = 1296m^3 + 396m^2 + 36m + 1$. Clearly $6m \mid n - 1$, $12m \mid n - 1$, and $18m \mid n - 1$. Therefore, the conditions of Exercise 48 are met, and we conclude that n is a Carmichael number. **b)** Letting $m = 51$ gives $n = 172{,}947{,}529$. **51.** $0 = (0, 0)$, $1 = (1, 1)$, $2 = (2, 2)$, $3 = (0, 3)$, $4 = (1, 4)$, $5 = (2, 0)$, $6 = (0, 1)$, $7 = (1, 2)$, $8 = (2, 3)$, $9 = (0, 4)$, $10 = (1, 0)$, $11 = (2, 1)$, $12 = (0, 2)$, $13 = (1, 3)$, $14 = (2, 4)$ **53.** We have $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, and $m_4 = 95$, so $m = 99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$. We find that $M_1 = m/m_1 = 903{,}070$, $M_2 = m/m_2 = 912{,}285$, $M_3 = m/m_3 = 921{,}690$, and $M_4 = m/m_4 = 941{,}094$. Using the Euclidean algorithm, we compute that $y_1 = 37$, $y_2 = 33$, $y_3 = 24$, and $y_4 = 4$ are inverses of M_k modulo m_k for $k = 1, 2, 3, 4$, respectively. It follows that the solution is $65 \cdot 903{,}070 \cdot 37 + 2 \cdot 912{,}285 \cdot 33 + 51 \cdot 921{,}690 \cdot 24 + 10 \cdot 941{,}094 \cdot 4 = 3{,}397{,}886{,}480 \equiv 537{,}140 \pmod{89{,}403{,}930}$. **55.** $\log_2 5 = 16$, $\log_2 6 = 14$ **57.** $\log_3 1 = 0$, $\log_3 2 = 14$, $\log_3 3 = 1$, $\log_3 4 = 12$, $\log_3 5 = 5$, $\log_3 6 = 15$, $\log_3 7 = 11$, $\log_3 8 = 10$, $\log_3 9 = 2$, $\log_3 10 = 3$, $\log_3 11 = 7$, $\log_3 12 = 13$, $\log_3 13 = 4$, $\log_3 14 = 9$, $\log_3 15 = 6$, $\log_3 16 = 8$ **59.** Assume that s is a solution of $x^2 \equiv a \pmod{p}$. Then because $(-s)^2 = s^2$, $-s$ is also a solution. Furthermore, $s \not\equiv -s \pmod{p}$. Otherwise, $p \mid 2s$, which implies that $p \mid s$, and this implies, using the original assumption, that $p \mid a$, which is a contradiction. Furthermore, if s and t are incongruent solutions modulo p, then because $s^2 \equiv t^2 \pmod{p}$, $p \mid s^2 - t^2$. This implies that $p \mid (s+t)(s-t)$, and by Lemma 3 in Section 4.3, $p \mid s - t$ or $p \mid s + t$, so $s \equiv t \pmod{p}$ or $s \equiv -t \pmod{p}$. Hence, there are at most two solutions. **61.** The value of $\left(\frac{a}{p}\right)$ depends only on whether a is a quadratic residue modulo p, that is, whether $x^2 \equiv a \pmod{p}$ has a solution. Because this depends only on the equivalence class of a modulo p, it follows that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod{p}$. **63.** By Exercise 62, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod{p}$. **65.** $x \equiv 8, 13, 22, \text{ or } 27 \pmod{35}$ **67.** Compute r^e **mod** p for $e = 0, 1, 2, \ldots, p-2$ until we get the answer a. Worst case and average case time complexity are $O(p \log p)$.

Section 4.5

1. 91, 57, 21, 5 **3.** **a)** 7, 19, 7, 7, 18, 0 **b)** Take the next available space **mod** 31. **5.** 1, 5, 4, 1, 5, 4, 1, 5, 4, ... **7.** 2, 6, 7, 10, 8, 2, 6, 7, 10, 8, ... **9.** 2357, 5554, 8469, 7239, 4031, 2489, 1951, 8064 **11.** 2, 1, 1, 1, ... **13.** Only string (d) **15.** 4 **17.** Correctly, of course **19.** **a)** Not valid **b)** Valid **c)** Valid **d)** Not valid **21.** **a)** No **b)** 5 **c)** 7 **d)** 8 **23.** Transposition errors involving the last digit **25.** **a)** Yes **b)** No **c)** Yes **d)** No **27.** Transposition errors will be detected if and only if the transposed digits are an odd number of positions apart and do not differ by 5. **29.** **a)** Valid **b)** Not valid **c)** Valid **d)** Valid **31.** Yes, as long as the two digits do not differ by 7 **33.** **a)** Not valid **b)** Valid **c)** Valid **d)** Not valid **35.** The given congruence is equivalent to $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 + 10d_8 \equiv 0 \pmod{11}$. Transposing adjacent digits x and y (with x on the left) causes the left-hand side to increase by $x - y$. Because $x \not\equiv y \pmod{11}$, the congruence will no longer hold. Therefore errors of this type are always detected.

Section 4.6

1. **a)** GR QRW SDVV JR **b)** QB ABG CNFF TB **c)** QX UXM AHJJ ZX 3. **a)** KOHQV MCIF GHSD **b)** RVBXP TJPZ NBZX **c)** DBYNE PHRM FYZA 5. **a)** SURRENDER NOW **b)** BE MY FRIEND **c)** TIME FOR FUN 7. TO SLEEP PERCHANCE TO DREAM 9. ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC 11. $p = 7c + 13$ **mod** 26 13. $a = 18$, $b = 5$ 15. BEWARE OF MARTIANS 17. Presumably something like an affine cipher 19. HURRICANE 21. The length of the key may well be the greatest common divisor of the distances between the starts of the repeated string (or a factor of the gcd). 23. Suppose we know both $n = pq$ and $(p-1)(q-1)$. To find p and q, first note that $(p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. From this we can find $s = p + q$. Because $q = s - p$, we have $n = p(s - p)$. Hence, $p^2 - ps + n = 0$. We now can use the quadratic formula to find p. Once we have found p, we can find q because $q = n/p$. 25. 2545 2757 1211 27. SILVER 29. Alice sends 5^8 **mod** $23 = 16$ to Bob. Bob sends 5^5 **mod** $23 = 20$ to Alice. Alice computes 20^8 **mod** $23 = 6$ and Bob computes 16^5 **mod** $23 = 6$. The shared key is 6. 31. 2186 2087 1279 1251 0326 0816 1948 33. Alice can decrypt the first part of Cathy's message to learn the key, and Bob can decrypt the second part of Cathy's message, which Alice forwarded to him, to learn the key. No one else besides Cathy can learn the key, because all of these communications use secure private keys.

Supplementary Exercises

1. The actual number of miles driven is $46518 + 100000k$ for some natural number k. 3. 5, 22, −12, −29 5. Because $ac \equiv bc \pmod{m}$ there is an integer k such that $ac = bc + km$. Hence, $a - b = km/c$. Because $a - b$ is an integer, $c \mid km$. Letting $d = \gcd(m, c)$, write $c = de$. Because no factor of e divides m/d, it follows that $d \mid m$ and $e \mid k$. Thus $a - b = (k/e)(m/d)$, where $k/e \in \mathbf{Z}$ and $m/d \in \mathbf{Z}$. Therefore $a \equiv b \pmod{m/d}$. 7. Proof of the contrapositive: If n is odd, then $n = 2k + 1$ for some integer k. Therefore $n^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2 \equiv 2 \pmod{4}$. But perfect squares of even numbers are congruent to 0 modulo 4 (because $(2m)^2 = 4m^2$), and perfect squares of odd numbers are congruent to 1 or 3 modulo 4, so $n^2 + 1$ is not a perfect square. 9. n is divisible by 8 if and only if the binary expansion of n ends with 000. 11. We assume that someone has chosen a positive integer less than 2^n, which we are to guess. We ask the person to write the number in binary, using leading 0s if necessary to make it n bits long. We then ask "Is the first bit a 1?", "Is the second bit a 1?", "Is the third bit a 1?", and so on. After we know the answers to these n questions, we will know the number, because we will know its binary expansion. 13. $(a_n a_{n-1} \ldots a_1 a_0)_{10} = \sum_{k=0}^{n} 10^k a_k \equiv \sum_{k=0}^{n} a_k \pmod{9}$ because $10^k \equiv 1 \pmod{9}$ for every nonnegative integer k. 15. Because for all $k \le n$, when Q_n is divided by k the remainder will be 1, it follows that no prime number less than or equal to n is a factor of Q_n. Thus by the fundamental theorem of arithmetic, Q_n must have a prime factor greater than n. 17. Take $a = 10$ and $b = 1$ in Dirichlet's theorem. 19. Every number greater than 11 can be written as either $8+2n$ or $9+2n$ for some $n \ge 2$. 21. Assume that every even integer greater than 2 is the sum of two primes, and let n be an integer greater than 5. If n is odd, write $n = 3 + (n - 3)$ and decompose $n - 3 = p + q$ into the sum of two primes; if n is even, then write $n = 2 + (n - 2)$ and decompose $n - 2 = p + q$ into the sum of two primes. For the converse, assume that every integer greater than 5 is the sum of three primes, and let n be an even integer greater than 2. Write $n + 2$ as the sum of three primes, one of which is necessarily 2, so $n + 2 = 2 + p + q$, whence $n = p + q$. 23. Recall that a nonconstant polynomial can take on the same value only a finite number of times. Thus f can take on the values 0 and ± 1 only finitely many times, so if there is not some y such that $f(y)$ is composite, then there must be some x_0 such that $\pm f(x_0)$ is prime, say p. Look at $f(x_0 + kp)$. When we plug $x_0 + kp$ in for x in the polynomial and multiply it out, every term will contain a factor of p except for the terms that form $f(x_0)$. Therefore $f(x_0+kp) = f(x_0)+mp = (m\pm 1)p$ for some integer m. As k varies, this value can be 0, p, or $-p$ only finitely many times; therefore it must be a composite number for some values of k. 25. 1 27. 1 29. If not, then suppose that $q_1, q_2, \ldots, q_n$ are all the primes of the form $6k + 5$. Let $Q = 6q_1 q_2 \cdots q_n - 1$. Note that Q is of the form $6k + 5$, where $k = q_1 q_2 \cdots q_n - 1$. Let $Q = p_1 p_2 \cdots p_t$ be the prime factorization of Q. No p_i is 2, 3, or any q_j, because the remainder when Q is divided by 2 is 1, by 3 is 2, and by q_j is $q_j - 1$. All odd primes other than 3 are of the form $6k + 1$ or $6k + 5$, and the product of primes of the form $6k + 1$ is also of this form. Therefore at least one of the p_i's must be of the form $6k+5$, a contradiction. 31. The product of numbers of the form $4k + 1$ is of the form $4k + 1$, but numbers of this form might have numbers not of this form as their only prime factors. For example, $49 = 4 \cdot 12 + 1$, but the prime factorization of 49 is $7 \cdot 7 = (4 \cdot 1 + 3)(4 \cdot 1 + 3)$. 33. **a)** Not mutually relatively prime **b)** Mutually relatively prime **c)** Mutually relatively prime **d)** Mutually relatively prime 35 1 37. $x \equiv 28 \pmod{30}$ 39. By the Chinese remainder theorem, it suffices to show that $n^9 - n \equiv 0 \pmod{2}$, $n^9 - n \equiv 0 \pmod{3}$, and $n^9 - n \equiv 0 \pmod{5}$. Each in turn follows from applying Fermat's little theorem. 41. By Fermat's little theorem, $p^{q-1} \equiv 1 \pmod{q}$ and clearly $q^{p-1} \equiv 0 \pmod{q}$. Therefore $p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod{q}$. Similarly, $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$. It follows from the Chinese remainder theorem that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. 43. If a_i is changed from x to y, then the change in the left-hand side of the congruence is either $y - x$ or $3(y - x)$, modulo 10, neither of which can be 0 because 1 and

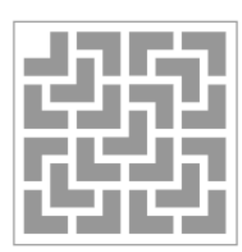
3 are relatively prime to 10. Therefore the sum can no longer be 0 modulo 10. **45.** Working modulo 10, solve for d_9. The check digit for 11100002 is 5. **47.** PLEASE SEND MONEY **49.** **a)** QAL HUVEM AT WVESGB **b)** QXB EVZZL ZEVZZRFS

CHAPTER 5

Section 5.1

1. Let $P(n)$ be the statement that the train stops at station n. *Basis step:* We are told that $P(1)$ is true. *Inductive step:* We are told that $P(n)$ implies $P(n+1)$ for each $n \geq 1$. Therefore by the principle of mathematical induction, $P(n)$ is true for all positive integers n. **3.** **a)** $1^2 = 1 \cdot 2 \cdot 3/6$ **b)** Both sides of $P(1)$ shown in part (a) equal 1. **c)** $1^2 + 2^2 + \cdots + k^2 = k(k+1)(2k+1)/6$ **d)** For each $k \geq 1$ that $P(k)$ implies $P(k+1)$; in other words, that assuming the inductive hypothesis [see part (c)] we can show $1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$ **e)** $(1^2 + 2^2 + \cdots + k^2) + (k+1)^2 = [k(k+1)(2k+1)/6] + (k+1)^2 = [(k+1)/6][k(2k+1) + 6(k+1)] = [(k+1)/6](2k^2 + 7k + 6) = [(k+1)/6](k+2)(2k+3) = (k+1)(k+2)(2k+3)/6$ **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. **5.** Let $P(n)$ be "$1^2 + 3^2 + \cdots + (2n+1)^2 = (n+1)(2n+1)(2n+3)/3$." *Basis step:* $P(0)$ is true because $1^2 = 1 = (0+1)(2 \cdot 0+1)(2 \cdot 0+3)/3$. *Inductive step:* Assume that $P(k)$ is true. Then $1^2 + 3^2 + \cdots + (2k+1)^2 + [2(k+1)+1]^2 = (k+1)(2k+1)(2k+3)/3 + (2k+3)^2 = (2k+3)[(k+1)(2k+1)/3 + (2k+3)] = (2k+3)(2k^2+9k+10)/3 = (2k+3)(2k+5)(k+2)/3 = [(k+1)+1][2(k+1)+1][2(k+1)+3]/3$. **7.** Let $P(n)$ be "$\sum_{j=0}^{n} 3 \cdot 5^j = 3(5^{n+1} - 1)/4$." *Basis step:* $P(0)$ is true because $\sum_{j=0}^{0} 3 \cdot 5^j = 3 = 3(5^1 - 1)/4$. *Inductive step:* Assume that $\sum_{j=0}^{k} 3 \cdot 5^j = 3(5^{k+1} - 1)/4$. Then $\sum_{j=0}^{k+1} 3 \cdot 5^j = (\sum_{j=0}^{k} 3 \cdot 5^j) + 3 \cdot 5^{k+1} = 3(5^{k+1} - 1)/4 + 3 \cdot 5^{k+1} = 3(5^{k+1} + 4 \cdot 5^{k+1} - 1)/4 = 3(5^{k+2} - 1)/4$. **9.** **a)** $2+4+6+\cdots+2n = n(n+1)$ **b)** *Basis step:* $2 = 1 \cdot (1+1)$ is true. *Inductive step:* Assume that $2 + 4 + 6 + \cdots + 2k = k(k+1)$. Then $(2 + 4 + 6 + \cdots + 2k) + 2(k+1) = k(k+1) + 2(k+1) = (k+1)(k+2)$. **11.** **a)** $\sum_{j=1}^{n} 1/2^j = (2^n - 1)/2^n$ **b)** *Basis step:* $P(1)$ is true because $\frac{1}{2} = (2^1 - 1)/2^1$. *Inductive step:* Assume that $\sum_{j=1}^{k} 1/2^j = (2^k - 1)/2^k$. Then $\sum_{j=1}^{k+1} \frac{1}{2^j} = (\sum_{j=1}^{k} \frac{1}{2^j}) + \frac{1}{2^{k+1}} = \frac{2^k - 1}{2^k} + \frac{1}{2^{k+1}} = \frac{2^{k+1} - 2 + 1}{2^{k+1}} = \frac{2^{k+1} - 1}{2^{k+1}}$. **13.** Let $P(n)$ be "$1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} n(n+1)/2$." *Basis step:* $P(1)$ is true because $1^2 = 1 = (-1)^0 1^2$. *Inductive step:* Assume that $P(k)$ is true. Then $1^2 - 2^2 + 3^2 - \cdots + (-1)^{k-1} k^2 + (-1)^k (k+1)^2 = (-1)^{k-1} k(k+1)/2 + (-1)^k (k+1)^2 = (-1)^k (k+1)[-k/2 + (k+1)] = (-1)^k (k+1)[(k/2) + 1] = (-1)^k (k+1)(k+2)/2$. **15.** Let $P(n)$ be "$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3$." *Basis step:* $P(1)$ is true because $1 \cdot 2 = 2 = 1(1+1)(1+2)/3$. *Inductive step:* Assume that $P(k)$ is true. Then $1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) + (k+1)(k+2) = [k(k+1)(k+2)/3] + (k+1)(k+2) = (k+1)(k+2)[(k/3) + 1] = (k+1)(k+2)(k+3)/3$. **17.** Let $P(n)$ be the statement that $1^4 + 2^4 + 3^4 + \cdots + n^4 = n(n+1)(2n+1)(3n^2 + 3n - 1)/30$. $P(1)$ is true because $1 \cdot 2 \cdot 3 \cdot 5/30 = 1$. Assume that $P(k)$ is true. Then $(1^4 + 2^4 + 3^4 + \cdots + k^4) + (k+1)^4 = k(k+1)(2k+1)(3k^2 + 3k - 1)/30 + (k+1)^4 = [(k+1)/30][k(2k+1)(3k^2 + 3k - 1) + 30(k+1)^3] = [(k+1)/30](6k^4 + 39k^3 + 91k^2 + 89k + 30) = [(k+1)/30](k+2)(2k+3)[3(k+1)^2 + 3(k+1) - 1]$. This demonstrates that $P(k+1)$ is true. **19.** **a)** $1 + \frac{1}{4} < 2 - \frac{1}{2}$ **b)** This is true because $5/4$ is less than $6/4$. **c)** $1 + \frac{1}{4} + \cdots + \frac{1}{k^2} < 2 - \frac{1}{k}$ **d)** 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 show $1 + \frac{1}{4} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}$ **e)** $1 + \frac{1}{4} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k} + \frac{1}{(k+1)^2} = 2 - \left[\frac{1}{k} - \frac{1}{(k+1)^2}\right] = 2 - \left[\frac{k^2 + 2k + 1 - k}{k(k+1)^2}\right] = 2 - \frac{k^2 + k}{k(k+1)^2} - \frac{1}{k(k+1)^2} = 2 - \frac{1}{k+1} - \frac{1}{k(k+1)^2} < 2 - \frac{1}{k+1}$ **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 integer n greater than 1. **21.** Let $P(n)$ be "$2^n > n^2$." *Basis step:* $P(5)$ is true because $2^5 = 32 > 25 = 5^2$. *Inductive step:* Assume that $P(k)$ is true, that is, $2^k > k^2$. Then $2^{k+1} = 2 \cdot 2^k > k^2 + k^2 > k^2 + 4k \geq k^2 + 2k + 1 = (k+1)^2$ because $k > 4$. **23.** By inspection we find that the inequality $2n + 3 \leq 2^n$ does not hold for $n = 0, 1, 2, 3$. Let $P(n)$ be the proposition that this inequality holds for the positive integer n. $P(4)$, the basis case, is true because $2 \cdot 4 + 3 = 11 \leq 16 = 2^4$. For the inductive step assume that $P(k)$ is true. Then, by the inductive hypothesis, $2(k+1)+3 = (2k+3)+2 < 2^k + 2$. But because $k \geq 1$, $2^k + 2 \leq 2^k + 2^k = 2^{k+1}$. This shows that $P(k+1)$ is true. **25.** Let $P(n)$ be "$1 + nh \leq (1+h)^n$, $h > -1$." *Basis step:* $P(0)$ is true because $1 + 0 \cdot h = 1 \leq 1 = (1+h)^0$. *Inductive step:* Assume $1 + kh \leq (1+h)^k$. Then because $(1+h) > 0$, $(1+h)^{k+1} = (1+h)(1+h)^k \geq (1+h)(1+kh) = 1 + (k+1)h + kh^2 \geq 1 + (k+1)h$. **27.** Let $P(n)$ be "$1/\sqrt{1} + 1/\sqrt{2} + 1/\sqrt{3} + \cdots + 1/\sqrt{n} > 2\left(\sqrt{n+1} - 1\right)$." *Basis step:* $P(1)$ is true because $1 > 2\left(\sqrt{2} - 1\right)$. *Inductive step:* Assume that $P(k)$ is true. Then $1 + 1/\sqrt{2} + \cdots + 1/\sqrt{k} + 1/\sqrt{k+1} > 2\left(\sqrt{k+1} - 1\right) + 1/\sqrt{k+1}$. If we show that $2\left(\sqrt{k+1} - 1\right) + 1/\sqrt{k+1} > 2\left(\sqrt{k+2} - 1\right)$, it follows that $P(k+1)$ is true. This inequality is equivalent to $2\left(\sqrt{k+2} - \sqrt{k+1}\right) < 1/\sqrt{k+1}$, which is equivalent to $2\left(\sqrt{k+2} - \sqrt{k+1}\right)\left(\sqrt{k+2} + \sqrt{k+1}\right) < \sqrt{k+1}/\sqrt{k+1} + \sqrt{k+2}/\sqrt{k+1}$. This is equivalent to $2 < 1 + \sqrt{k+2}/\sqrt{k+1}$, which is clearly true. **29.** Let $P(n)$ be "$H_{2^n} \leq 1 + n$." *Basis step:* $P(0)$ is true because $H_{2^0} = H_1 = 1 \leq 1 + 0$. *Inductive step:* Assume that $H_{2^k} \leq 1 + k$. Then $H_{2^{k+1}} = H_{2^k} + \sum_{j=2^k+1}^{2^{k+1}} \frac{1}{j} \leq 1 + k + 2^k \left(\frac{1}{2^{k+1}}\right) < 1 + k + 1 = 1 + (k+1)$. **31.** *Basis step:* $1^2 + 1 = 2$ is divisible by 2. *Inductive step:* Assume the inductive hypothesis, that $k^2 + k$ is divisible by 2. Then $(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + 2(k+1)$, the sum of a multiple of 2 (by the inductive hypothesis) and a multiple of 2 (by definition), hence, divisible by 2. **33.** Let $P(n)$ be "$n^5 - n$ is divisible by 5." *Basis step:* $P(0)$ is true because $0^5 - 0 = 0$ is divisible by 5. *Inductive step:* Assume that $P(k)$ is true, that is, $k^5 - 5$ is divisible by 5. Then $(k+1)^5 - (k+1) = (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k+1) = (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k)$ is also divisible by 5, because both terms in this sum are divisible by 5. **35.** Let $P(n)$ be the proposition that $(2n-1)^2 - 1$ is divisible by 8. The basis case $P(1)$ is true because $8 \mid 0$. Now assume that $P(k)$ is true. Because $[(2(k+1)-1]^2 - 1 = [(2k-1)^2 - 1] + 8k$, $P(k+1)$ is true because both terms on the right-hand side are divisible by 8. This shows that $P(n)$ is true for all positive integers n, so $m^2 - 1$ is divisible by 8 whenever m is an odd positive integer. **37.** *Basis step:* $11^{1+1} + 12^{2\cdot 1-1} = 121 + 12 = 133$ *Inductive step:* Assume the inductive hypothesis, that $11^{n+1} + 12^{2n-1}$ is divisible by 133. Then $11^{(n+1)+1} + 12^{2(n+1)-1} = 11 \cdot 11^{n+1} + 144 \cdot 12^{2n-1} = 11 \cdot 11^{n+1} + (11 + 133) \cdot 12^{2n-1} = 11(11^{n+1} + 12^{2n-1}) + 133 \cdot 12^{2n-1}$. The expression in parentheses is divisible by 133 by the inductive hypothesis, and obviously the second term is divisible by 133, so the entire quantity is divisible by 133, as desired. **39.** *Basis step:* $A_1 \subseteq B_1$ tautologically implies that $\bigcap_{j=1}^{1} A_j \subseteq \bigcap_{j=1}^{1} B_j$. *Inductive step:* Assume the inductive hypothesis that if $A_j \subseteq B_j$ for $j = 1, 2, \ldots, k$, then $\bigcap_{j=1}^{k} A_j \subseteq \bigcap_{j=1}^{k} B_j$. We want to show that if $A_j \subseteq B_j$ for $j = 1, 2, \ldots, k+1$, then $\bigcap_{j=1}^{k+1} A_j \subseteq \bigcap_{j=1}^{k+1} B_j$. Let x be an arbitrary element of $\bigcap_{j=1}^{k+1} A_j = \left(\bigcap_{j=1}^{k} A_j\right) \cap A_{k+1}$. Because $x \in \bigcap_{j=1}^{k} A_j$, we know by the inductive hypothesis that $x \in \bigcap_{j=1}^{k} B_j$; because $x \in A_{k+1}$, we know from the given fact that $A_{k+1} \subseteq B_{k+1}$ that $x \in B_{k+1}$. Therefore, $x \in \left(\bigcap_{j=1}^{k} B_j\right) \cap B_{k+1} = \bigcap_{j=1}^{k+1} B_j$. **41.** Let $P(n)$ be "$(A_1 \cup A_2 \cup \cdots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B)$." *Basis step:* $P(1)$ is trivially true. *Inductive step:* Assume that $P(k)$ is true. Then $(A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}) \cap B = [(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}] \cap B = [(A_1 \cup A_2 \cup \cdots \cup A_k) \cap B] \cup (A_{k+1} \cap B) = [(A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_k \cap B)] \cup (A_{k+1} \cap B) = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_k \cap B) \cup (A_{k+1} \cap B)$. **43.** Let $P(n)$ be "$\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k}$." *Basis step:* $P(1)$ is trivially true. *Inductive step:* Assume that $P(k)$ is true. Then $\overline{\bigcup_{j=1}^{k+1} A_j} = \overline{\left(\bigcup_{j=1}^{k} A_j\right) \cup A_{k+1}} = \overline{\left(\bigcup_{j=1}^{k} A_j\right)} \cap \overline{A_{k+1}} = \left(\bigcap_{j=1}^{k} \overline{A_j}\right) \cap \overline{A_{k+1}} = \bigcap_{j=1}^{k+1} \overline{A_j}$. **45.** Let $P(n)$ be the statement that a set with n elements has $n(n-1)/2$ two-element subsets. $P(2)$, the basis case, is true, because a set with two elements has one subset with two elements—namely, itself—and $2(2-1)/2 = 1$. Now assume that $P(k)$ is true. Let S be a set with $k+1$ elements. Choose an element a in S and let $T = S - \{a\}$. A two-element subset of S either contains a or does not. Those subsets not containing a are the subsets of T with two elements; by the inductive hypothesis there are $k(k-1)/2$ of these. There are k subsets of S with two elements that contain a, because such a subset contains a and one of the k elements in T. Hence, there are $k(k-1)/2 + k = (k+1)k/2$ two-element subsets of S. This completes the inductive proof. **47.** Reorder the locations if necessary so that $x_1 \le x_2 \le x_3 \le \cdots \le x_d$. Place the first tower at position $t_1 = x_1 + 1$. Assume tower k has been placed at position t_k. Then place tower $k+1$ at position $t_{k+1} = x + 1$, where x is the smallest x_i greater than $t_k + 1$. **49.** The two sets do not overlap if $n + 1 = 2$. In fact, the conditional statement $P(1) \to P(2)$ is false. **51.** The mistake is in applying the inductive hypothesis to look at $\max(x-1, y-1)$, because even though x and y are positive integers, $x - 1$ and $y - 1$ need not be (one or both could be 0). **53.** For the basis step ($n = 2$) the first person cuts the cake into two portions that she thinks are each $1/2$ of the cake, and the second person chooses the portion he thinks is at least $1/2$ of the cake (at least one of the pieces must satisfy that condition). For the inductive step, suppose there are $k + 1$ people. By the inductive hypothesis, we can suppose that the first k people have divided the cake among themselves so that each person is satisfied that he got at least a fraction $1/k$ of the cake. Each of them now cuts his or her piece into $k+1$ pieces of equal size. The last person gets to choose one piece from each of the first k people's portions. After this is done, each of the first k people is satisfied that she still has $(1/k)(k/(k+1)) = 1/(k+1)$ of the cake. To see that the last person is satisfied, suppose that he thought that the ith person ($1 \le i \le k$) had a portion p_i of the cake, where $\sum_{i=1}^{k} p_i = 1$. By choosing what he thinks is the largest piece from each person, he is satisfied that he has at least $\sum_{i=1}^{k} p_i/(k+1) = (1/(k+1)) \sum_{i=1}^{k} p_i = 1/(k+1)$ of the cake. **55.** We use the notation (i, j) to mean the square in row i and column j and use induction on $i + j$ to show that every square can be reached by the knight. *Basis step:* There are six base cases, for the cases when $i + j \le 2$. The knight is already at $(0, 0)$ to start, so the empty sequence of moves reaches that square. To reach $(1, 0)$, the knight moves $(0, 0) \to (2, 1) \to (0, 2) \to (1, 0)$. Similarly, to reach $(0, 1)$, the knight moves $(0, 0) \to (1, 2) \to (2, 0) \to (0, 1)$. Note that the knight has reached $(2, 0)$ and $(0, 2)$ in the process. For the last basis step there is $(0, 0) \to (1, 2) \to (2, 0) \to (0, 1) \to (2, 2) \to (0, 3) \to (1, 1)$. *Inductive step:* Assume the inductive hypothesis, that the knight can reach any square (i, j) for which $i + j = k$, where k is an integer greater than 1. We must show how the knight can reach each square (i, j) when $i + j = k + 1$. Because $k + 1 \ge 3$, at least one of i and j is at least 2. If $i \ge 2$, then by the inductive hypothesis, there is a sequence of moves ending at $(i - 2, j + 1)$, because $i - 2 + j + 1 = i + j - 1 = k$; from there it is just one step to (i, j); similarly, if $j \ge 2$. **57.** *Basis step:* The base cases $n = 0$ and $n = 1$ are true because the derivative of x^0 is 0 and the derivative of $x^1 = x$ is 1. *Inductive step:* Using the product rule, the inductive hypothesis, and the basis step shows that $\frac{d}{dx}x^{k+1} = \frac{d}{dx}(x \cdot x^k) = x \cdot \frac{d}{dx}x^k + x^k \frac{d}{dx}x = x \cdot kx^{k-1} + x^k \cdot 1 = kx^k + x^k = (k+1)x^k$. **59.** *Basis step:* For $k = 0$, $1 \equiv 1 \pmod{m}$. *Inductive step:* Suppose that $a \equiv b \pmod{m}$ and $a^k \equiv b^k \pmod{m}$; we must show that $a^{k+1} \equiv b^{k+1} \pmod{m}$. By Theorem 5 from Section 4.1, $a \cdot a^k \equiv b \cdot b^k \pmod{m}$, which by definition says that $a^{k+1} \equiv b^{k+1} \pmod{m}$. **61.** Let $P(n)$ be "$[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n)] \to [(p_1 \wedge \cdots \wedge p_{n-1}) \to p_n]$." *Basis step:* $P(2)$ is true because $(p_1 \to p_2) \to (p_1 \to p_2)$ is a tautology. *Inductive step:* Assume $P(k)$ is true. To show $[(p_1 \to p_2) \wedge \cdots \wedge (p_{k-1} \to p_k) \wedge (p_k \to p_{k+1})] \to [(p_1 \wedge \cdots \wedge p_{k-1} \wedge p_k) \to p_{k+1}]$ is a tautology, assume that the hypothesis of this conditional statement is true. Because both the hypothesis and $P(k)$ are true, it follows that $(p_1 \wedge \cdots \wedge p_{k-1}) \to p_k$ is true. Because this is true, and because $p_k \to p_{k+1}$ is true (it is part of the assumption) it follows by hypothetical syllogism that $(p_1 \wedge \cdots \wedge p_{k-1}) \to p_{k+1}$ is true. The weaker statement $(p_1 \wedge \cdots \wedge p_{k-1} \wedge p_k) \to p_{k+1}$ follows from this. **63.** We will first prove the result when n is a power of 2, that is, if $n = 2^k$, $k = 1, 2, \ldots$. Let $P(k)$ be the statement $A \geq G$, where A and G are the arithmetic and geometric means, respectively, of a set of $n = 2^k$ positive real numbers. *Basis step:* $k = 1$ and $n = 2^1 = 2$. Note that $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$. Expanding this shows that $a_1 - 2\sqrt{a_1 a_2} + a_2 \geq 0$, that is, $(a_1 + a_2)/2 \geq (a_1 a_2)^{1/2}$. *Inductive step:* Assume that $P(k)$ is true, with $n = 2^k$. We will show that $P(k+1)$ is true. We have $2^{k+1} = 2n$. Now $(a_1 + a_2 + \cdots + a_{2n})/(2n) = [(a_1 + a_2 + \cdots + a_n)/n + (a_{n+1} + a_{n+2} + \cdots + a_{2n})/n]/2$ and similarly $(a_1 a_2 \cdots a_{2n})^{1/(2n)} = [(a_1 \cdots a_n)^{1/n} (a_{n+1} \cdots a_{2n})^{1/n}]^{1/2}$. To simplify the notation, let $A(x, y, \ldots)$ and $G(x, y, \ldots)$ denote the arithmetic mean and geometric mean of $x, y, \ldots$, respectively. Also, if $x \leq x'$, $y \leq y'$, and so on, then $A(x, y, \ldots) \leq A(x', y', \ldots)$ and $G(x, y, \ldots) \leq G(x', y', \ldots)$. Hence, $A(a_1, \ldots, a_{2n}) = A(A(a_1, \ldots, a_n), A(a_{n+1}, \ldots, a_{2n})) \geq A(G(a_1, \ldots, a_n), G(a_{n+1}, \ldots, a_{2n})) \geq G(G(a_1, \ldots, a_n), G(a_{n+1}, \ldots, a_{2n})) = G(a_1, \ldots, a_{2n})$. This finishes the proof for powers of 2. Now if n is not a power of 2, let m be the next higher power of 2, and let $a_{n+1}, \ldots, a_m$ all equal $A(a_1, \ldots, a_n) = \overline{a}$. Then we have $[(a_1 a_2 \cdots a_n)\overline{a}^{m-n}]^{1/m} \leq A(a_1, \ldots, a_m)$, because m is a power of 2. Because $A(a_1, \ldots, a_m) = \overline{a}$, it follows that $(a_1 \cdots a_n)^{1/m} \overline{a}^{1-n/m} \leq \overline{a}^{n/m}$. Raising both sides to the (m/n)th power gives $G(a_1, \ldots, a_n) \leq A(a_1, \ldots, a_n)$. **65.** *Basis step:* For $n = 1$, the left-hand side is just $\frac{1}{1}$, which is 1. For $n = 2$, there are three nonempty subsets $\{1\}$, $\{2\}$, and $\{1, 2\}$, so the left-hand side is $\frac{1}{1} + \frac{1}{2} + \frac{1}{1 \cdot 2} = 2$. *Inductive step:* Assume that the statement is true for k. The set of the first $k + 1$ positive integers has many nonempty subsets, but they fall into three categories: a nonempty subset of the first k positive integers together with $k + 1$, a nonempty subset of the first k positive integers, or just $\{k + 1\}$. By the inductive hypothesis, the sum of the first category is k. For the second category, we can factor out $1/(k + 1)$ from each term of the sum and what remains is just k by the inductive hypothesis, so this part of the sum is $k/(k + 1)$. Finally, the third category simply yields $1/(k + 1)$. Hence, the entire summation is $k + k/(k + 1) + 1/(k + 1) = k + 1$. **67.** *Basis step:* If $A_1 \subseteq A_2$, then A_1 satisfies the condition of being a subset of each set in the collection; otherwise $A_2 \subseteq A_1$, so A_2 satisfies the condition. *Inductive step:* Assume the inductive hypothesis, that the conditional statement is true for k sets, and suppose we are given $k + 1$ sets that satisfy the given conditions. By the inductive hypothesis, there must be a set A_i for some $i \leq k$ such that $A_i \subseteq A_j$ for $1 \leq j \leq k$. If $A_i \subseteq A_{k+1}$, then we are done. Otherwise, we know that $A_{k+1} \subseteq A_i$, and this tells us that A_{k+1} satisfies the condition of being a subset of A_j for $1 \leq j \leq k + 1$. **69.** $G(1) = 0$, $G(2) = 1$, $G(3) = 3$, $G(4) = 4$ **71.** To show that $2n - 4$ calls are sufficient to exchange all the gossip, select persons 1, 2, 3, and 4 to be the central committee. Every person outside the central committee calls one person on the central committee. At this point the central committee members *as a group* know all the scandals. They then exchange information among themselves by making the calls 1-2, 3-4, 1-3, and 2-4 in that order. At this point, *every* central committee member knows all the scandals. Finally, again every person outside the central committee calls one person on the central committee, at which point everyone knows all the scandals. [The total number of calls is $(n - 4) + 4 + (n - 4) = 2n - 4$.] That this cannot be done with fewer than $2n - 4$ calls is much harder to prove; see Sandra M. Hedetniemi, Stephen T. Hedetniemi, and Arthur L. Liestman, "A survey of gossiping and broadcasting in communication networks," *Networks* **18** (1988), no. 4, 319–349, for details. **73.** We prove this by mathematical induction. The basis step ($n = 2$) is true tautologically. For $n = 3$, suppose that the intervals are (a, b), (c, d), and (e, f), where without loss of generality we can assume that $a \leq c \leq e$. Because $(a, b) \cap (e, f) \neq \emptyset$, we must have $e < b$; for a similar reason, $e < d$. It follows that the number halfway between e and the smaller of b and d is common to all three intervals. Now for the inductive step, assume that whenever we have k intervals that have pairwise nonempty intersections then there is a point common to all the intervals, and suppose that we are given intervals $I_1, I_2, \ldots, I_{k+1}$ that have pairwise nonempty intersections. For each i from 1 to k, let $J_i = I_i \cap I_{k+1}$. We claim that the collection $J_1, J_2, \ldots, J_k$ satisfies the inductive hypothesis, that is, that $J_{i_1} \cap J_{i_2} \neq \emptyset$ for each choice of subscripts i_1 and i_2. This follows from the $n = 3$ case proved above, using the sets I_{i_1}, I_{i_2}, and I_{k+1}. We can now invoke the inductive hypothesis to conclude that there is a number common to all of the sets J_i for $i = 1, 2, \ldots, k$, which perforce is in the intersection of all the sets I_i for $i = 1, 2, \ldots, k + 1$. **75.** Pair up the people. Have the people stand at mutually distinct small distances from their partners but far away from everyone else. Then each person throws a pie at his or her partner, so everyone gets hit.

77.



79. Let $P(n)$ be the statement that every $2^n \times 2^n \times 2^n$ checkerboard with a $1 \times 1 \times 1$ cube removed can be covered by tiles that are $2 \times 2 \times 2$ cubes each with a $1 \times 1 \times 1$ cube removed. The basis step, $P(1)$, holds because one tile coincides with the solid to be tiled. Now assume that $P(k)$ holds. Now consider a $2^{k+1} \times 2^{k+1} \times 2^{k+1}$ cube with a $1 \times 1 \times 1$ cube removed. Split this object into eight pieces using planes parallel to its faces and running through its center. The missing $1 \times 1 \times 1$ piece occurs in one of these eight pieces. Now position one tile with its center at the center of the large object so that the missing $1 \times 1 \times 1$ cube lies in the octant in which the large object is missing a $1 \times 1 \times 1$ cube. This creates eight $2^k \times 2^k \times 2^k$ cubes, each missing a $1 \times 1 \times 1$ cube. By the inductive hypothesis we can fill each of these eight objects with tiles. Putting these tilings together produces the desired tiling.

81.

83. Let $Q(n)$ be $P(n+b-1)$. The statement that $P(n)$ is true for $n = b, b+1, b+2, \ldots$ is the same as the statement that $Q(m)$ is true for all positive integers m. We are given that $P(b)$ is true [i.e., that $Q(1)$ is true], and that $P(k) \to P(k+1)$ for all $k \geq b$ [i.e., that $Q(m) \to Q(m+1)$ for all positive integers m]. Therefore, by the principle of mathematical induction, $Q(m)$ is true for all positive integers m.

Section 5.2

1. *Basis step:* We are told we can run one mile, so $P(1)$ is true. *Inductive step:* Assume the inductive hypothesis, that we can run any number of miles from 1 to k. We must show that we can run $k+1$ miles. If $k = 1$, then we are already told that we can run two miles. If $k > 1$, then the inductive hypothesis tells us that we can run $k-1$ miles, so we can run $(k-1)+2 = k+1$ miles. 3. **a)** $P(8)$ is true, because we can form 8 cents of postage with one 3-cent stamp and one 5-cent stamp. $P(9)$ is true, because we can form 9 cents of postage with three 3-cent stamps. $P(10)$ is true, because we can form 10 cents of postage with two 5-cent stamps. **b)** The statement that using just 3-cent and 5-cent stamps we can form j cents postage for all j with $8 \leq j \leq k$, where we assume that $k \geq 10$ **c)** Assuming the inductive hypothesis, we can form $k+1$ cents postage using just 3-cent and 5-cent stamps **d)** Because $k \geq 10$, 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. **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 8. 5. **a)** 4, 8, 11, 12, 15, 16, 19, 20, 22, 23, 24, 26, 27, 28, and all values greater than or equal to 30 **b)** Let $P(n)$ be the statement that we can form n cents of postage using just 4-cent and 11-cent stamps. We want to prove that $P(n)$ is true for all $n \geq 30$. For the basis step, $30 = 11 + 11 + 4 + 4$. 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 an 11-cent stamp, then replace it by three 4-cent stamps. Otherwise, k cents was formed from just 4-cent stamps. Because $k \geq 30$, there must be at least eight 4-cent stamps involved. Replace eight 4-cent stamps by three 11-cent stamps, and we have formed $k+1$ cents in postage. **c)** $P(n)$ is the same as in part (b). To prove that $P(n)$ is true for all $n \geq 30$, we check for the basis step that $30 = 11+11+4+4$, $31 = 11+4+4+4+4+4$, $32 = 4+4+4+4+4+4+4+4$, and $33 = 11+11+11$. For the inductive step, assume the inductive hypothesis, that $P(j)$ is true for all j with $30 \leq j \leq k$, where k is an arbitrary integer greater than or equal to 33. We want to show that $P(k+1)$ is true. Because $k-3 \geq 30$, 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. In this proof, our inductive hypothesis was that $P(j)$ was true for all values of j between 30 and k inclusive, rather than just that $P(30)$ was true. 7. We can form all amounts except \$1 and \$3. Let $P(n)$ be the statement that we can form n dollars using just 2-dollar and 5-dollar bills. We want to prove that $P(n)$ is true for all $n \geq 5$. (It is clear that \$1 and \$3 cannot be formed and that \$2 and \$4 can be formed.) For the basis step, note that $5 = 5$ and $6 = 2+2+2$. Assume the inductive hypothesis, that $P(j)$ is true for all j with $5 \leq j \leq k$, where k is an arbitrary integer greater than or equal to 6. We want to show that $P(k+1)$ is true. Because $k-1 \geq 5$, we know that $P(k-1)$ is true, that is, that we can form $k-1$ dollars. Add another 2-dollar bill, and we have formed $k+1$ dollars. 9. Let $P(n)$ be the statement that there is no positive integer b such that $\sqrt{2} = n/b$. *Basis step:* $P(1)$ is true because $\sqrt{2} > 1 \geq 1/b$ for all positive integers b. *Inductive step:* Assume that $P(j)$ is true for all $j \leq k$, where k is an arbitrary positive integer; we prove that $P(k+1)$ is true by contradiction. Assume that $\sqrt{2} = (k+1)/b$ for some positive integer b. Then $2b^2 = (k+1)^2$, so $(k+1)^2$ is even, and hence, $k+1$ is even. So write $k+1 = 2t$ for some positive integer t, whence $2b^2 = 4t^2$ and $b^2 = 2t^2$. By the same reasoning as before, b is even, so $b = 2s$ for some positive integer s. Then $\sqrt{2} = (k+1)/b = (2t)/(2s) = t/s$. But $t \leq k$, so this contradicts the inductive hypothesis, and our proof of the inductive step is complete. 11. *Basis step:* There are four base cases. If $n = 1 = 4 \cdot 0 + 1$, then clearly the second player wins. If there are two, three, or four matches ($n = 4 \cdot 0 + 2$, $n = 4 \cdot 0 + 3$, or $n = 4 \cdot 1$), then the first player can win by removing all but one match. *Inductive step:* Assume the strong inductive hypothesis, that in games with k or fewer matches, the first player can win if $k \equiv 0, 2,$ or $3 \pmod 4$ and the second player can win if $k \equiv 1 \pmod 4$. Suppose we have a game with $k+1$ matches, with $k \geq 4$. If $k+1 \equiv 0 \pmod 4$, then the first player can remove three matches, leaving $k-2$ matches for the other player. Because $k-2 \equiv 1 \pmod 4$, by the inductive hypothesis, this is a game that the second player

at that point (who is the first player in our game) can win. Similarly, if $k+1 \equiv 2 \pmod 4$, then the first player can remove one match; and if $k+1 \equiv 3 \pmod 4$, then the first player can remove two matches. Finally, if $k+1 \equiv 1 \pmod 4$, then the first player must leave k, $k-1$, or $k-2$ matches for the other player. Because $k \equiv 0 \pmod 4$, $k-1 \equiv 3 \pmod 4$, and $k-2 \equiv 2 \pmod 4$, by the inductive hypothesis, this is a game that the first player at that point (who is the second player in our game) can win. **13.** Let $P(n)$ be the statement that exactly $n-1$ moves are required to assemble a puzzle with n pieces. Now $P(1)$ is trivially true. Assume that $P(j)$ is true for all $j \le k$, and consider a puzzle with $k+1$ pieces. The final move must be the joining of two blocks, of size j and $k+1-j$ for some integer j with $1 \le j \le k$. By the inductive hypothesis, it required $j-1$ moves to construct the one block, and $k+1-j-1 = k-j$ moves to construct the other. Therefore, $1+(j-1)+(k-j) = k$ moves are required in all, so $P(k+1)$ is true. **15.** Let the Chomp board have n rows and n columns. We claim that the first player can win the game by making the first move to leave just the top row and leftmost column. Let $P(n)$ be the statement that if a player has presented his opponent with a Chomp configuration consisting of just n cookies in the top row and n cookies in the leftmost column, then he can win the game. We will prove $\forall n\, P(n)$ by strong induction. We know that $P(1)$ is true, because the opponent is forced to take the poisoned cookie at his first turn. Fix $k \ge 1$ and assume that $P(j)$ is true for all $j \le k$. We claim that $P(k+1)$ is true. It is the opponent's turn to move. If she picks the poisoned cookie, then the game is over and she loses. Otherwise, assume she picks the cookie in the top row in column j, or the cookie in the left column in row j, for some j with $2 \le j \le k+1$. The first player now picks the cookie in the left column in row j, or the cookie in the top row in column j, respectively. This leaves the position covered by $P(j-1)$ for his opponent, so by the inductive hypothesis, he can win. **17.** Let $P(n)$ be the statement that if a simple polygon with n sides is triangulated, then at least two of the triangles in the triangulation have two sides that border the exterior of the polygon. We will prove $\forall n \ge 4\, P(n)$. The statement is clearly true for $n = 4$, because there is only one diagonal, leaving two triangles with the desired property. Fix $k \ge 4$ and assume that $P(j)$ is true for all j with $4 \le j \le k$. Consider a polygon with $k+1$ sides, and some triangulation of it. Pick one of the diagonals in this triangulation. First suppose that this diagonal divides the polygon into one triangle and one polygon with k sides. Then the triangle has two sides that border the exterior. Furthermore, the k-gon has, by the inductive hypothesis, two triangles that have two sides that border the exterior of that k-gon, and only one of these triangles can fail to be a triangle that has two sides that border the exterior of the original polygon. The only other case is that this diagonal divides the polygon into two polygons with j sides and $k+3-j$ sides for some j with $4 \le j \le k-1$. By the inductive hypothesis, each of these two polygons has two triangles that have two sides that border their exterior, and in each case only one of these triangles can fail to be a triangle that has two sides that border the exterior of the original polygon. **19.** Let $P(n)$ be the statement that the area of a simple polygon with n sides and vertices all at lattice points is given by $I(P) + B(P)/2 - 1$. We will prove $P(n)$ for all $n \ge 3$. We begin with an additivity lemma: If P is a simple polygon with all vertices at lattice points, divided into polygons P_1 and P_2 by a diagonal, then $I(P) + B(P)/2 - 1 = [I(P_1) + B(P_1)/2 - 1] + [I(P_2) + B(P_2)/2 - 1]$. To prove this, suppose there are k lattice points on the diagonal, not counting its endpoints. Then $I(P) = I(P_1) + I(P_2) + k$ and $B(P) = B(P_1) + B(P_2) - 2k - 2$; and the result follows by simple algebra. What this says in particular is that if Pick's formula gives the correct area for P_1 and P_2, then it must give the correct formula for P, whose area is the sum of the areas for P_1 and P_2; and similarly if Pick's formula gives the correct area for P and one of the P_i's, then it must give the correct formula for the other P_i. Next we prove the theorem for rectangles whose sides are parallel to the coordinate axes. Such a rectangle necessarily has vertices at (a, b), (a, c), (d, b), and (d, c), where a, b, c, and d are integers with $b < c$ and $a < d$. Its area is $(c-b)(d-a)$. Also, $B = 2(c-b+d-a)$ and $I = (c-b-1)(d-a-1) = (c-b)(d-a)-(c-b)-(d-a)+1$. Therefore, $I + B/2 - 1 = (c-b)(d-a) - (c-b) - (d-a) + 1 + (c-b+d-a) - 1 = (c-b)(d-a)$, which is the desired area. Next consider a right triangle whose legs are parallel to the coordinate axes. This triangle is half a rectangle of the type just considered, for which Pick's formula holds, so by the additivity lemma, it holds for the triangle as well. (The values of B and I are the same for each of the two triangles, so if Picks's formula gave an answer that was either too small or too large, then it would give a correspondingly wrong answer for the rectangle.) For the next step, consider an arbitrary triangle with vertices at lattice points that is not of the type already considered. Embed it in as small a rectangle as possible. There are several possible ways this can happen, but in any case (and adding one more edge in one case), the rectangle will have been partitioned into the given triangle and two or three right triangles with sides parallel to the coordinate axes. Again by the additivity lemma, we are guaranteed that Pick's formula gives the correct area for the given triangle. This completes the proof of $P(3)$, the basis step in our strong induction proof. For the inductive step, given an arbitrary polygon, use Lemma 1 in the text to split it into two polygons. Then by the additivity lemma above and the inductive hypothesis, we know that Pick's formula gives the correct area for this polygon. **21. a)** In the left figure $\angle abp$ is smallest, but $\overline{bp}$ is not an interior diagonal. **b)** In the right figure $\overline{bd}$ is not an interior diagonal. **c)** In the right figure $\overline{bd}$ is not an interior diagonal. **23. a)** When we try to prove the inductive step and find a triangle in each subpolygon with at least two sides bordering the exterior, it may happen in each case that the triangle we are guaranteed in fact borders the diagonal (which is part of the boundary of that polygon). This leaves us with no triangles guaranteed to touch the boundary of the *original* polygon. **b)** We proved the stronger statement $\forall n \ge 4\, T(n)$ in Exercise 17. **25. a)** The inductive step here allows us to conclude that

$P(3), P(5), \ldots$ are all true, but we can conclude nothing about $P(2), P(4), \ldots$. **b)** $P(n)$ is true for all positive integers n, using strong induction. **c)** The inductive step here enables us to conclude that $P(2)$, $P(4)$, $P(8)$, $P(16)$, …are all true, but we can conclude nothing about $P(n)$ when n is not a power of 2. **d)** This is mathematical induction; we can conclude that $P(n)$ is true for all positive integers n. 27. Suppose, for a proof by contradiction, that there is some positive integer n such that $P(n)$ is not true. Let m be the smallest positive integer greater than n for which $P(m)$ *is* true; we know that such an m exists because $P(m)$ is true for infinitely many values of m. But we know that $P(m) \to P(m-1)$, so $P(m-1)$ is also true. Thus, $m-1$ cannot be greater than n, so $m-1=n$ and $P(n)$ is in fact true. This contradiction shows that $P(n)$ is true for all n. 29. The error is in going from the base case $n=0$ to the next case, $n=1$; we cannot write 1 as the sum of two smaller natural numbers. 31. Assume that the well-ordering property holds. Suppose that $P(1)$ is true and that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(n)] \to P(n+1)$ is true for every positive integer n. Let S be the set of positive integers n for which $P(n)$ is false. We will show $S=\emptyset$. Assume that $S \neq \emptyset$. Then by the well-ordering property there is a least integer m in S. We know that m cannot be 1 because $P(1)$ is true. Because $n=m$ is the least integer such that $P(n)$ is false, $P(1), P(2), \ldots, P(m-1)$ are true, and $m-1 \geq 1$. Because $[P(1) \wedge P(2) \wedge \cdots \wedge P(m-1)] \to P(m)$ is true, it follows that $P(m)$ must also be true, which is a contradiction. Hence, $S=\emptyset$. 33. In each case, give a proof by contradiction based on a "smallest counterexample," that is, values of n and k such that $P(n,k)$ is not true and n and k are smallest in some sense. **a)** Choose a counterexample with $n+k$ as small as possible. We cannot have $n=1$ and $k=1$, because we are given that $P(1,1)$ is true. Therefore, either $n>1$ or $k>1$. In the former case, by our choice of counterexample, we know that $P(n-1,k)$ is true. But the inductive step then forces $P(n,k)$ to be true, a contradiction.The latter case is similar. So our supposition that there is a counterexample mest be wrong, and $P(n,k)$ is true in all cases. **b)** Choose a counterexample with n as small as possible. We cannot have $n=1$, because we are given that $P(1,k)$ is true for all k. Therefore, $n>1$. By our choice of counterexample, we know that $P(n-1,k)$ is true. But the inductive step then forces $P(n,k)$ to be true, a contradiction. **c)** Choose a counterexample with k as small as possible. We cannot have $k=1$, because we are given that $P(n,1)$ is true for all n. Therefore, $k>1$. By our choice of counterexample, we know that $P(n,k-1)$ is true. But the inductive step then forces $P(n,k)$ to be true, a contradiction. 35. Let $P(n)$ be the statement that if $x_1, x_2, \ldots, x_n$ are n distinct real numbers, then $n-1$ multiplications are used to find the product of these numbers no matter how parentheses are inserted in the product. We will prove that $P(n)$ is true using strong induction. The basis case $P(1)$ is true because $1-1=0$ multiplications are required to find the product of x_1, a product with only one factor. Suppose that $P(k)$ is true for $1 \leq k \leq n$. The last multiplication used to find the product of the $n+1$ distinct real numbers $x_1, x_2, \ldots, x_n, x_{n+1}$ is a multiplication of the product of the first k of these numbers for some k and the product of the last $n+1-k$ of them. By the inductive hypothesis, $k-1$ multiplications are used to find the product of k of the numbers, no matter how parentheses were inserted in the product of these numbers, and $n-k$ multiplications are used to find the product of the other $n+1-k$ of them, no matter how parentheses were inserted in the product of these numbers. Because one more multiplication is required to find the product of all $n+1$ numbers, the total number of multiplications used equals $(k-1)+(n-k)+1=n$. Hence, $P(n+1)$ is true. 37. Assume that $a=dq+r=dq'+r'$ with $0 \leq r < d$ and $0 \leq r' < d$. Then $d(q-q')=r'-r$. It follows that d divides $r'-r$. Because $-d < r'-r < d$, we have $r'-r=0$. Hence, $r'=r$. It follows that $q=q'$. 39. This is a paradox caused by self-reference. The answer is clearly "no." There are a finite number of English words, so only a finite number of strings of 15 words or fewer; therefore, only a finite number of positive integers can be so described, not all of them. 41. Suppose that the well-ordering property were false. Let S be a nonempty set of nonnegative integers that has no least element. Let $P(n)$ be the statement "$i \notin S$ for $i=0,1,\ldots,n$." $P(0)$ is true because if $0 \in S$ then S has a least element, namely, 0. Now suppose that $P(n)$ is true. Thus, $0 \notin S, 1 \notin S, \ldots, n \notin S$. Clearly, $n+1$ cannot be in S, for if it were, it would be its least element. Thus $P(n+1)$ is true. So by the principle of mathematical induction, $n \notin S$ for all nonnegative integers n. Thus, $S=\emptyset$, a contradiction. 43. Strong induction implies the principle of mathematical induction, for if one has shown that $P(k) \to P(k+1)$ is true, then one has also shown that $[P(1) \wedge \cdots \wedge P(k)] \to P(k+1)$ is true. By Exercise 41, the principle of mathematical induction implies the well-ordering property. Therefore by assuming strong induction as an axiom, we can prove the well-ordering property.

Section 5.3

1. **a)** $f(1)=3$, $f(2)=5$, $f(3)=7$, $f(4)=9$ **b)** $f(1)=3$, $f(2)=9$, $f(3)=27$, $f(4)=81$ **c)** $f(1)=2$, $f(2)=4$, $f(3)=16$, $f(4)=65{,}536$ **d)** $f(1)=3$, $f(2)=13$, $f(3)=183$, $f(4)=33{,}673$ 3. **a)** $f(2)=-1$, $f(3)=5$, $f(4)=2$, $f(5)=17$ **b)** $f(2)=-4$, $f(3)=32$, $f(4)=-4096$, $f(5)=536{,}870{,}912$ **c)** $f(2)=8$, $f(3)=176$, $f(4)=92{,}672$, $f(5)=25{,}764, 174, 848$ **d)** $f(2)=-\frac{1}{2}$, $f(3)=-4$, $f(4)=\frac{1}{8}$, $f(5)=-32$ 5. **a)** Not valid **b)** $f(n)=1-n$. *Basis step:* $f(0)=1=1-0$. *Inductive step:* if $f(k)=1-k$, then $f(k+1)=f(k)-1=1-k-1=1-(k+1)$. **c)** $f(n)=4-n$ if $n>0$, and $f(0)=2$. *Basis step:* $f(0)=2$ and $f(1)=3=4-1$. *Inductive step* (with $k \geq 1$): $f(k+1)=f(k)-1=(4-k)-1=4-(k+1)$. **d)** $f(n)=2^{\lfloor (n+1)/2 \rfloor}$. *Basis step:* $f(0)=1=2^{\lfloor (0+1)/2 \rfloor}$ and $f(1)=2=2^{\lfloor (1+1)/2 \rfloor}$. *Inductive step* (with $k \geq 1$): $f(k+1)=2f(k-1)=2 \cdot 2^{\lfloor k/2 \rfloor}=2^{\lfloor k/2 \rfloor+1}=2^{\lfloor ((k+1)+1)/2 \rfloor}$. **e)** $f(n)=3^n$. *Basis step:* Trivial. *Inductive step:* For odd n, $f(n)=3f(n-1)=3 \cdot 3^{n-1}=3^n$; and for even $n>1$, $f(n)=9f(n-2)=9 \cdot 3^{n-2}=3^n$. 7. There

are many possible correct answers. We will supply relatively simple ones. **a)** $a_{n+1} = a_n + 6$ for $n \geq 1$ and $a_1 = 6$ **b)** $a_{n+1} = a_n + 2$ for $n \geq 1$ and $a_1 = 3$ **c)** $a_{n+1} = 10a_n$ for $n \geq 1$ and $a_1 = 10$ **d)** $a_{n+1} = a_n$ for $n \geq 1$ and $a_1 = 5$ **9.** $F(0) = 0$, $F(n) = F(n-1) + n$ for $n \geq 1$ **11.** $P_m(0) = 0$, $P_m(n+1) = P_m(n) + m$ **13.** Let $P(n)$ be "$f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$." *Basis step:* $P(1)$ is true because $f_1 = 1 = f_2$. *Inductive step:* Assume that $P(k)$ is true. Then $f_1 + f_3 + \cdots + f_{2k-1} + f_{2k+1} = f_{2k} + f_{2k+1} = f_{2k+2} + f_{2(k+1)}$. **15.** *Basis step:* $f_0 f_1 + f_1 f_2 = 0 \cdot 1 + 1 \cdot 1 = 1^2 = f_2^2$. *Inductive step:* Assume that $f_0 f_1 + f_1 f_2 + \cdots + f_{2k-1} f_{2k} = f_{2k}^2$. Then $f_0 f_1 + f_1 f_2 + \cdots + f_{2k-1} f_{2k} + f_{2k} f_{2k+1} + f_{2k+1} f_{2k+2} = f_{2k}^2 + f_{2k} f_{2k+1} + f_{2k+1} f_{2k+2} = f_{2k}(f_{2k} + f_{2k+1}) + f_{2k+1} f_{2k+2} = f_{2k} f_{2k+2} + f_{2k+1} f_{2k+2} = (f_{2k} + f_{2k+1}) f_{2k+2} = f_{2k+2}^2$. **17.** The number of divisions used by the Euclidean algorithm to find $\gcd(f_{n+1}, f_n)$ is 0 for $n = 0$, 1 for $n = 1$, and $n - 1$ for $n \geq 2$. To prove this result for $n \geq 2$ we use mathematical induction. For $n = 2$, one division shows that $\gcd(f_3, f_2) = \gcd(2, 1) = \gcd(1, 0) = 1$. Now assume that $k - 1$ divisions are used to find $\gcd(f_{k+1}, f_k)$. To find $\gcd(f_{k+2}, f_{k+1})$, first divide f_{k+2} by f_{k+1} to obtain $f_{k+2} = 1 \cdot f_{k+1} + f_k$. After one div- ision we have $\gcd(f_{k+2}, f_{k+1}) = \gcd(f_{k+1}, f_k)$. By the inductive hypothesis it follows that exactly $k - 1$ more divisions are required. This shows that k divisions are required to find $\gcd(f_{k+2}, f_{k+1})$, finishing the inductive proof. **19.** $|A| = -1$. Hence, $|A^n| = (-1)^n$. It follows that $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$. **21. a)** Proof by induction. *Basis step:* For $n = 1$, $\max(-a_1) = -a_1 = -\min(a_1)$. For $n = 2$, there are two cases. If $a_2 \geq a_1$, then $-a_1 \geq -a_2$, so $\max(-a_1, -a_2) = -a_1 = -\min(a_1, a_2)$. If $a_2 < a_1$, then $-a_1 < -a_2$, so $\max(-a_1, -a_2) = -a_2 = -\min(a_1, a_2)$. *Inductive step:* Assume true for k with $k \geq 2$. Then $\max(-a_1, -a_2, \ldots, -a_k, -a_{k+1}) = \max(\max(-a_1, \ldots, -a_k), -a_{k+1}) = \max(-\min(a_1, \ldots, a_k), -a_{k+1}) = -\min(\min(a_1, \ldots, a_k), a_{k+1}) = -\min(a_1, \ldots, a_{k+1})$. **b)** Proof by mathematical induction. *Basis step:* For $n = 1$, the result is the identity $a_1 + b_1 = a_1 + b_1$. For $n = 2$, first consider the case in which $a_1 + b_1 \geq a_2 + b_2$. Then $\max(a_1 + b_1, a_2 + b_2) = a_1 + b_1$. Also note that $a_1 \leq \max(a_1, a_2)$ and $b_1 \leq \max(b_1, b_2)$, so $a_1 + b_1 \leq \max(a_1, a_2) + \max(b_1, b_2)$. Therefore, $\max(a_1+b_1, a_2+b_2) = a_1+b_1 \leq \max(a_1, a_2)+\max(b_1, b_2)$. The case with $a_1 + b_1 < a_2 + b_2$ is similar. *Inductive step:* Assume that the result is true for k. Then $\max(a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k, a_{k+1} + b_{k+1}) = \max(\max(a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k), a_{k+1} + b_{k+1}) \leq \max(\max(a_1, a_2, \ldots, a_k) + \max(b_1, b_2, \ldots, b_k), a_{k+1} + b_{k+1}) \leq \max(\max(a_1, a_2, \ldots, a_k), a_{k+1}) + \max(\max(b_1, b_2, \ldots, b_k), b_{k+1}) = \max(a_1, a_2, \ldots, a_k, a_{k+1}) + \max(b_1, b_2, \ldots, b_k, b_{k+1})$. **c)** Same as part (b), but replace every occurrence of "max" by "min" and invert each inequality. **23.** $5 \in S$, and $x + y \in S$ if $x, y \in S$. **25. a)** $0 \in S$, and if $x \in S$, then $x + 2 \in S$ and $x - 2 \in S$. **b)** $2 \in S$, and if $x \in S$, then $x + 3 \in S$. **c)** $1 \in S$, $2 \in S$, $3 \in S$, $4 \in S$, and if $x \in S$, then $x + 5 \in S$. **27. a)** (0, 1), (1, 1), (2, 1); (0, 2), (1, 2), (2, 2), (3, 2), (4, 2); (0, 3), (1, 3), (2, 3), (3, 3), (4, 3), (5, 3), (6, 3); (0, 4), (1, 4), (2, 4), (3, 4), (4, 4), (5, 4), (6, 4), (7, 4), (8, 4) **b)** Let $P(n)$ be the statement that $a \leq 2b$ whenever $(a, b) \in S$ is obtained by n applications of the recursive step. *Basis step:* $P(0)$ is true, because the only element of S obtained with no applications of the recursive step is $(0, 0)$, and indeed $0 \leq 2 \cdot 0$. *Inductive step:* Assume that $a \leq 2b$ 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. Because 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 $a \leq 2b$. Add $0 \leq 2$, $1 \leq 2$, and $2 \leq 2$, respectively, to obtain $a \leq 2(b + 1)$, $a + 1 \leq 2(b + 1)$, and $a + 2 \leq 2(b + 1)$, as desired. **c)** This holds for the basis step, because $0 \leq 0$. If this holds for (a, b), then it also holds for the elements obtained from (a, b) in the recursive step, because adding $0 \leq 2$, $1 \leq 2$, and $2 \leq 2$, respectively, to $a \leq 2b$ yields $a \leq 2(b + 1)$, $a + 1 \leq 2(b + 1)$, and $a + 2 \leq 2(b + 1)$. **29. a)** Define S by $(1, 1) \in S$, and if $(a, b) \in S$, then $(a + 2, b) \in S$, $(a, b + 2) \in S$, and $(a + 1, b + 1) \in S$. All elements put in S satisfy the condition, because $(1, 1)$ has an even sum of coordinates, and if (a, b) has an even sum of coordinates, then so do $(a+2, b)$, $(a, b+2)$, and $(a+1, b+1)$. Conversely, we show by induction on the sum of the coordinates that if $a + b$ is even, then $(a, b) \in S$. If the sum is 2, then $(a, b) = (1, 1)$, and the basis step put (a, b) into S. Otherwise the sum is at least 4, and at least one of $(a - 2, b)$, $(a, b - 2)$, and $(a - 1, b - 1)$ must have positive integer coordinates whose sum is an even number smaller than $a + b$, and therefore must be in S. Then one application of the recursive step shows that $(a, b) \in S$. **b)** Define S by $(1, 1)$, $(1, 2)$, and $(2, 1)$ are in S, and if $(a, b) \in S$, then $(a + 2, b)$ and $(a, b + 2)$ are in S. To prove that our definition works, we note first that $(1, 1)$, $(1, 2)$, and $(2, 1)$ all have an odd coordinate, and if (a, b) has an odd coordinate, then so do $(a + 2, b)$ and $(a, b + 2)$. Conversely, we show by induction on the sum of the coordinates that if (a, b) has at least one odd coordinate, then $(a, b) \in S$. If $(a, b) = (1, 1)$ or $(a, b) = (1, 2)$ or $(a, b) = (2, 1)$, then the basis step put (a, b) into S. Otherwise either a or b is at least 3, so at least one of $(a - 2, b)$ and $(a, b - 2)$ must have positive integer coordinates whose sum is smaller than $a + b$, and therefore must be in S. Then one application of the recursive step shows that $(a, b) \in S$. **c)** $(1, 6) \in S$ and $(2, 3) \in S$, and if $(a, b) \in S$, then $(a + 2, b) \in S$ and $(a, b + 6) \in S$. To prove that our definition works, we note first that $(1, 6)$ and $(2, 3)$ satisfy the condition, and if (a, b) satisfies the condition, then so do $(a + 2, b)$ and $(a, b + 6)$. Conversely we show by induction on the sum of the coordinates that if (a, b) satisfies the condition, then $(a, b) \in S$. For sums 5 and 7, the only points are $(1, 6)$, which the basis step put into S, $(2, 3)$, which the basis step put into S, and $(4, 3) = (2 + 2, 3)$, which is in S by one application of the recursive definition. For a sum greater than 7, either $a \geq 3$, or

$a \le 2$ and $b \ge 9$, in which case either $(a-2, b)$ or $(a, b-6)$ must have positive integer coordinates whose sum is smaller than $a+b$ and satisfy the condition for being in S. Then one application of the recursive step shows that $(a, b) \in S$. **31.** If x is a set or a variable representing a set, then x is a well-formed formula. If x and y are well-formed formulae, then so are $\overline{x}$, $(x \cup y)$, $(x \cap y)$, and $(x - y)$. **33. a)** If $x \in D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $m(x) = x$; if $s = tx$, where $t \in D^*$ and $x \in D$, then $m(s) = \min(m(s), x)$. **b)** Let $t = wx$, where $w \in D^*$ and $x \in D$. If $w = \lambda$, then $m(st) = m(sx) = \min(m(s), x) = \min(m(s), m(x))$ by the recursive step and the basis step of the definition of m. Otherwise, $m(st) = m((sw)x) = \min(m(sw), x)$ by the definition of m. Now $m(sw) = \min(m(s), m(w))$ by the inductive hypothesis of the structural induction, so $m(st) = \min(\min(m(s), m(w)), x) = \min(m(s), \min(m(w), x))$ by the meaning of min. But $\min(m(w), x) = m(wx) = m(t)$ by the recursive step of the definition of m. Thus, $m(st) = \min(m(s), m(t))$. **35.** $\lambda^R = \lambda$ and $(ux)^R = xu^R$ for $x \in \Sigma$, $u \in \Sigma^*$. **37.** $w^0 = \lambda$ and $w^{n+1} = ww^n$. **39.** When the string consists of n 0s followed by n 1s for some non- negative integer n **41.** Let $P(i)$ be "$l(w^i) = i \cdot l(w)$." $P(0)$ is true because $l(w^0) = 0 = 0 \cdot l(w)$. Assume $P(i)$ is true. Then $l(w^{i+1}) = l(ww^i) = l(w) + l(w^i) = l(w) + i \cdot l(w) = (i+1) \cdot l(w)$. **43.** *Basis step:* For the full binary tree consisting of just a root the result is true because $n(T) = 1$ and $h(T) = 0$, and $1 \ge 2 \cdot 0 + 1$. *Inductive step:* Assume that $n(T_1) \ge 2h(T_1) + 1$ and $n(T_2) \ge 2h(T_2) + 1$. By the recursive definitions of $n(T)$ and $h(T)$, we have $n(T) = 1 + n(T_1) + n(T_2)$ and $h(T) = 1 + \max(h(T_1), h(T_2))$. Therefore $n(T) = 1 + n(T_1) + n(T_2) \ge 1 + 2h(T_1) + 1 + 2h(T_2) + 1 \ge 1 + 2 \cdot \max(h(T_1), h(T_2)) + 2 = 1 + 2(\max(h(T_1), h(T_2)) + 1) = 1 + 2h(T)$. **45.** *Basis step:* $a_{0,0} = 0 = 0 + 0$. *Inductive step:* Assume that $a_{m',n'} = m' + n'$ whenever (m', n') is less than (m, n) in the lexicographic ordering of $\mathbf{N} \times \mathbf{N}$. If $n = 0$ then $a_{m,n} = a_{m-1,n} + 1 = m - 1 + n + 1 = m + n$. If $n > 0$, then $a_{m,n} = a_{m,n-1} + 1 = m + n - 1 + 1 = m + n$. **47. a)** $P_{m,m} = P_m$ because a number exceeding m cannot be used in a partition of m. **b)** Because there is only one way to partition 1, namely, $1 = 1$, it follows that $P_{1,n} = 1$. Because there is only one way to partition m into 1s, $P_{m,1} = 1$. When $n > m$ it follows that $P_{m,n} = P_{m,m}$ because a number exceeding m cannot be used. $P_{m,m} = 1 + P_{m,m-1}$ because one extra partition, namely, $m = m$, arises when m is allowed in the partition. $P_{m,n} = P_{m,n-1} + P_{m-n,n}$ if $m > n$ because a partition of m into integers not exceeding n either does not use any ns and hence, is counted in $P_{m,n-1}$ or else uses an n and a partition of $m - n$, and hence, is counted in $P_{m-n,n}$. **c)** $P_5 = 7$, $P_6 = 11$ **49.** Let $P(n)$ be "$A(n, 2) = 4$." *Basis step:* $P(1)$ is true because $A(1, 2) = A(0, A(1, 1)) = A(0, 2) = 2 \cdot 2 = 4$. *Inductive step:* Assume that $P(n)$ is true, that is, $A(n, 2) = 4$. Then $A(n+1, 2) = A(n, A(n+1, 1)) = A(n, 2) = 4$. **51. a)** 16 **b)** 65,536 **53.** Use a double induction argument to prove the stronger statement: $A(m, k) > A(m, l)$ when $k > l$. *Basis step:* When $m = 0$ the statement is true because $k > l$ implies that $A(0, k) = 2k > 2l = A(0, l)$. *Inductive step:* Assume that $A(m, x) > A(m, y)$ for all nonnegative integers x and y with $x > y$. We will show that this implies that $A(m+1, k) > A(m+1, l)$ if $k > l$. *Basis steps:* When $l = 0$ and $k > 0$, $A(m+1, l) = 0$ and either $A(m+1, k) = 2$ or $A(m+1, k) = A(m, A(m+1, k-1))$. If $m = 0$, this is $2A(1, k-1) = 2^k$. If $m > 0$, this is greater than 0 by the inductive hypothesis. In all cases, $A(m+1, k) > 0$, and in fact, $A(m+1, k) \ge 2$. If $l = 1$ and $k > 1$, then $A(m+1, l) = 2$ and $A(m+1, k) = A(m, A(m+1, k-1))$, with $A(m+1, k-1) \ge 2$. Hence, by the inductive hypothesis, $A(m, A(m+1, k-1)) \ge A(m, 2) > A(m, 1) = 2$. *Inductive step:* Assume that $A(m+1, r) > A(m+1, s)$ for all $r > s$, $s = 0, 1, \ldots, l$. Then if $k+1 > l+1$ it follows that $A(m+1, k+1) = A(m, A(m+1, k)) > A(m, A(m+1, k)) = A(m+1, l+1)$. **55.** From Exercise 54 it follows that $A(i, j) \ge A(i-1, j) \ge \cdots \ge A(0, j) = 2j \ge j$. **57.** Let $P(n)$ be "$F(n)$ is well-defined." Then $P(0)$ is true because $F(0)$ is specified. Assume that $P(k)$ is true for all $k < n$. Then $F(n)$ is well-defined at n because $F(n)$ is given in terms of $F(0), F(1), \ldots, F(n-1)$. So $P(n)$ is true for all integers n. **59. a)** The value of $F(1)$ is ambiguous. **b)** $F(2)$ is not defined because $F(0)$ is not defined. **c)** $F(3)$ is ambiguous and $F(4)$ is not defined because $F(\frac{4}{3})$ makes no sense. **d)** The definition of $F(1)$ is ambiguous because both the second and third clause seem to apply. **e)** $F(2)$ cannot be computed because trying to compute $F(2)$ gives $F(2) = 1 + F(F(1)) = 1 + F(2)$. **61. a)** 1 **b)** 2 **c)** 3 **d)** 3 **e)** 4 **f)** 4 **g)** 5 **63.** $f_0^*(n) = \lceil n/a \rceil$ **65.** $f_2^*(n) = \lceil \log \log n \rceil$ for $n \ge 2$, $f_2^*(1) = 0$

Section 5.4

1. First, we use the recursive step to write $5! = 5 \cdot 4!$. We then use the recursive step repeatedly to write $4! = 4 \cdot 3!$, $3! = 3 \cdot 2!$, $2! = 2 \cdot 1!$, and $1! = 1 \cdot 0!$. Inserting the value of $0! = 1$, and working back through the steps, we see that $1! = 1 \cdot 1 = 1$, $2! = 2 \cdot 1! = 2 \cdot 1 = 2$, $3! = 3 \cdot 2! = 3 \cdot 2 = 6$, $4! = 4 \cdot 3! = 4 \cdot 6 = 24$, and $5! = 5 \cdot 4! = 5 \cdot 24 = 120$. **3.** With this input, the algorithm uses the **else** clause to find that $\gcd(8, 13) = \gcd(13 \textbf{ mod } 8, 8) = \gcd(5, 8)$. It uses this clause again to find that $\gcd(5, 8) = \gcd(8 \textbf{ mod } 5, 5) = \gcd(3, 5)$, then to get $\gcd(3, 5) = \gcd(5 \textbf{ mod } 3, 3) = \gcd(2, 3)$, then $\gcd(2, 3) = \gcd(3 \textbf{ mod } 2, 2) = \gcd(1, 2)$, 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 $\gcd(8, 13) = 1$. **5.** First, because $n = 11$ is odd, we use the **else** clause to see that $mpower(3, 11, 5) = (mpower(3, 5, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5$. We next use the **else** clause again to see that $mpower(3, 5, 5) = (mpower(3, 2, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5$. Then we use the **else if** clause to see that $mpower(3, 2, 5) = mpower(3, 1, 5)^2 \textbf{ mod } 5$. Using the **else** clause again, we have $mpower(3, 1, 5) = (mpower(3, 0, 5)^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5$. Finally, using the **if** clause, we see that $mpower(3, 0, 5) = 1$. Working backward it follows that $mpower(3, 1, 5) = (1^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 3$, $mpower(3, 2, 5) = 3^2 \textbf{ mod } 5 = 4$, $mpower(3, 5, 5) = (4^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 3$, and finally $mpower(3, 11, 5) = (3^2 \textbf{ mod } 5 \cdot 3 \textbf{ mod } 5) \textbf{ mod } 5 = 2$. We conclude that $3^{11} \textbf{ mod } 5 = 2$.

7. **procedure** *mult*(n: positive integer, x: integer)
 if $n = 1$ **then return** x
 else return $x + mult(n - 1, x)$

9. **procedure** *sum of odds*(n: positive integer)
 if $n = 1$ **then return** 1
 else return *sum of odds* $(n - 1) + 2n - 1$

11. **procedure** *smallest*($a_1, \ldots, a_n$: integers)
 if $n = 1$ **then return** a_1
 else return
  $\min(smallest(a_1, \ldots, a_{n-1}), a_n)$

13. **procedure** *modfactorial*(n, m: positive integers)
 if $n = 1$ **then return** 1
 else return
  $(n \cdot modfactorial(n - 1, m)) \textbf{ mod } m$

15. **procedure** *gcd*(a, b: nonnegative integers)
 $\{a < b$ assumed to hold$\}$
 if $a = 0$ **then return** b
 else if $a = b - a$ **then return** a
 else if $a < b - a$ **then return** $gcd(a, b - a)$
 else return $gcd(b - a, a)$

17. **procedure** *multiply*(x, y: nonnegative integers)
 if $y = 0$ **then return** 0
 else if y is even **then**
  return $2 \cdot multiply(x, y/2)$
 else return $2 \cdot multiply(x, (y-1)/2) + x$

19. We use strong induction on a. *Basis step:* If $a = 0$, we know that $\gcd(0, b) = b$ for all $b > 0$, and that is precisely what the **if** clause does. *Inductive step:* Fix $k > 0$, assume the inductive hypothesis—that the algorithm works correctly for all values of its first argument less than k—and consider what happens with input (k, b), where $k < b$. Because $k > 0$, the **else** clause is executed, and the answer is whatever the algorithm gives as output for inputs $(b \textbf{ mod } k, k)$. Because $b \textbf{ mod } k < k$, the input pair is valid. By our inductive hypothesis, this output is in fact $\gcd(b \textbf{ mod } k, k)$, which equals $\gcd(k, b)$ by Lemma 1 in Section 4.3. 21. If $n = 1$, then $nx = x$, and the algorithm correctly returns x. Assume that the algorithm correctly computes kx. To compute $(k + 1)x$ it recursively computes the product of $k + 1 - 1 = k$ and x, and then adds x. By the inductive hypothesis, it computes that product correctly, so the answer returned is $kx + x = (k+1)x$, which is correct.

23. **procedure** *square*(n: nonnegative integer)
 if $n = 0$ **then return** 0
 else return $square(n - 1) + 2(n - 1) + 1$

Let $P(n)$ be the statement that this algorithm correctly computes n^2. Because $0^2 = 0$, the algorithm works correctly (using the **if** clause) if the input is 0. Assume that the algorithm works correctly for input k. Then for input $k + 1$, it gives as output (because of the **else** clause) its output when the input is k, plus $2(k + 1 - 1) + 1$. By the inductive hypothesis, its output at k is k^2, so its output at $k + 1$ is $k^2 + 2(k + 1 - 1) + 1 = k^2 + 2k + 1 = (k + 1)^2$, as desired.
25. n multiplications versus 2^n 27. $O(\log n)$ versus n

29. **procedure** a(n: nonnegative integer)
 if $n = 0$ **then return** 1
 else if $n = 1$ **then return** 2
 else return $a(n - 1) \cdot a(n - 2)$

31. Iterative

33. **procedure** *iterative*(n: nonnegative integer)
 if $n = 0$ **then** $z := 1$
 else if $n = 1$ **then** $z := 2$
 else
  $x := 1$
  $y := 2$
  $z := 3$
  for $i := 1$ **to** $n - 2$
   $w := x + y + z$
   $x := y$
   $y := z$
   $z := w$
 return z $\{z$ is the nth term of the sequence$\}$

35. We first give a recursive procedure and then an iterative procedure.

procedure r(n: nonnegative integer)
if $n < 3$ **then return** $2n + 1$
else return $r(n - 1) \cdot (r(n - 2))^2 \cdot (r(n - 3))^3$

procedure i(n: nonnegative integer)
if $n = 0$ **then** $z := 1$
else if $n = 1$ **then** $z := 3$
else
 $x := 1$
 $y := 3$
 $z := 5$
 for $i := 1$ **to** $n - 2$
  $w := z \cdot y^2 \cdot x^3$
  $x := y$
  $y := z$
  $z := w$
return z $\{z$ is the nth term of the sequence$\}$

The iterative version is more efficient.

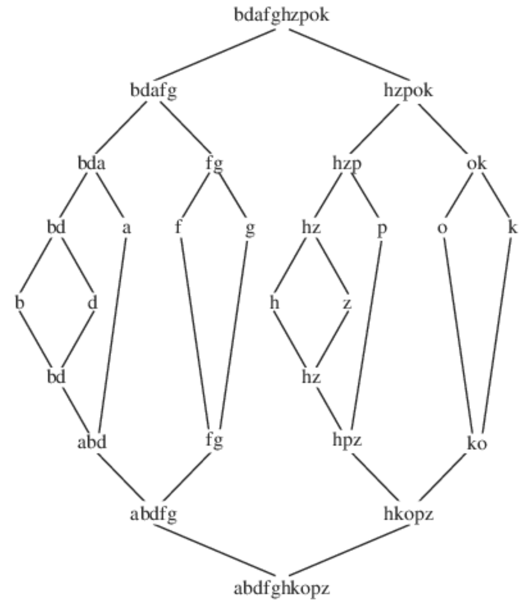
37. **procedure** *reverse*(w: bit string)
 $n :=$ length(w)
 if $n \le 1$ **then return** w
 else return
  $substr(w, n, n) reverse(substr(w, 1, n - 1))$
 $\{substr(w, a, b)$ is the substring of w consisting of
  the symbols in the ath through bth positions$\}$

39. The procedure correctly gives the reversal of λ as λ (basis step), and because the reversal of a string consists of its last character followed by the reversal of its first $n - 1$ characters (see Exercise 35 in Section 5.3), the algorithm behaves correctly when $n > 0$ by the inductive hypothesis. 41. The

algorithm implements the idea of Example 14 in Section 5.1. If $n = 1$ (basis step), place the one right triomino so that its armpit corresponds to the hole in the 2×2 board. If $n > 1$, then divide the board into four boards, each of size $2^{n-1} \times 2^{n-1}$, notice which quarter the hole occurs in, position one right triomino at the center of the board with its armpit in the quarter where the missing square is (see Figure 7 in Section 5.1), and invoke the algorithm recursively four times—once on each of the $2^{n-1} \times 2^{n-1}$ boards, each of which has one square missing (either because it was missing to begin with, or because it is covered by the central triomino).

43. **procedure** $A(m, n$: nonnegative integers)
if $m = 0$ **then return** $2n$
else if $n = 0$ **then return** 0
else if $n = 1$ **then return** 2
else return $A(m - 1, A(m, n - 1))$

45.



47. Let the two lists be $1, 2, \ldots, m - 1, m + n - 1$ and $m, m + 1, \ldots, m + n - 2, m + n$, respectively. 49. If $n = 1$, then the algorithm does nothing, which is correct because a list with one element is already sorted. Assume that the algorithm works correctly for $n = 1$ through $n = k$. If $n = k+1$, then the list is split into two lists, L_1 and L_2. By the inductive hypothesis, *mergesort* correctly sorts each of these sublists; furthermore, *merge* correctly merges two sorted lists into one because with each comparison the smallest element in $L_1 \cup L_2$ not yet put into L is put there. 51. $O(n)$ 53. 6 55. $O(n^2)$

Section 5.5

1. Suppose that $x = 0$. The program segment first assigns the value 1 to y and then assigns the value $x + y = 0 + 1 = 1$ to z. 3. Suppose that $y = 3$. The program segment assigns the value 2 to x and then assigns the value $x + y = 2 + 3 = 5$ to z. Because $y = 3 > 0$ it then assigns the value $z + 1 = 5 + 1 = 6$ to z.

5.
$$\begin{array}{l} (p \wedge \textit{condition}1)\{S_1\}q \\ (p \wedge \neg\textit{condition}1 \wedge \textit{condition}2)\{S_2\}q \\ \quad\vdots \\ (p \wedge \neg\textit{condition}1 \wedge \neg\textit{condition}2 \\ \qquad \cdots \wedge \neg\textit{condition}(n-1)\{S_n\}q \\ \hline \therefore\ p\{\textbf{if } \textit{condition}1 \textbf{ then } S_1; \\ \qquad \textbf{else if } \textit{condition}2 \textbf{ then } S_2; \ldots;\ \textbf{else } S_n\}q \end{array}$$

7. We will show that p : "$\textit{power} = x^{i-1}$ and $i \le n + 1$" is a loop invariant. Note that p is true initially, because before the loop starts, $i = 1$ and $\textit{power} = 1 = x^0 = x^{1-1}$. Next, we must show that if p is true and $i \le n$ after an execution of the loop, then p remains true after one more execution. The loop increments i by 1. Hence, because $i \le n$ before this pass, $i \le n + 1$ after this pass. Also the loop assigns $\textit{power} \cdot x$ to $\textit{power}$. By the inductive hypothesis we see that $\textit{power}$ is assigned the value $x^{i-1} \cdot x = x^i$. Hence, p remains true. Furthermore, the loop terminates after n traversals of the loop with $i = n + 1$ because i is assigned the value 1 prior to entering the loop, is incremented by 1 on each pass, and the loop terminates when $i > n$. Consequently, at termination $\textit{power} = x^n$, as desired. 9. Suppose that p is "m and n are integers." Then if the condition $n < 0$ is true, $a = -n = |n|$ after S_1 is executed. If the condition $n < 0$ is false, then $a = n = |n|$ after S_1 is executed. Hence, $p\{S_1\}q$ is true where q is $p \wedge (a = |n|)$. Because S_2 assigns the value 0 to both k and x, it is clear that $q\{S_2\}r$ is true where r is $q \wedge (k = 0) \wedge (x = 0)$. Suppose that r is true. Let $P(k)$ be "$x = mk$ and $k \le a$." We can show that $P(k)$ is a loop invariant for the loop in S_3. $P(0)$ is true because before the loop is entered $x = 0 = m \cdot 0$ and $0 \le a$. Now assume $P(k)$ is true and $k < a$. Then $P(k + 1)$ is true because x is assigned the value $x + m = mk + m = m(k + 1)$. The loop terminates when $k = a$, and at that point $x = ma$. Hence, $r\{S_3\}s$ is true where s is "$a = |n|$ and $x = ma$." Now assume that s is true. Then if $n < 0$ it follows that $a = -n$, so $x = -mn$. In this case S_4 assigns $-x = mn$ to $\textit{product}$. If $n > 0$ then $x = ma = mn$, so S_4 assigns mn to $\textit{product}$. Hence, $s\{S_4\}t$ is true. 11. Suppose that the initial assertion p is true. Then because $p\{S\}q_0$ is true, q_0 is true after the segment S is executed. Because $q_0 \to q_1$ is true, it also follows that q_1 is true after S is executed. Hence, $p\{S\}q_1$ is true. 13. We will use the proposition p, "$\gcd(a, b) = \gcd(x, y)$ and $y \ge 0$," as the loop invariant. Note that p is true before the loop is entered, because at that point $x = a$, $y = b$, and y is a positive integer, using the initial assertion. Now assume that p is true and $y > 0$; then the loop will be executed again. Inside the loop, x and y are replaced by y and x **mod** y, respectively. By Lemma 1 of Section 4.3, $\gcd(x, y) = \gcd(y, x \textbf{ mod } y)$. Therefore, after execution of the loop, the value of $\gcd(x, y)$ is the same as it was before. Moreover, because y is the remainder, it is at least 0. Hence, p remains true, so it is a loop invariant. Furthermore, if the loop terminates, then $y = 0$. In this case, we have $\gcd(x, y) = x$, the final assertion. Therefore, the program, which gives x as its output, has correctly computed

$\gcd(a, b)$. Finally, we can prove the loop must terminate, because each iteration causes the value of y to decrease by at least 1. Therefore, the loop can be iterated at most b times.

Supplementary Exercises

1. Let $P(n)$ be the statement that this equation holds. *Basis step:* $P(1)$ says $2/3 = 1 - (1/3^1)$, which is true. *Inductive step:* Assume that $P(k)$ is true. Then $2/3 + 2/9 + 2/27 + \cdots + 2/3^n + 2/3^{n+1} = 1 - 1/3^n + 2/3^{n+1}$ (by the inductive hypothesis), and this equals $1 - 1/3^{n+1}$, as desired. **3.** Let $P(n)$ be "$1 \cdot 1 + 2 \cdot 2 + \cdots + n \cdot 2^{n-1} = (n-1)2^n + 1$." *Basis step:* $P(1)$ is true because $1 \cdot 1 = 1 = (1-1)2^1 + 1$. *Inductive step:* Assume that $P(k)$ is true. Then $1 \cdot 1 + 2 \cdot 2 + \cdots + k \cdot 2^{k-1} + (k+1) \cdot 2^k = (k-1)2^k + 1 + (k+1)2^k = 2k \cdot 2^k + 1 = [(k+1) - 1]2^{k+1} + 1$. **5.** Let $P(n)$ be "$1/(1 \cdot 4) + \cdots + 1/[(3n-2)(3n+1)] = n/(3n+1)$." *Basis step:* $P(1)$ is true because $1/(1 \cdot 4) = 1/4$. *Inductive step:* Assume $P(k)$ is true. Then $1/(1 \cdot 4) + \cdots + 1/[(3k-2)(3k+1)] + 1/[(3k+1)(3k+4)] = k/(3k+1) + 1/[(3k+1)(3k+4)] = [k(3k+4)+1]/[(3k+1)(3k+4)] = [(3k+1)(k+1)]/[(3k+1)(3k+4)] = (k+1)/(3k+4)$. **7.** Let $P(n)$ be "$2^n > n^3$." *Basis step:* $P(10)$ is true because $1024 > 1000$. *Inductive step:* Assume $P(k)$ is true. Then $(k+1)^3 = k^3 + 3k^2 + 3k + 1 \le k^3 + 9k^2 \le k^3 + k^3 = 2k^3 < 2 \cdot 2^k = 2^{k+1}$. **9.** Let $P(n)$ be "$a - b$ is a factor of $a^n - b^n$." *Basis step:* $P(1)$ is trivially true. Assume $P(k)$ is true. Then $a^{k+1} - b^{k+1} = a^{k+1} - ab^k + ab^k - b^{k+1} = a(a^k - b^k) + b^k(a-b)$. Then because $a - b$ is a factor of $a^k - b^k$ and $a - b$ is a factor of $a - b$, it follows that $a - b$ is a factor of $a^{k+1} - b^{k+1}$. **11.** *Basis step:* When $n = 1$, $6^{n+1} + 7^{2n-1} = 36 + 7 = 43$. *Inductive step:* Assume the inductive hypothesis, that 43 divides $6^{n+1} + 7^{2n-1}$; we must show that 43 divides $6^{n+2} + 7^{2n+1}$. We have $6^{n+2} + 7^{2n+1} = 6 \cdot 6^{n+1} + 49 \cdot 7^{2n-1} = 6 \cdot 6^{n+1} + 6 \cdot 7^{2n-1} + 43 \cdot 7^{2n-1} = 6(6^{n+1} + 7^{2n-1}) + 43 \cdot 7^{2n-1}$. By the inductive hypothesis the first term is divisible by 43, and the second term is clearly divisible by 43; therefore the sum is divisible by 43. **13.** Let $P(n)$ be "$a + (a+d) + \cdots + (a+nd) = (n+1)(2a+nd)/2$." *Basis step:* $P(1)$ is true because $a + (a+d) = 2a + d = 2(2a+d)/2$. *Inductive step:* Assume that $P(k)$ is true. Then $a + (a+d) + \cdots + (a+kd) + [a + (k+1)d] = (k+1)(2a+kd)/2 + a + (k+1)d = \frac{1}{2}(2ak + 2a + k^2d + kd + 2a + 2kd + 2d) = \frac{1}{2}(2ak + 4a + k^2d + 3kd + 2d) = \frac{1}{2}(k+2)[2a + (k+1)d]$. **15.** *Basis step:* This is true for $n = 1$ because $5/6 = 10/12$. *Inductive step:* Assume that the equation holds for $n = k$, and consider $n = k+1$. Then $\sum_{i=1}^{k+1} \frac{i+4}{i(i+1)(i+2)} = \sum_{i=1}^{k} \frac{i+4}{i(i+1)(i+2)} + \frac{k+5}{(k+1)(k+2)(k+3)} = \frac{k(3k+7)}{2(k+1)(k+2)} + \frac{k+5}{(k+1)(k+2)(k+3)}$ (by the inductive hypothesis) $= \frac{1}{(k+1)(k+2)} \cdot (\frac{k(3k+7)}{2} + \frac{k+5}{k+3}) = \frac{1}{2(k+1)(k+2)(k+3)} \cdot [k(3k+7)(k+3) + 2(k+5)] = \frac{1}{2(k+1)(k+2)(k+3)} \cdot (3k^3 + 16k^2 + 23k + 10) = \frac{1}{2(k+1)(k+2)(k+3)} \cdot (3k+10)(k+1)^2 = \frac{1}{2(k+2)(k+3)} \cdot (3k+10)(k+1) = \frac{(k+1)(3(k+1)+7)}{2((k+1)+1)((k+1)+2)}$, as desired. **17.** *Basis step:* The statement is true for $n = 1$ because the derivative of $g(x) = xe^x$ is $x \cdot e^x + e^x = (x+1)e^x$ by the product rule. *Inductive step:* Assume that the statement is true for $n = k$, i.e., the kth derivative is given by $g^{(k)} = (x+k)e^x$. Differentiating by the product rule gives the $(k+1)$st derivative: $g^{(k+1)} = (x+k)e^x + e^x = [x + (k+1)]e^x$, as desired. **19.** We will use strong induction to show that f_n is even if $n \equiv 0 \pmod 3$ and is odd otherwise. *Basis step:* This follows because $f_0 = 0$ is even and $f_1 = 1$ is odd. *Inductive step:* Assume that if $j \le k$, then f_j is even if $j \equiv 0 \pmod 3$ and is odd otherwise. Now suppose $k + 1 \equiv 0 \pmod 3$. Then $f_{k+1} = f_k + f_{k-1}$ is even because f_k and f_{k-1} are both odd. If $k + 1 \equiv 1 \pmod 3$, then $f_{k+1} = f_k + f_{k-1}$ is odd because f_k is even and f_{k-1} is odd. Finally, if $k + 1 \equiv 2 \pmod 3$, then $f_{k+1} = f_k + f_{k-1}$ is odd because f_k is odd and f_{k-1} is even. **21.** Let $P(n)$ be the statement that $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$ for every nonnegative integer k. *Basis step:* This consists of showing that $P(0)$ and $P(1)$ both hold. $P(0)$ is true because $f_k f_0 + f_{k+1} f_1 = f_{k+1} \cdot 0 + f_{k+1} \cdot 1 = f_1$. Because $f_k f_1 + f_{k+1} f_2 = f_k + f_{k+1} = f_{k+2}$, it follows that $P(1)$ is true. *Inductive step:* Now assume that $P(j)$ holds. Then, by the inductive hypothesis and the recursive definition of the Fibonacci numbers, it follows that $f_{k+1} f_{j+1} + f_{k+2} f_{j+2} = f_k(f_{j-1} + f_j) + f_{k+1}(f_j + f_{j+1}) = (f_k f_{j-1} + f_{k+1} f_j) + (f_k f_j + f_{k+1} f_{j+1}) = f_{j-1+k+1} + f_{j+k+1} = f_{j+k+2}$. This shows that $P(j+1)$ is true. **23.** Let $P(n)$ be the statement $l_0^2 + l_1^2 + \cdots + l_n^2 = l_n l_{n+1} + 2$. *Basis step:* $P(0)$ and $P(1)$ both hold because $l_0^2 = 2^2 = 2 \cdot 1 + 2 = l_0 l_1 + 2$ and $l_0^2 + l_1^2 = 2^2 + 1^2 = 1 \cdot 3 + 2 = l_1 l_3 + 2$. *Inductive step:* Assume that $P(k)$ holds. Then by the inductive hypothesis $l_0^2 + l_1^2 + \cdots + l_k^2 + l_{k+1}^2 = l_k l_{k+1} + 2 + l_{k+1}^2 = l_{k+1}(l_k + l_{k+1}) + 2 = l_{k+1} l_{k+2} + 2$. This shows that $P(k+1)$ holds. **25.** Let $P(n)$ be the statement that the identity holds for the integer n. *Basis step:* $P(1)$ is obviously true. *Inductive step:* Assume that $P(k)$ is true. Then $\cos((k+1)x) + i\sin((k+1)x) = \cos(kx + x) + i\sin(kx + x) = \cos kx \cos x - \sin kx \sin x + i(\sin kx \cos x + \cos kx \sin x) = \cos x(\cos kx + i \sin kx)(\cos x + i \sin x) = (\cos x + i \sin x)^k(\cos x + i \sin x) = (\cos x + i \sin x)^{k+1}$. It follows that $P(k+1)$ is true. **27.** Rewrite the right-hand side as $2^{n+1}(n^2 - 2n + 3) - 6$. For $n = 1$ we have $2 = 4 \cdot 2 - 6$. Assume that the equation holds for $n = k$, and consider $n = k+1$. Then $\sum_{j=1}^{k+1} j^2 2^j = \sum_{j=1}^{k} j^2 2^j + (k+1)^2 2^{k+1} = 2^{k+1}(k^2 - 2k + 3) - 6 + (k^2 + 2k + 1)2^{k+1}$ (by the inductive hypothesis) $= 2^{k+1}(2k^2 + 4) - 6 = 2^{k+2}(k^2 + 2) - 6 = 2^{k+2}[(k+1)^2 - 2(k+1) + 3] - 6$. **29.** Let $P(n)$ be the statement that this equation holds. *Basis step:* In $P(2)$ both sides reduce to $1/3$. *Inductive step:* Assume that $P(k)$ is true. Then $\sum_{j=1}^{k+1} 1/(j^2 - 1) = \left(\sum_{j=1}^{k} 1/(j^2 - 1)\right) + 1/[(k+1)^2 - 1] = (k-1)(3k+2)/[4k(k+1)] + 1/[(k+1)^2 - 1]$ by the inductive hypothesis. This simplifies to $(k-1)(3k+2)/[4k(k+1)] + 1/(k^2 + 2k) = (3k^3 + 5k^2)/[4k(k+1)(k+2)] = \{[(k+1) - 1][3(k+1) + 2]\}/[4(k+1)(k+2)]$, which is exactly what $P(k+1)$ asserts. **31.** Let $P(n)$ be the assertion that at least $n + 1$ lines are needed to cover the lattice points in the given triangular region. *Basis step:* $P(0)$ is true, because we need at least one line to cover the one point at $(0, 0)$. *Inductive step:* Assume the inductive hypothesis, that at least $k + 1$ lines are needed to cover the lattice points with $x \geq 0$, $y \geq 0$, and $x + y \leq k$. Consider the triangle of lattice points defined by $x \geq 0$, $y \geq 0$, and $x + y \leq k + 1$. By way of contradiction, assume that $k + 1$ lines could cover this set. Then these lines must cover the $k + 2$ points on the line $x + y = k + 1$. But only the line $x + y = k + 1$ itself can cover more than one of these points, because two distinct lines intersect in at most one point. Therefore none of the $k + 1$ lines that are needed (by the inductive hypothesis) to cover the set of lattice points within the triangle but not on this line can cover more than one of the points on this line, and this leaves at least one point uncovered. Therefore our assumption that $k + 1$ lines could cover the larger set is wrong, and our proof is complete. **33.** Let $P(n)$ be $\mathbf{B}^k = \mathbf{M}\mathbf{A}^k\mathbf{M}^{-1}$. *Basis step:* Part of the given conditions. *Inductive step:* Assume the inductive hypothesis. Then $\mathbf{B}^{k+1} = \mathbf{B}\mathbf{B}^k = \mathbf{M}\mathbf{A}\mathbf{M}^{-1}\mathbf{B}^k = \mathbf{M}\mathbf{A}\mathbf{M}^{-1}\mathbf{M}\mathbf{A}^k\mathbf{M}^{-1}$ (by the inductive hypothesis) $= \mathbf{M}\mathbf{A}\mathbf{I}\mathbf{A}^k\mathbf{M}^{-1} = \mathbf{M}\mathbf{A}\mathbf{A}^k\mathbf{M}^{-1} = \mathbf{M}\mathbf{A}^{k+1}\mathbf{M}^{-1}$. **35.** We prove by mathematical induction the following stronger statement: For every $n \geq 3$, we can write $n!$ as the sum of n of its distinct positive divisors, one of which is 1. That is, we can write $n! = a_1 + a_2 + \cdots + a_n$, where each a_i is a divisor of $n!$, the divisors are listed in strictly decreasing order, and $a_n = 1$. *Basis step:* $3! = 3 + 2 + 1$. *Inductive step:* Assume that we can write $k!$ as a sum of the desired form, say $k! = a_1 + a_2 + \cdots + a_k$, where each a_i is a divisor of $n!$, the divisors are listed in strictly decreasing order, and $a_n = 1$. Consider $(k + 1)!$. Then we have $(k + 1)! = (k + 1)k! = (k + 1)(a_1 + a_2 + \cdots + a_k) = (k + 1)a_1 + (k + 1)a_2 + \cdots + (k + 1)a_k = (k + 1)a_1 + (k + 1)a_2 + \cdots + k \cdot a_k + a_k$. Because each a_i was a divisor of $k!$, each $(k + 1)a_i$ is a divisor of $(k + 1)!$. Furthermore, $k \cdot a_k = k$, which is a divisor of $(k + 1)!$, and $a_k = 1$, so the new last summand is again 1. (Notice also that our list of summands is still in strictly decreasing order.) Thus we have written $(k + 1)!$ in the desired form. **37.** When $n = 1$ the statement is vacuously true. Assume that the statement is true for $n = k$, and consider $k + 1$ people standing in a line, with a woman first and a man last. If the kth person is a woman, then we have that woman standing in front of the man at the end. If the kth person is a man, then the first k people in line satisfy the conditions of the inductive hypothesis for the first k people in line, so again we can conclude that there is a woman directly in front of a man somewhere in the line. **39.** *Basis step:* When $n = 1$ there is one circle, and we can color the inside blue and the outside red to satisfy the conditions. *Inductive step:* Assume the inductive hypothesis that if there are k circles, then the regions can be 2-colored such that no regions with a common boundary have the same color, and consider a situation with $k + 1$ circles. Remove one of the circles, producing a picture with k circles, and invoke the inductive hypothesis to color it in the prescribed manner. Then replace the removed circle and change the color of every region inside this circle. The resulting figure satisfies the condition, because if two regions have a common boundary, then either that boundary involved the new circle, in which case the regions on either side used to be the same region and now the inside portion is different from the outside, or else the boundary did not involve the new circle, in which case the regions are colored differently because they were colored differently before the new circle was restored. **41.** If $n = 1$ then the equation reads $1 \cdot 1 = 1 \cdot 2/2$, which is true. Assume that the equation is true for n and consider it for $n + 1$. Then $\sum_{j=1}^{n+1}(2j - 1)\left(\sum_{k=j}^{n+1} \frac{1}{k}\right) = \sum_{j=1}^{n}(2j - 1)\left(\sum_{k=j}^{n+1} \frac{1}{k}\right) + [2(n + 1) - 1] \cdot \frac{1}{n+1} = \sum_{j=1}^{n}(2j - 1)\left(\frac{1}{n+1} + \sum_{k=j}^{n} \frac{1}{k}\right) + \frac{2n+1}{n+1} = \left(\frac{1}{n+1}\sum_{j=1}^{n}(2j - 1)\right) + \left(\sum_{j=1}^{n}(2j - 1)\sum_{k=j}^{n} \frac{1}{k}\right) + \frac{2n+1}{n+1} = \left(\frac{1}{n+1} \cdot n^2\right) + \frac{n(n+1)}{2} + \frac{2n+1}{n+1}$ (by the inductive hypothesis) $= \frac{2n^2+n(n+1)^2+(4n+2)}{2(n+1)} = \frac{2(n+1)^2+n(n+1)^2}{2(n+1)} = \frac{(n+1)(n+2)}{2}$. **43.** Let $T(n)$ be the statement that the sequence of towers of 2 is eventually constant modulo n. We use strong induction to prove that $T(n)$ is true for all positive integers n. *Basis step:* When $n = 1$ (and $n = 2$), the sequence of towers of 2 modulo n is the sequence of all 0s. *Inductive step:* Suppose that k is an integer with $k \geq 2$. Suppose that $T(j)$ is true for $1 \leq j \leq k - 1$. In the proof of the inductive step we denote the rth term of the sequence modulo n by a_r. First suppose k is even. Let $k = 2^s q$ where $s \geq 1$ and $q < k$ is odd. When j is large enough, $a_{j-2} \geq s$, and for such j, $a_j = 2^{2^{a_{j-2}}}$ is a multiple of 2^s. It follows that for sufficiently large j, $a_j \equiv 0 \pmod{2^s}$. Hence, for large enough i, 2^s divides $a_{i+1} - a_i$. By the inductive hypothesis $T(q)$ is true, so the sequence $a_1, a_2, a_3, \ldots$ is eventually constant modulo q. This implies that for large enough i, q divides $a_{i+1} - a_i$. Because $\gcd(q, 2^s) = 1$ and for sufficiently large i both q and 2^s divide $a_{i+1} - a_i$, $k = 2^s q$ divides $a_{i+1} - a_i$ for sufficiently large i. Hence, for sufficiently large i, $a_{i+1} - a_i \equiv 0 \pmod{k}$. This means that the sequence is eventually constant modulo k. Finally, suppose k is odd. Then $\gcd(2, k) = 1$, so by Euler's theorem (found in elementary number theory books, such as [Ro10]), we know that $2^{\phi(k)} \equiv 1 \pmod{k}$. Let $r = \phi(k)$. Because $r < k$, by the inductive hypothesis $T(r)$, the sequence $a_1, a_2, a_3, \ldots$ is eventually constant modulo r, say equal to c. Hence for large enough i, for some integer t_i, $a_i = t_i r + c$. Hence $a_{i+1} = 2^{a_i} = 2^{t_i r + c} = (2^r)^{t_i} 2^c \equiv 2^c \pmod{k}$. This shows that $a_1, a_2, \ldots$ is eventually constant modulo k. **45. a)** 92 **b)** 91 **c)** 91 **d)** 91 **e)** 91 **f)** 91 **47.** The basis step is incorrect because $n \neq 1$ for the sum shown. **49.** Let $P(n)$ be "the plane is divided into $n^2 - n + 2$ regions by n circles if every two of these circles have two common points but no three have a common point." *Basis step:* $P(1)$ is true because a circle divides the plane into $2 = 1^2 - 1 + 2$ regions. *Inductive step:* Assume that $P(k)$ is true, that is, k circles with the specified properties divide the plane into $k^2 - k + 2$ regions. Suppose that a $(k + 1)$st circle is added. This circle intersects each of the other k circles in two points, so these points of intersection form $2k$ new arcs, each of which splits an old region. Hence, there are $2k$ regions split, which shows that there are $2k$ more regions than there were previously. Hence, $k + 1$ circles satisfying the specified properties divide the plane into $k^2 - k + 2 + 2k = (k^2 + 2k + 1) - (k + 1) + 2 = (k + 1)^2 - (k + 1) + 2$ regions. **51.** Suppose $\sqrt{2}$ were rational. Then $\sqrt{2} = a/b$, where a and b are positive integers. It follows that the set $S = \{n\sqrt{2} \mid n \in \mathbf{N}\} \cap \mathbf{N}$ is a nonempty set of positive integers, because $b\sqrt{2} = a$ belongs to S. Let t be the least element of S, which exists by the well-ordering property. Then $t = s\sqrt{2}$ for some integer s. We have $t - s = s\sqrt{2} - s = s(\sqrt{2} - 1)$, so $t - s$ is a positive integer because $\sqrt{2} > 1$. Hence, $t - s$ belongs to S. This is a contradiction because $t - s = s\sqrt{2} - s < s$. Hence, $\sqrt{2}$ is irrational. **53.** **a)** Let $d = \gcd(a_1, a_2, \ldots, a_n)$. Then d is a divisor of each a_i and so must be a divisor of $\gcd(a_{n-1}, a_n)$. Hence, d is a common divisor of $a_1, a_2, \ldots, a_{n-2}$, and $\gcd(a_{n-1}, a_n)$. To show that it is the greatest common divisor of these numbers, suppose that c is a common divisor of them. Then c is a divisor of a_i for $i = 1, 2, \ldots, n - 2$ and a divisor of $\gcd(a_{n-1}, a_n)$, so it is a divisor of a_{n-1} and a_n. Hence, c is a common divisor of $a_1, a_2, \ldots, a_{n-1}$, and a_n. Hence, it is a divisor of d, the greatest common divisor of $a_1, a_2, \ldots, a_n$. It follows that d is the greatest common divisor, as claimed. **b)** If $n = 2$, apply the Euclidean algorithm. Otherwise, apply the Euclidean algorithm to a_{n-1} and a_n, obtaining $d = \gcd(a_{n-1}, a_n)$, and then apply the algorithm recursively to $a_1, a_2, \ldots, a_{n-2}, d$. **55.** $f(n) = n^2$. Let $P(n)$ be "$f(n) = n^2$." *Basis step:* $P(1)$ is true because $f(1) = 1 = 1^2$, which follows from the definition of f. *Inductive step:* Assume $f(n) = n^2$. Then $f(n+1) = f((n+1) - 1) + 2(n+1) - 1 = f(n) + 2n + 1 = n^2 + 2n + 1 = (n + 1)^2$. **57.** **a)** λ, 0, 1, 00, 01, 11, 000, 001, 011, 111, 0000, 0001, 0011, 0111, 1111, 00000, 00001, 00011, 00111, 01111, 11111 **b)** $S = \{\alpha\beta \mid \alpha$ is a string of m 0s and β is a string of n 1s, $m \geq 0, n \geq 0\}$ **59.** Apply the first recursive step to λ to get () $\in B$. Apply the second recursive step to this string to get ()() $\in B$. Apply the first recursive step to this string to get (()()) $\in B$. By Exercise 62, (())) is not in B because the number of left parentheses does not equal the number of right parentheses. **61.** λ, (), (()), ()() **63.** **a)** 0 **b)** -2 **c)** 2 **d)** 0

65.

procedure *generate*(n: nonnegative integer)
if n is odd **then**
  $S := S(n - 1)$ {the S constructed by *generate*$(n - 1)$}
  $T := T(n - 1)$ {the T constructed by *generate*$(n - 1)$}
else if $n = 0$ **then**
  $S := \emptyset$
  $T := \{\lambda\}$
else
  $S' := S(n - 2)$ {the S constructed by *generate*$(n - 2)$}
  $T' := T(n - 2)$ {the T constructed by *generate*$(n - 2)$}
  $T := T' \cup \{(x) \mid x \in T' \cup S' \wedge \text{length}(x) = n - 2\}$
  $S := S' \cup \{xy \mid x \in T' \wedge y \in T' \cup S' \wedge \text{length}(xy) = n\}$
$\{T \cup S$ is the set of balanced strings of length at most $n\}$

67. If $x \leq y$ initially, then $x := y$ is not executed, so $x \leq y$ is a true final assertion. If $x > y$ initially, then $x := y$ is executed, so $x \leq y$ is again a true final assertion.
69. **procedure** *zerocount*$(a_1, a_2, \ldots, a_n$: list of integers)
  if $n = 1$ **then**
    if $a_1 = 0$ **then return** 1
    else return 0
  else
    if $a_n = 0$ **then return** *zerocount*$(a_1, a_2, \ldots, a_{n-1}) + 1$
    else return *zerocount*$(a_1, a_2, \ldots, a_{n-1})$

71. We will prove that $a(n)$ is a natural number and $a(n) \leq n$. This is true for the base case $n = 0$ because $a(0) = 0$. Now assume that $a(n-1)$ is a natural number and $a(n-1) \leq n-1$. Then $a(a(n-1))$ is a applied to a natural number less than or equal to $n - 1$. Hence, $a(a(n-1))$ is also a natural number minus than or equal to $n - 1$. Therefore, $n - a(a(n-1))$ is n minus some natural number less than or equal to $n-1$, which is a natural number less than or equal to n. **73.** From Exercise 72, $a(n) = \lfloor (n+1)\mu \rfloor$ and $a(n-1) = \lfloor n\mu \rfloor$. Because $\mu < 1$, these two values are equal or they differ by 1. First suppose that $\mu n - \lfloor \mu n \rfloor < 1 - \mu$. This is equivalent to $\mu(n+1) < 1 + \lfloor \mu n \rfloor$. If this is true, then $\lfloor \mu(n + 1) \rfloor = \lfloor \mu n \rfloor$. On the other hand, if $\mu n - \lfloor \mu n \rfloor \geq 1 - \mu$, then $\mu(n + 1) \geq 1 + \lfloor \mu n \rfloor$, so $\lfloor \mu(n + 1) \rfloor = \lfloor \mu n \rfloor + 1$, as desired. **75.** $f(0) = 1$, $m(0) = 0$; $f(1) = 1$, $m(1) = 0$; $f(2) = 2$, $m(2) = 1$; $f(3) = 2$, $m(3) = 2$; $f(4) = 3$, $m(4) = 2$; $f(5) = 3$, $m(5) = 3$; $f(6) = 4$, $m(6) = 4$; $f(7) = 5$, $m(7) = 4$; $f(8) = 5$, $m(8) = 5$; $f(9) = 6$, $m(9) = 6$ **77.** The last occurrence of n is in the position for which the total number of 1s, 2s, $\ldots$, ns all together is that position number. But because a_k is the number of occurrences of k, this is just $\sum_{k=1}^{n} a_k$, as desired. Because $f(n)$ is the sum of the first n terms of the sequence, $f(f(n))$ is the sum of the first $f(n)$ terms of the sequence. But because $f(n)$ is the last term whose value is n, this means that the sum is the sum of all terms of the sequence whose value is at most n. Because there are a_k terms of the sequence whose value is k, this sum is $\sum_{k=1}^{n} k \cdot a_k$, as desired

CHAPTER 6

Section 6.1

1. **a)** 5850 **b)** 343 **3.** **a)** 4^{10} **b)** 5^{10} **5.** 42 **7.** 26^3 **9.** 676 **11.** 2^8 **13.** $n + 1$ (counting the empty string) **15.** 475,255 (counting the empty string) **17.** 1,321,368,961 **19.** **a)** 729 **b)** 256 **c)** 1024 **d)** 64 **21.** **a)** Seven: 56, 63, 70, 77, 84, 91, 98 **b)** Five: 55, 66, 77, 88, 99 **c)** One: 77 **23.** **a)** 128 **b)** 450 **c)** 9 **d)** 675 **e)** 450 **f)** 450 **g)** 225 **h)** 75 **25.** **a)** 990 **b)** 500 **c)** 27 **27.** 3^{50} **29.** 52,457,600 **31.** 20,077,200 **33.** **a)** 37,822,859,361 **b)** 8,204,716,800 **c)** 40,159,050, 880 **d)** 12,113,640,000 **e)** 171,004,205,215 **f)** 72,043,541,640 **g)** 6,230,721,635 **h)** 223,149,655 **35.** **a)** 0 **b)** 120 **c)** 720 **d)** 2520 **37.** **a)** 2 if $n = 1$, 2 if $n = 2$, 0 if $n \geq 3$ **b)** 2^{n-2} for $n > 1$; 1 if $n = 1$ **c)** $2(n - 1)$ **39.** $(n + 1)^m$ **41.** If n is even, $2^{n/2}$; if n is odd, $2^{(n+1)/2}$ **43.** **a)** 175 **b)** 248 **c)** 232 **d)** 84 **45.** 60 **47.** **a)** 240 **b)** 480 **c)** 360 **49.** 352 **51.** 147 **53.** 33 **55.** **a)** 9,920,671,339,261,325,541,376 $\approx 9.9 \times 10^{21}$ **b)** 6,641,514,961,387,068,437,760 $\approx 6.6 \times 10^{21}$ **c)** About 314,000 years **57.** $54(64^{65536} - 1)/63$

59. 7,104,000,000,000 **61.** $16^{10} + 16^{26} + 16^{58}$ **63.** 666,667 **65.** 18 **67.** 17 **69.** 22 **71.** Let $P(m)$ be the sum rule for m tasks. For the basis case take $m = 2$. This is just the sum rule for two tasks. Now assume that $P(m)$ is true. Consider $m + 1$ tasks, $T_1, T_2, \ldots, T_m, T_{m+1}$, which can be done in $n_1, n_2, \ldots, n_m, n_{m+1}$ ways, respectively, such that no two of these tasks can be done at the same time. To do one of these tasks, we can either do one of the first m of these or do task T_{m+1}. By the sum rule for two tasks, the number of ways to do this is the sum of the number of ways to do one of the first m tasks, plus n_{m+1}. By the inductive hypothesis, this is $n_1 + n_2 + \cdots + n_m + n_{m+1}$, as desired. **73.** $n(n-3)/2$

Section 6.2

1. Because there are six classes, but only five weekdays, the pigeonhole principle shows that at least two classes must be held on the same day. **3.** **a)** 3 **b)** 14 **5.** Because there are four possible remainders when an integer is divided by 4, the pigeonhole principle implies that given five integers, at least two have the same remainder. **7.** Let $a, a+1, \ldots, a+n-1$ be the integers in the sequence. The integers $(a+i)$ **mod** n, $i = 0, 1, 2, \ldots, n-1$, are distinct, because $0 < (a+j) - (a+k) < n$ whenever $0 \le k < j \le n-1$. Because there are n possible values for $(a+i)$ **mod** n and there are n different integers in the set, each of these values is taken on exactly once. It follows that there is exactly one integer in the sequence that is divisible by n. **9.** 4951 **11.** The midpoint of the segment joining the points (a, b, c) and (d, e, f) is $((a+d)/2, (b+e)/2, (c+f)/2)$. It has integer coefficients if and only if a and d have the same parity, b and e have the same parity, and c and f have the same parity. Because there are eight possible triples of parity [such as (*even*, *odd*, *even*)], by the pigeonhole principle at least two of the nine points have the same triple of parities. The midpoint of the segment joining two such points has integer coefficients. **13.** **a)** Group the first eight positive integers into four subsets of two integers each so that the integers of each subset add up to 9: $\{1, 8\}$, $\{2, 7\}$, $\{3, 6\}$, and $\{4, 5\}$. If five integers are selected from the first eight positive integers, by the pigeonhole principle at least two of them come from the same subset. Two such integers have a sum of 9, as desired. **b)** No. Take $\{1, 2, 3, 4\}$, for example. **15.** 4 **17.** 21,251 **19.** **a)** If there were fewer than 9 freshmen, fewer than 9 sophomores, and fewer than 9 juniors in the class, there would be no more than 8 with each of these three class standings, for a total of at most 24 students, contradicting the fact that there are 25 students in the class. **b)** If there were fewer than 3 freshmen, fewer than 19 sophomores, and fewer than 5 juniors, then there would be at most 2 freshmen, at most 18 sophomores, and at most 4 juniors, for a total of at most 24 students. This contradicts the fact that there are 25 students in the class. **21.** 4, 3, 2, 1, 8, 7, 6, 5, 12, 11, 10, 9, 16, 15, 14, 13 **23.** Number the seats around the table from 1 to 50, and think of seat 50 as being adjacent to seat 1. There are 25 seats with odd numbers and 25 seats with even numbers. If no more than 12 boys occupied the odd-numbered seats, then at least 13 boys would occupy the even-numbered seats, and vice versa. Without loss of generality, assume that at least 13 boys occupy the 25 odd-numbered seats. Then at least two of those boys must be in consecutive odd-numbered seats, and the person sitting between them will have boys as both of his or her neighbors.

25.
```
procedure long(a_1, ..., a_n: positive integers)
{first find longest increasing subsequence}
max := 0; set := 00...00 {n bits}
for i := 1 to 2^n
  last := 0; count := 0, OK := true
  for j := 1 to n
    if set(j) = 1 then
      if a_j > last then last := a_j
      count := count + 1
    else OK := false
  if count > max then
    max := count
    best := set
  set := set + 1 (binary addition)
{max is length and best indicates the sequence}
{repeat for decreasing subsequence with only
   changes being a_j < last instead of a_j > last
   and last := ∞ instead of last := 0}
```

27. By symmetry we need prove only the first statement. Let A be one of the people. Either A has at least four friends, or A has at least six enemies among the other nine people (because $3 + 5 < 9$). Suppose, in the first case, that B, C, D, and E are all A's friends. If any two of these are friends with each other, then we have found three mutual friends. Otherwise $\{B, C, D, E\}$ is a set of four mutual enemies. In the second case, let $\{B, C, D, E, F, G\}$ be a set of enemies of A. By Example 11, among B, C, D, E, F, and G there are either three mutual friends or three mutual enemies, who form, with A, a set of four mutual enemies. **29.** We need to show two things: that if we have a group of n people, then among them we must find either a pair of friends or a subset of n of them all of whom are mutual enemies; and that there exists a group of $n-1$ people for which this is not possible. For the first statement, if there is any pair of friends, then the condition is satisfied, and if not, then every pair of people are enemies, so the second condition is satisfied. For the second statement, if we have a group of $n-1$ people all of whom are enemies of each other, then there is neither a pair of friends nor a subset of n of them all of whom are mutual enemies. **31.** There are 6,432,816 possibilities for the three initials and a birthday. So, by the generalized pigeonhole principle, there are at least $\lceil 37{,}000{,}000/6{,}432{,}816 \rceil = 6$ people who share the same initials and birthday. **33.** Because $800{,}001 > 200{,}000$, the pigeonhole principle guarantees that there are at least two Parisians with the same number of hairs on their heads. The generalized pigeonhole principle guarantees that there are at least $\lceil 800{,}001/200{,}000 \rceil = 5$ Parisians with the same number of hairs on their heads. **35.** 18 **37.** Because there are six computers, the number of other computers a computer is connected to is an integer between 0 and 5, inclusive. However, 0 and 5 cannot both occur. To see this, note that if some computer is connected to no others, then no computer is connected to all five others, and if some computer is connected to all five others, then no computer is connected to no others. Hence, by the pigeonhole principle, because there are at most five possibilities for the number of computers a computer is connected to, there are at least two computers in the set of six connected to the same number of others. **39.** Label the computers C_1 through C_{100}, and label the printers P_1 through P_{20}. If we connect C_k to P_k for $k = 1, 2, \ldots, 20$ and connect each of the computers C_{21} through C_{100} to *all* the printers, then we have used a total of $20 + 80 \cdot 20 = 1620$ cables. Clearly this is sufficient, because if computers C_1 through C_{20} 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, because they are connected to all the printers. Now we must show that 1619 cables is not enough. Because there are 1619 cables and 20 printers, the average number of computers per printer is 1619/20, which is less than 81. Therefore some printer must be connected to fewer than 81 computers. That means it is connected to 80 or fewer computers, so there are 20 computers that are not connected to it. If those 20 computers all needed a printer simultaneously, then they would be out of luck, because they are connected to at most the 19 other printers. **41.** Let a_i be the number of matches completed by hour i. Then $1 \le a_1 < a_2 < \cdots < a_{75} \le 125$. Also $25 \le a_1 + 24 < a_2 + 24 < \cdots < a_{75} + 24 \le 149$. There are 150 numbers $a_1, \ldots, a_{75}, a_1 + 24, \ldots, a_{75} + 24$. By the pigeonhole principle, at least two are equal. Because all the a_is are distinct and all the $(a_i + 24)$s are distinct, it follows that $a_i = a_j + 24$ for some $i > j$. Thus, in the period from the $(j + 1)$st to the ith hour, there are exactly 24 matches. **43.** Use the generalized pigeonhole principle, placing the $|S|$ objects $f(s)$ for $s \in S$ in $|T|$ boxes, one for each element of T. **45.** Let d_j be $jx - N(jx)$, where $N(jx)$ is the integer closest to jx for $1 \le j \le n$. Each d_j is an irrational number between $-1/2$ and $1/2$. We will assume that n is even; the case where n is odd is messier. Consider the n intervals $\{x \mid j/n < x < (j + 1)/n\}$, $\{x \mid -(j + 1)/n < x < -j/n\}$ for $j = 0, 1, \ldots, (n/2) - 1$. If d_j belongs to the interval $\{x \mid 0 < x < 1/n\}$ or to the interval $\{x \mid -1/n < x < 0\}$ for some j, we are done. If not, because there are $n - 2$ intervals and n numbers d_j, the pigeonhole principle tells us that there is an interval $\{x \mid (k - 1)/n < x < k/n\}$ containing d_r and d_s with $r < s$. The proof can be finished by showing that $(s - r)x$ is within $1/n$ of its nearest integer. **47. a)** Assume that $i_k \le n$ for all k. Then by the generalized pigeonhole principle, at least $\lceil (n^2 + 1)/n \rceil = n + 1$ of the numbers $i_1, i_2, \ldots, i_{n^2+1}$ are equal. **b)** If $a_{k_j} < a_{k_{j+1}}$, then the subsequence consisting of a_{k_j} followed by the increasing subsequence of length $i_{k_{j+1}}$ starting at $a_{k_{j+1}}$ contradicts the fact that $i_{k_j} = i_{k_{j+1}}$. Hence, $a_{k_j} > a_{k_{j+1}}$. **c)** If there is no increasing subsequence of length greater than n, then parts (a) and (b) apply. Therefore, we have $a_{k_{n+1}} > a_{k_n} > \cdots > a_{k_2} > a_{k_1}$, a decreasing sequence of length $n + 1$.

Section 6.3

1. abc, acb, bac, bca, cab, cba **3.** 720 **5. a)** 120 **b)** 720 **c)** 8 **d)** 6720 **e)** 40,320 **f)** 3,628,800 **7.** 15,120 **9.** 1320 **11. a)** 210 **b)** 386 **c)** 848 **d)** 252 **13.** $2(n!)^2$ **15.** 65,780 **17.** $2^{100} - 5051$ **19. a)** 1024 **b)** 45 **c)** 176 **d)** 252 **21. a)** 120 **b)** 24 **c)** 120 **d)** 24 **e)** 6 **f)** 0 **23.** 609,638,400 **25. a)** 94,109,400 **b)** 941,094 **c)** 3,764,376 **d)** 90,345,024 **e)** 114,072 **f)** 2328 **g)** 24 **h)** 79,727,040 **i)** 3,764,376 **j)** 109,440 **27. a)** 12,650 **b)** 303,600 **29. a)** 37,927 **b)** 18,915 **31. a)** 122,523,030 **b)** 72,930,375 **c)** 223,149,655 **d)** 100,626,625 **33.** 54,600 **35.** 45 **37.** 912 **39.** 11,232,000 **41.** $n!/(r(n - r)!)$ **43.** 13 **45.** 873

Section 6.4

1. $x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$ **3.** $x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6$ **5.** 101 **7.** $-2^{10}\binom{19}{9} = -94{,}595{,}072$ **9.** $-2^{101}3^{99}\binom{200}{99}$ **11.** $(-1)^{(200-k)/3}\binom{100}{(200-k)/3}$ if $k \equiv 2 \pmod 3$ and $-100 \le k \le 200$; 0 otherwise **13.** 1 9 36 84 126 126 84 36 9 1 **15.** The sum of *all* the positive numbers $\binom{n}{k}$, as k runs from 0 to n, is 2^n, so each one of them is no bigger than this sum. **17.** $\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots 2} \le \frac{n \cdot n \cdot \cdots \cdot n}{2 \cdot 2 \cdot \cdots \cdot 2} = n^k/2^{k-1}$ **19.** $\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{n!}{k!(n-k+1)!} \cdot [k + (n - k + 1)] = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}$ **21. a)** We show that each side counts the number of ways to choose from a set with n elements a subset with k elements and a distinguished element of that set. For the left-hand side, first choose the k-set (this can be done in $\binom{n}{k}$ ways) and then choose one of the k elements in this subset to be the distinguished element (this can be done in k ways). For the right-hand side, first choose the distinguished element out of the entire n-set (this can be done in n ways), and then choose the remaining $k - 1$ elements of the subset from the remaining $n - 1$ elements of the set (this can be done in $\binom{n-1}{k-1}$ ways). **b)** $k\binom{n}{k} = k \cdot \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1)!}{(k-1)!(n-k)!} = n\binom{n-1}{k-1}$ **23.** $\binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!} = \frac{(n+1)}{k}\frac{n!}{(k-1)![n-(k-1)]!} = (n + 1)\binom{n}{k-1}/k$. This identity together with $\binom{n}{0} = 1$ gives a recursive definition. **25.** $\binom{2n}{n+1} + \binom{2n}{n} = \binom{2n+1}{n+1} = \frac{1}{2}\left[\binom{2n+1}{n+1} + \binom{2n+1}{n+1}\right] = \frac{1}{2}\left[\binom{2n+1}{n+1} + \binom{2n+1}{n}\right] = \frac{1}{2}\binom{2n+2}{n+1}$ **27. a)** $\binom{n+r+1}{r}$ counts the number of ways to choose a sequence of r 0s and $n + 1$ 1s by choosing the positions of the 0s. Alternately, suppose that the $(j + 1)$st term is the last term equal to 1, so that $n \le j \le n+r$. Once we have determined where the last 1 is, we decide where the 0s are to be placed in the j spaces before the last 1. There are n 1s and $j - n$ 0s in this range. By the sum rule it follows that there are $\sum_{j=n}^{n+r}\binom{j}{j-n} = \sum_{k=0}^{r}\binom{n+k}{k}$ ways to do this. **b)** Let $P(r)$ be the statement to be proved. The basis step is the equation $\binom{n}{0} = \binom{n+1}{0}$, which is just $1 = 1$. Assume that $P(r)$ is true. Then $\sum_{k=0}^{r+1}\binom{n+k}{k} = \sum_{k=0}^{r}\binom{n+k}{k} + \binom{n+r+1}{r+1} = \binom{n+r+1}{r} + \binom{n+r+1}{r+1} = \binom{n+r+2}{r+1}$, using the inductive hypothesis and Pascal's identity. 29. We can choose the leader first in n different ways. We can then choose the rest of the committee in 2^{n-1} ways. Hence, there are $n2^{n-1}$ ways to choose the committee and its leader. Meanwhile, the number of ways to select a committee with k people is $\binom{n}{k}$. Once we have chosen a committee with k people, there are k ways to choose its leader. Hence, there are $\sum_{k=1}^{n} k\binom{n}{k}$ ways to choose the committee and its leader. Hence, $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$. 31. Let the set have n elements. From Corollary 2 we have $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0$. It follows that $\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots = \binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots$. The left-hand side gives the number of subsets with an even number of elements, and the right-hand side gives the number of subsets with an odd number of elements. 33. **a)** A path of the desired type consists of m moves to the right and n moves up. Each such path can be represented by a bit string of length $m+n$ with m 0s and n 1s, where a 0 represents a move to the right and a 1 a move up. **b)** The number of bit strings of length $m+n$ containing exactly n 1s equals $\binom{m+n}{n} = \binom{m+n}{m}$ because such a string is determined by specifying the positions of the n 1s or by specifying the positions of the m 0s. 35. By Exercise 33 the number of paths of length n of the type described in that exercise equals 2^n, the number of bit strings of length n. On the other hand, a path of length n of the type described in Exercise 33 must end at a point that has n as the sum of its coordinates, say $(n-k, k)$ for some k between 0 and n, inclusive. By Exercise 33, the number of such paths ending at $(n-k, k)$ equals $\binom{n-k+k}{k} = \binom{n}{k}$. Hence, $\sum_{k=0}^{n}\binom{n}{k} = 2^n$. 37. By Exercise 33 the number of paths from $(0, 0)$ to $(n+1, r)$ of the type described in that exercise equals $\binom{n+r+1}{r}$. But such a path starts by going j steps vertically for some j with $0 \le j \le r$. The number of these paths beginning with j vertical steps equals the number of paths of the type described in Exercise 33 that go from $(1, j)$ to $(n+1, r)$. This is the same as the number of such paths that go from $(0, 0)$ to $(n, r-j)$, which by Exercise 33 equals $\binom{n+r-j}{r-j}$. Because $\sum_{j=0}^{r}\binom{n+r-j}{r-j} = \sum_{k=0}^{r}\binom{n+k}{k}$, it follows that $\sum_{k=1}^{r}\binom{n+k}{k} = \binom{n+r-1}{r}$. 39. **a)** $\binom{n+1}{2}$ **b)** $\binom{n+2}{3}$ **c)** $\binom{2n-2}{n-1}$ **d)** $\binom{n-1}{\lfloor (n-1)/2 \rfloor}$ **e)** Largest odd entry in nth row of Pascal's triangle **f)** $\binom{3n-3}{n-1}$

Section 6.5

1. 243 3. 26^6 5. 125 7. 35 9. **a)** 1716 **b)** 50,388 **c)** 2,629,575 **d)** 330 11. 9 13. 4,504,501 15. **a)** 10,626 **b)** 1,365 **c)** 11,649 **d)** 106 17. 2,520 19. 302,702,400 21. 3003 23. 7,484,400 25. 30,492 27. $C(59, 50)$ 29. 35 31. 83,160 33. 63 35. 19,635 37. 210 39. 27,720 41. $52!/(7!^5 17!)$ 43. Approximately 6.5×10^{32} 45. **a)** $C(k+n-1, n)$ **b)** $(k+n-1)!/(k-1)!$ 47. There are $C(n, n_1)$ ways to choose n_1 objects for the first box. Once these objects are chosen, there are $C(n-n_1, n_2)$ ways to choose objects for the second box. Similarly, there are $C(n-n_1-n_2, n_3)$ ways to choose objects for the third box. Continue in this way until there is $C(n-n_1-n_2-\cdots-n_{k-1}, n_k) = C(n_k, n_k) = 1$ way to choose the objects for the last box (because $n_1+n_2+\cdots+n_k = n$). By the product rule, the number of ways to make the entire assignment is $C(n, n_1)C(n-n_1, n_2)C(n-n_1-n_2, n_3)\cdots C(n-n_1-n_2-\cdots-n_{k-1}, n_k)$, which equals $n!/(n_1!n_2!\cdots n_k!)$, as straightforward simplification shows. 49. **a)** Because $x_1 \le x_2 \le \cdots \le x_r$, it follows that $x_1+0 < x_2+1 < \cdots < x_r+r-1$. The inequalities are strict because $x_j+j-1 < x_{j+1}+j$ as long as $x_j \le x_{j+1}$. Because $1 \le x_j \le n+r-1$, this sequence is made up of r distinct elements from T. **b)** Suppose that $1 \le x_1 < x_2 < \cdots < x_r \le n+r-1$. Let $y_k = x_k-(k-1)$. Then it is not hard to see that $y_k \le y_{k+1}$ for $k = 1, 2, \ldots, r-1$ and that $1 \le y_k \le n$ for $k = 1, 2, \ldots r$. It follows that $\{y_1, y_2, \ldots, y_r\}$ is an r-combination with repetitions allowed of S. **c)** From parts (a) and (b) it follows that there is a one-to-one correspondence of r-combinations with repetitions allowed of S and r-combinations of T, a set with $n+r-1$ elements. We conclude that there are $C(n+r-1, r)$ r-combinations with repetitions allowed of S. 51. 65 53. 65 55. 2 57. 3 59. **a)** 150 **b)** 25 **c)** 6 **d)** 2 61. 90,720 63. The terms in the expansion are of the form $x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m}$, where $n_1+n_2+\cdots+n_m = n$. Such a term arises from choosing the x_1 in n_1 factors, the x_2 in n_2 factors, $\ldots$, and the x_m in n_m factors. This can be done in $C(n; n_1, n_2, \ldots, n_m)$ ways, because a choice is a permutation of n_1 labels "1," n_2 labels "2," $\ldots$, and n_m labels "m." 65. 2520

Section 6.6

1. 14532, 15432, 21345, 23451, 23514, 31452, 31542, 43521, 45213, 45321 3. AAA1, AAA2, AAB1, AAB2, AAC1, AAC2, ABA1, ABA2, ABB1, ABB2, ABC1, ABC2, ACA1, ACA2, ACB1, ACB2, ACC1, ACC2, BAA1, BAA2, BAB1, BAB2, BAC1, BAC2, BBA1, BBA2, BBB1, BBB2, BBC1, BBC2, BCA1, BCA2, BCB1, BCB2, BCC1, BCC2, CAA1, CAA2, CAB1, CAB2, CAC1, CAC2, CBA1, CBA2, CBB1, CBB2, CBC1, CBC2, CCA1, CCA2, CCB1, CCB2, CCC1, CCC2 5. **a)** 2134 **b)** 54132 **c)** 12534 **d)** 45312) 7.1234, 1243, 1324, 1342, 1423, 1432, 2134, 2143, 2314, 2341, 2413, 2431, 3124, 3142, 3214, 3241, 3412, 3421, 4123, 4132, 4213, 4231, 4312, 4321 9. $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 2, 5\}$, $\{1, 3, 4\}$, $\{1, 3, 5\}$, $\{1, 4, 5\}$, $\{2, 3, 4\}$, $\{2, 3, 5\}$, $\{2, 4, 5\}$, $\{3, 4, 5\}$ 11. The bit string representing the next larger r-combination must differ from the bit string representing the original one in position i because positions $i+1, \ldots, r$ are occupied by the largest possible numbers. Also a_i+1 is the smallest possible number we can put in position i if we want a combination greater than the original one. Then $a_i+2, \ldots, a_i+r-i+1$ are the smallest allowable numbers for positions $i+1$ to r. Thus, we have produced the next r-combination. 13. 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 **15.** We will show that it is a bijection by showing that it has an inverse. Given a positive integer less than $n!$, let $a_1, a_2, \ldots, a_{n-1}$ be its Cantor digits. Put n in position $n - a_{n-1}$; then clearly, a_{n-1} is the number of integers less than n that follow n in the permutation. Then put $n - 1$ in free position $(n - 1) - a_{n-2}$, where we have numbered the free positions $1, 2, \ldots, n - 1$ (excluding the position that n is already in). Continue until 1 is placed in the only free position left. Because we have constructed an inverse, the correspondence is a bijection.

17. **procedure** *Cantor permutation*(n, i: integers with
    $n \geq 1$ and $0 \leq i < n!$)
$x := n$
for $j := 1$ **to** n
    $p_j := 0$
for $k := 1$ **to** $n - 1$
    $c := \lfloor x/(n-k)! \rfloor$; $x := x - c(n-k)!$; $h := n$
    while $p_h \neq 0$
        $h := h - 1$
    for $j := 1$ **to** c
        $h := h - 1$
        while $p_h \neq 0$
            $h := h - 1$
    $p_h := n - k + 1$
$h := 1$
while $p_h \neq 0$
    $h := h + 1$
$p_h := 1$
$\{p_1 p_2 \ldots p_n$ is the permutation corresponding
    to $i\}$

Supplementary Exercises

1. **a)** 151,200 **b)** 1,000,000 **c)** 210 **d)** 5005 **3.** 3^{100} **5.** 24,600 **7.** **a)** 4060 **b)** 2688 **c)** 25,009,600 **9.** **a)** 192 **b)** 301 **c)** 300 **d)** 300 **11.** 639 **13.** The maximum possible sum is 240, and the minimum possible sum is 15. So the number of possible sums is 226. Because there are 252 subsets with five elements of a set with 10 elements, by the pigeonhole principle it follows that at least two have the same sum. **15.** **a)** 50 **b)** 50 **c)** 14 **d)** 17 **17.** Let a_1, $a_2, \ldots, a_m$ be the integers, and let $d_i = \sum_{j=1}^{i} a_j$. If $d_i \equiv 0 \pmod{m}$ for some i, we are done. Otherwise $d_1 \ \mathbf{mod}\ m$, $d_2 \ \mathbf{mod}\ m, \ldots, d_m \ \mathbf{mod}\ m$ are m integers with values in $\{1, 2, \ldots, m - 1\}$. By the pigeonhole principle $d_k = d_l$ for some $1 \leq k < l \leq m$. Then $\sum_{j=k+1}^{l} a_j = d_l - d_k \equiv 0 \pmod{m}$. **19.** The decimal expansion of the rational number a/b can be obtained by division of b into a, where a is written with a decimal point and an arbitrarily long string of 0s following it. The basic step is finding the next digit of the quotient, namely, $\lfloor r/b \rfloor$, where r is the remainder with the next digit of the dividend brought down. The current remainder is obtained from the previous remainder by subtracting b times the previous digit of the quotient. Eventually the dividend has nothing but 0s to bring down. Furthermore, there are only b possible remainders. Thus, at some point, by the pigeonhole principle, we will have the same situation as had previously arisen. From that point onward, the calculation must follow the same pattern. In particular, the quotient will repeat. **21.** **a)** 125,970 **b)** 20 **c)** 141,120,525 **d)** 141,120,505 **e)** 177,100 **f)** 141,078,021 **23.** **a)** 10 **b)** 8 **c)** 7 **25.** 3^n **27.** $C(n + 2, r + 1) = C(n + 1, r + 1) + C(n + 1, r) = 2C(n + 1, r + 1) - C(n + 1, r + 1) + C(n + 1, r) = 2C(n + 1, r + 1) - (C(n, r + 1) + C(n, r)) + (C(n, r) + C(n, r - 1)) = 2C(n + 1, r + 1) - C(n, r + 1) + C(n, r - 1)$ **29.** Substitute $x = 1$ and $y = 3$ into the binomial theorem. **31.** Both sides count the number of ways to choose a subset of three distinct numbers $\{i, j, k\}$ with $i < j < k$ from $\{1, 2, \ldots, n\}$. **33.** $C(n + 1, 5)$ **35.** 3,491,888,400 **37.** 5^{24} **39.** **a)** 45 **b)** 57 **c)** 12 **41.** **a)** 386 **b)** 56 **43.** 0 if $n < m$; $C(n - 1, n - m)$ if $n \geq m$ **45.** **a)** 15,625 **b)** 202 **c)** 210 **d)** 10 **47.** **a)** 3 **b)** 11 **c)** 6 **d)** 10 **49.** There are two possibilities: three people seated at one table with everyone else sitting alone, which can be done in $2C(n, 3)$ ways (choose the three people and seat them in one of two arrangements), or two groups of two people seated together with everyone else sitting alone, which can be done in $3C(n, 4)$ ways (choose four people and then choose one of the three ways to pair them up). Both $2C(n, 3) + 3C(n, 4)$ and $(3n - 1)C(n, 3)/4$ equal $n^4/8 - 5n^3/12 + 3n^2/8 - n/12$. **51.** The number of permutations of $2n$ objects of n different types, two of each type, is $(2n)!/2^n$. Because this must be an integer, the denominator must divide the numerator. **53.** CCGGUCCGAAAG

55. **procedure** *next permutation*(n: positive integer,
    $a_1, a_2, \ldots, a_r$: positive integers not exceeding
    n with $a_1 a_2 \ldots a_r \neq nn \ldots n$)
$i := r$
while $a_i = n$
    $a_i := 1$
    $i := i - 1$
$a_i := a_i + 1$
$\{a_1 a_2 \ldots a_r$ is the next permutation in lexicographic
    order$\}$

57. We must show that if there are $R(m, n - 1) + R(m - 1, n)$ people at a party, then there must be at least m mutual friends or n mutual enemies. Consider one person; let's call him Jerry. Then there are $R(m - 1, n) + R(m, n - 1) - 1$ other people at the party, and by the pigeonhole principle there must be at least $R(m - 1, n)$ friends of Jerry or $R(m, n - 1)$ enemies of Jerry among these people. First let's suppose there are $R(m - 1, n)$ friends of Jerry. By the definition of R, among these people we are guaranteed to find either $m - 1$ mutual friends or n mutual enemies. In the former case, these $m - 1$ mutual friends together with Jerry are a set of m mutual friends; and in the latter case, we have the desired set of n mutual enemies. The other situation is similar: Suppose there are $R(m, n - 1)$ enemies of Jerry; we are guaranteed to find among them either m mutual friends or $n - 1$ mutual enemies. In the former case, we have the desired set of m mutual friends, and in the latter case, these $n - 1$ mutual enemies together with Jerry are a set of n mutual enemies.

CHAPTER 7

Section 7.1

1. 1/13 **3.** 1/2 **5.** 1/2 **7.** 1/64 **9.** 47/52 **11.** $1/C(52, 5)$ **13.** $1 - [C(48, 5)/C(52, 5)]$ **15.** $C(13, 2)C(4, 2)C(4, 2)C(44, 1)/C(52, 5)$ **17.** $10{,}240/C(52, 5)$ **19.** $1{,}302{,}540/C(52, 5)$ **21.** 1/64 **23.** 8/25 **25. a)** $1/C(50, 6) = 1/15{,}890{,}700$ **b)** $1/C(52, 6) = 1/20{,}358{,}520$ **c)** $1/C(56, 6) = 1/32{,}468{,}436$ **d)** $1/C(60, 6) = 1/50{,}063{,}860$ **27. a)** 139,128/319,865 **b)** 212, 667/511,313 **c)** 151,340/386,529 **d)** 163,647/446,276 **29.** $1/C(100, 8)$ **31.** 3/100 **33. a)** 1/7,880,400 **b)** 1/8,000,000 **35. a)** 9/19 **b)** 81/361 **c)** 1/19 **d)** 1,889,568/2,476,099 **e)** 48/361 **37.** Three dice **39.** The door the contestant chooses is chosen at random without knowing where the prize is, but the door chosen by the host is not chosen at random, because he always avoids opening the door with the prize. This makes any argument based on symmetry invalid. **41. a)** 671/1296 **b)** $1 - 35^{24}/36^{24}$; no **c)** The former

Section 7.2

1. $p(T) = 1/4$, $p(H) = 3/4$ **3.** $p(1) = p(3) = p(5) = p(6) = 1/16$; $p(2) = p(4) = 3/8$ **5.** 9/49 **7. a)** 1/2 **b)** 1/2 **c)** 1/3 **d)** 1/4 **e)** 1/4 **9. a)** 1/26! **b)** 1/26 **c)** 1/2 **d)** 1/26 **e)** 1/650 **f)** 1/15,600 **11.** Clearly, $p(E \cup F) \geq p(E) = 0.7$. 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 $0.7 + 0.5 - p(E \cap F) \leq 1$. Solving for $p(E \cap F)$ gives $p(E \cap F) \geq 0.2$. **13.** Because $p(E \cup F) = p(E) + p(F) - p(E \cap F)$ and $p(E \cup F) \leq 1$, it follows that $1 \geq p(E) + p(F) - p(E \cap F)$. From this inequality we conclude that $p(E) + p(F) \leq 1 + p(E \cap F)$. **15.** We will use mathematical induction to prove that the inequality holds for $n \geq 2$. Let $P(n)$ be the statement that $p(\bigcup_{j=1}^{n} E_j) \leq \sum_{j=1}^{n} p(E_j)$. *Basis step:* $P(2)$ is true because $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2) \leq p(E_1) + p(E_2)$. *Inductive step:* Assume that $P(k)$ is true. Using the basis case and the inductive hypothesis, it follows that $p(\bigcup_{j=1}^{k+1} E_j) \leq p(\bigcup_{j=1}^{k} E_j) + p(E_{k+1}) \leq \sum_{j=1}^{k+1} p(E_j)$. This shows that $P(k+1)$ is true, completing the proof by mathematical induction. **17.** Because $E \cup \overline{E}$ is the entire sample space S, the event F can be split into two disjoint events: $F = S \cap F = (E \cup \overline{E}) \cap F = (E \cap F) \cup (\overline{E} \cap F)$, using the distributive law. Therefore, $p(F) = p((E \cap F) \cup (\overline{E} \cap F)) = p(E \cap F) + p(\overline{E} \cap F)$, because these two events are disjoint. Subtracting $p(E \cap F)$ from both sides, using the fact that $p(E \cap F) = p(E) \cdot p(F)$ (the hypothesis that E and F are independent), and factoring, we have $p(F)[1 - p(E)] = p(\overline{E} \cap F)$. Because $1 - p(E) = p(\overline{E})$, this says that $p(\overline{E} \cap F) = p(\overline{E}) \cdot p(F)$, as desired. **19. a)** 1/12 **b)** $1 - \frac{11}{12} \cdot \frac{10}{12} \cdot \cdots \cdot \frac{13-n}{12}$ **c)** 5 **21.** 614 **23.** 1/4 **25.** 3/8 **27. a)** Not independent **b)** Not independent **c)** Not independent **29.** 3/16 **31. a)** $1/32 = 0.03125$ **b)** $0.49^5 \approx 0.02825$ **c)** 0.03795012 **33. a)** 5/8 **b)** 0.627649 **c)** 0.6431 **35. a)** p^n **b)** $1 - p^n$ **c)** $p^n + n \cdot p^{n-1} \cdot (1 - p)$ **d)** $1 - [p^n + n \cdot p^{n-1} \cdot (1 - p)]$ **37.** $p(\bigcup_{i=1}^{\infty} E_i)$ is the sum of $p(s)$ for each outcome s in $\bigcup_{i=1}^{\infty} E_i$. Because the E_is are pairwise disjoint, this is the sum of the probabilities of all the outcomes in any of the E_is, which is what $\sum_{i=1}^{\infty} p(E_i)$ is. (We can rearrange the summands and still get the same answer because this series converges absolutely.) **39. a)** $\overline{E} = \bigcup_{j=1}^{\binom{m}{k}} F_j$, so the given inequality now follows from Boole's Inequality (Exercise 15). **b)** The probability that a particular player not in the jth set beats all k of the players in the jth set is $(1/2)^k = 2^{-k}$. Therefore, the probability that this player does not do so is $1 - 2^{-k}$, so the probability that all $m - k$ of the players not in the jth set are unable to boast of a perfect record against everyone in the jth set is $(1 - 2^{-k})^{m-k}$. That is precisely $p(F_j)$. **c)** The first inequality follows immediately, because all the summands are the same and there are $\binom{m}{k}$ of them. If this probability is less than 1, then it must be possible that $\overline{E}$ fails, i.e., that E happens. So there is a tournament that meets the conditions of the problem as long as the second inequality holds. **d)** $m \geq 21$ for $k = 2$, and $m \geq 91$ for $k = 3$

41.
```
procedure probabilistic prime(n, k)
  composite := false
  i := 0
  while composite = false and i < k
    i := i + 1
    choose b uniformly at random with 1 < b < n
    apply Miller's test to base b
    if n fails the test then composite := true
  if composite = true then print ("composite")
  else print ("probably prime")
```

Section 7.3

NOTE: In the answers for Section 7.3, all probabilities given in decimal form are rounded to three decimal places. **1.** 3/5 **3.** 3/4 **5.** 0.481 **7. a)** 0.999 **b)** 0.324 **9. a)** 0.740 **b)** 0.260 **c)** 0.002 **d)** 0.998 **11.** 0.724 **13.** 3/17 **15. a)** 1/3 **b)** $p(M = j \mid W = k) = 1$ if i, j, and k are distinct; $p(M = j \mid W = k) = 0$ if $j = k$ or $j = i$; $p(M = j \mid W = k) = 1/2$ if $i = k$ and $j \neq i$ **c)** 2/3 **d)** You should change doors, because you now have a 2/3 chance to win by switching. **17.** The definition of conditional probability tells us that $p(F_j \mid E) = p(E \cap F_j)/p(E)$. For the numerator, again using the definition of conditional probability, we have $p(E \cap F_j) = p(E \mid F_j)p(F_j)$, as desired. For the denominator, we show that $p(E) = \sum_{i=1}^{n} p(E \mid F_i)p(F_i)$. The events $E \cap F_i$ partition the event E; that is, $(E \cap F_{i_1}) \cap (E \cap F_{i_2}) = \emptyset$ when $i_i \neq i_2$ (because the F_i's are mutually exclusive), and $\bigcup_{i=1}^{n} (E \cap F_{i_1}) = E$ (because the $\bigcup_{i=1}^{n} F_i = S$). Therefore, $p(E) = \sum_{i=1}^{n} p(E \cap F_i) = \sum_{i=1}^{n} p(E \mid F_i)p(F_i)$. **19.** No **21.** Yes **23.** By Bayes' theorem, $p(S \mid E_1 \cap E_2) = p(E_1 \cap E_2 \mid S)p(S)/[p(E_1 \cap E_2 \mid S)p(S) + p(E_1 \cap E_2 \mid \overline{S})p(\overline{S})]$.

Because we are assuming no prior knowledge about whether a message is or is not spam, we set $p(S) = p(\overline{S}) = 0.5$, and so the equation above simplifies to $p(S \mid E_1 \cap E_2) = p(E_1 \cap E_2 \mid S)/[p(E_1 \cap E_2 \mid S) + p(E_1 \cap E_2 \mid \overline{S})]$. Because of the assumed independence of E_1, E_2, and S, we have $p(E_1 \cap E_2 \mid S) = p(E_1 \mid S) \cdot p(E_2 \mid S)$, and similarly for $\overline{S}$.

Section 7.4

1. 2.5 3. $5/3$ 5. $336/49$ 7. 170 9. $(4n + 6)/3$ 11. $50{,}700{,}551/10{,}077{,}696 \approx 5.03$ 13. 6 15. $p(X \geq j) = \sum_{k=j}^{\infty} p(X = k) = \sum_{k=j}^{\infty}(1 - p)^{k-1}p = p(1-p)^{j-1}\sum_{k=0}^{\infty}(1-p)^k = p(1-p)^{j-1}/(1-(1-p)) = (1-p)^{j-1}$ 17. 2302 19. $(7/2) \cdot 7 \neq 329/12$ 21. 10 23. 1472 pounds 25. $p + (n-1)p(1-p)$ 27. $5/2$ 29. **a)** 0 **b)** n 31. This is not true. For example, let X be the number of heads in one flip of a fair coin, and let Y be the number of heads in one flip of a second fair coin. Then $A(X) + A(Y) = 1$ but $A(X + Y) = 0.5$. 33. **a)** We are told that X_1 and X_2 are independent. To see that X_1 and X_3 are independent, we enumerate the eight possibilities for (X_1, X_2, X_3) and find that $(0, 0, 0)$, $(1, 0, 1)$, $(0, 1, 1)$, $(1, 1, 0)$ each have probability $1/4$ and the others have probability 0 (because of the definition of X_3). Thus, $p(X_1 = 0 \wedge X_3 = 0) = 1/4$, $p(X_1 = 0) = 1/2$, and $p(X_3 = 0) = 1/2$, so it is true that $p(X_1 = 0 \wedge X_3 = 0) = p(X_1 = 0)p(X_3 = 0)$. Essentially the same calculation shows that $p(X_1 = 0 \wedge X_3 = 1) = p(X_1 = 0)p(X_3 = 1)$, $p(X_1 = 1 \wedge X_3 = 0) = p(X_1 = 1)p(X_3 = 0)$, and $p(X_1 = 1 \wedge X_3 = 1) = p(X_1 = 1)p(X_3 = 1)$. Therefore by definition, X_1 and X_3 are independent. The same reasoning shows that X_2 and X_3 are independent. To see that X_3 and $X_1 + X_2$ are not independent, we observe that $p(X_3 = 1 \wedge X_1 + X_2 = 2) = 0$. But $p(X_3 = 1)p(X_1 + X_2 = 2) = (1/2)(1/4) = 1/8$. **b)** We see from the calculation in part (a) that X_1, X_2, and X_3 are all Bernoulli random variables, so the variance of each is $(1/2)(1/2) = 1/4$. Therefore, $V(X_1) + V(X_2) + V(X_3) = 3/4$. We use the calculations in part (a) to see that $E(X_1 + X_2 + X_3) = 3/2$, and then $V(X_1 + X_2 + X_3) = 3/4$. **c)** In order to use the first part of Theorem 7 to show that $V((X_1 + X_2 + \cdots + X_k) + X_{k+1}) = V(X_1 + X_2 + \cdots + X_k) + V(X_{k+1})$ in the inductive step of a proof by mathematical induction, we would have to know that $X_1 + X_2 + \cdots + X_k$ and X_{k+1} are independent, but we see from part (a) that this is not necessarily true. 35. $1/100$ 37. $E(X)/a = \sum_r (r/a) \cdot p(X = r) \geq \sum_{r \geq a} 1 \cdot p(X = r) = p(X \geq a)$ 39. **a)** $10/11$ **b)** 0.9999 41. **a)** Each of the $n!$ permutations occurs with probability $1/n!$, so $E(X)$ is the number of comparisons, averaged over all these permutations. **b)** Even if the algorithm continues $n - 1$ rounds, X will be at most $n(n-1)/2$. It follows from the formula for expectation that $E(X) \leq n(n-1)/2$. **c)** The algorithm proceeds by comparing adjacent elements and then swapping them if necessary. Thus, the only way that inverted elements can become uninverted is for them to be compared and swapped. **d)** Because $X(P) \geq I(P)$ for all P, it follows from the definition of expectation that $E(X) \geq E(I)$. **e)** This summation counts 1 for every instance of an inversion. **f)** This follows from Theorem 3. **g)** By Theorem 2 with $n = 1$, the expectation of $I_{j,k}$ is the probability that a_k precedes a_j in the permutation. This is clearly $1/2$ by symmetry. **h)** The summation in part (f) consists of $C(n, 2) = n(n-1)/2$ terms, each equal to $1/2$, so the sum is $n(n-1)/4$. **i)** From part (a) and part (b) we know that $E(X)$, the object of interest, is at most $n(n-1)/2$, and from part (d) and part (h) we know that $E(X)$ is at least $n(n-1)/4$, both of which are $\Theta(n^2)$. 43. 1 45. $V(X + Y) = E((X + Y)^2) - E(X + Y)^2 = E(X^2 + 2XY + Y^2) - [E(X) + E(Y)]^2 = E(X^2) + 2E(XY) + E(Y^2) - E(X)^2 - 2E(X)E(Y) - E(Y)^2 = E(X^2) - E(X)^2 + 2[E(XY) - E(X)E(Y)] + E(Y^2) - E(Y)^2 = V(X) + 2\,\mathrm{Cov}(X, Y) + V(Y)$ 47. $[(n-1)/n]^m$ 49. $(n-1)^m/n^{m-1}$

Supplementary Exercises

1. $1/109{,}668$ 3. **a)** $1/195{,}249{,}054$ **b)** $1/5{,}138{,}133$ **c)** $45/357{,}599$ **d)** $18{,}285/18{,}821$ 5. **a)** $1/C(52, 13)$ **b)** $4/C(52, 13)$ **c)** $2{,}944{,}656/C(52, 13)$ **d)** $35{,}335{,}872/C(52, 13)$ 7. **a)** $9/2$ **b)** $21/4$ 9. **a)** 9 **b)** $21/2$ 11. **a)** 8 **b)** $49/6$ 13. **a)** $n/2^{n-1}$ **b)** $p(1-p)^{k-1}$, where $p = n/2^{n-1}$ **c)** $2^{n-1}/n$ 15. $\frac{(m-1)(n-1)+\gcd(m,n)-1}{mn-1}$ 17. **a)** $2/3$ **b)** $2/3$ 19. $1/32$ 21. **a)** The probability that one wins 2^n dollars is $1/2^n$, because that happens precisely when the player gets $n-1$ tails followed by a head. The expected value of the winnings is therefore the sum of 2^n times $1/2^n$ as n goes from 1 to infinity. Because each of these terms is 1, the sum is infinite. In other words, one should be willing to wager any amount of money and expect to come out ahead in the long run. **b)** \$9, \$9 23. **a)** $1/3$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and $B = \{1, 2, 3, 4\}$; $1/12$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{4, 5, 6, 7, 8, 9, 10, 11, 12\}$, and $B = \{1, 2, 3, 4\}$ **b)** 1 when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{4, 5, 6, 7, 8, 9, 10, 11, 12\}$, and $B = \{1, 2, 3, 4\}$; $3/4$ when $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and $B = \{1, 2, 3, 4\}$ 25. **a)** $p(E_1 \cap E_2) = p(E_1)p(E_2)$, $p(E_1 \cap E_3) = p(E_1)p(E_3)$, $p(E_2 \cap E_3) = p(E_2)p(E_3)$, $p(E_1 \cap E_2 \cap E_3) = p(E_1)p(E_2)p(E_3)$ **b)** Yes **c)** Yes; yes **d)** Yes; no **e)** $2^n - n - 1$ 27. **a)** $1/2$ under first interpretation; $1/3$ under second interpretation **b)** Let M be the event that both of Mr. Smith's children are boys and let B be the event that Mr. Smith chose a boy for today's walk. Then $p(M) = 1/4$, $p(B \mid M) = 1$, and $p(B \mid \overline{M}) = 1/3$. Apply Bayes' theorem to compute $p(M \mid B) = 1/2$. **c)** This variation is equivalent to the second interpretation discussed in part (a), so the answer is unambiguously $1/3$. 29. $V(aX + b) = E((aX + b)^2) - E(aX + b)^2 = E(a^2X^2 + 2abX + b^2) - [aE(X) + b]^2 = E(a^2X^2) + E(2abX) + E(b^2) - [a^2E(X)^2 + 2abE(X) + b^2] = a^2E(X^2) + 2abE(X) + b^2 - a^2E(X)^2 - 2abE(X) - b^2 =$

$a^2[E(X^2) - E(X)^2] = a^2V(X)$ **31.** To count every element in the sample space exactly once, we must include every element in each of the sets and then take away the double counting of the elements in the intersections. Thus $p(E_1 \cup E_2 \cup \cdots \cup E_m) = p(E_1) + p(E_2) + \cdots + p(E_m) - p(E_1 \cap E_2) - p(E_1 \cap E_3) - \cdots - p(E_1 \cap E_m) - p(E_2 \cap E_3) - p(E_2 \cap E_4) - \cdots - p(E_2 \cap E_m) - \cdots - p(E_{m-1} \cap E_m) = qm - (m(m-1)/2)r$, because $C(m, 2)$ terms are being subtracted. But $p(E_1 \cup E_2 \cup \cdots \cup E_m) = 1$, so we have $qm - [m(m-1)/2]r = 1$. Because $r \geq 0$, this equation tells us that $qm \geq 1$, so $q \geq 1/m$. Because $q \leq 1$, this equation also implies that $[m(m-1)/2]r = qm - 1 \leq m - 1$, from which it follows that $r \leq 2/m$. **33. a)** We purchase the cards until we have gotten one of each type. That means we have purchased X cards in all. On the other hand, that also means that we purchased X_0 cards until we got the first type we got, and then purchased X_1 more cards until we got the second type we got, and so on. Thus, X is the sum of the X_j's. **b)** Once j distinct types have been obtained, there are $n - j$ new types available out of a total of n types available. Because it is equally likely that we get each type, the probability of success on the next purchase (getting a new type) is $(n - j)/n$. **c)** This follows immediately from the definition of geometric distribution, the definition of X_j, and part (b). **d)** From part (c) it follows that $E(X_j) = n/(n - j)$. Thus by the linearity of expectation and part (a), we have $E(X) = E(X_0) + E(X_1) + \cdots + E(X_{n-1}) = \frac{n}{n} + \frac{n}{n-1} + \cdots + \frac{n}{1} = n\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{1}\right)$. **e)** About 224.46 **35.** $24 \cdot 13^4/(52 \cdot 51 \cdot 50 \cdot 49)$

CHAPTER 8

Section 8.1

1. Let $P(n)$ be "$H_n = 2^n - 1$." *Basis step:* $P(1)$ is true because $H_1 = 1$. *Inductive step:* Assume that $H_n = 2^n - 1$. Then because $H_{n+1} = 2H_n + 1$, it follows that $H_{n+1} = 2(2^n - 1) + 1 = 2^{n+1} - 1$. **3. a)** $a_n = 2a_{n-1} + a_{n-5}$ for $n \geq 5$ **b)** $a_0 = 1$, $a_1 = 2$, $a_2 = 4$, $a_3 = 8$, $a_4 = 16$ **c)** 1217 **5.** 9494 **7. a)** $a_n = a_{n-1} + a_{n-2} + 2^{n-2}$ for $n \geq 2$ **b)** $a_0 = 0$, $a_1 = 0$ **c)** 94 **9. a)** $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n \geq 3$ **b)** $a_0 = 1$, $a_1 = 2$, $a_2 = 4$ **c)** 81 **11. a)** $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$ **b)** $a_0 = 1$, $a_1 = 1$ **c)** 34 **13. a)** $a_n = 2a_{n-1} + 2a_{n-2}$ for $n \geq 2$ **b)** $a_0 = 1$, $a_1 = 3$ **c)** 448 **15. a)** $a_n = 2a_{n-1} + a_{n-2}$ for $n \geq 2$ **b)** $a_0 = 1$, $a_1 = 3$ **c)** 239 **17. a)** $a_n = 2a_{n-1}$ for $n \geq 2$ **b)** $a_1 = 3$ **c)** 96 **19. a)** $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$ **b)** $a_0 = 1$, $a_1 = 1$ **c)** 89 **21. a)** $R_n = n + R_{n-1}$, $R_0 = 1$ **b)** $R_n = n(n+1)/2 + 1$ **23. a)** $S_n = S_{n-1} + (n^2 - n + 2)/2$, $S_0 = 1$ **b)** $S_n = (n^3 + 5n + 6)/6$ **25.** 64 **27. a)** $a_n = 2a_{n-1} + 2a_{n-2}$ **b)** $a_0 = 1$, $a_1 = 3$ **c)** 1224 **29.** Clearly, $S(m, 1) = 1$ for $m \geq 1$. If $m \geq n$, then a function that is not onto from the set with m elements to the set with n elements can be specified by picking the size of the range, which is an integer between 1 and $n - 1$ inclusive, picking the elements of the range, which can be done in $C(n, k)$ ways, and picking an onto function onto the range, which can be done in $S(m, k)$ ways. Hence, there are $\sum_{k=1}^{n-1} C(n, k)S(m, k)$ func- tions that are not onto. But there are n^m functions altogether, so $S(m, n) = n^m - \sum_{k=1}^{n-1} C(n, k)S(m, k)$. **31. a)** $C_5 = C_0C_4 + C_1C_3 + C_2C_2 + C_3C_1 + C_4C_0 = 1 \cdot 14 + 1 \cdot 5 + 2 \cdot 2 + 5 \cdot 1 + 14 \cdot 1 = 42$ **b)** $C(10, 5)/6 = 42$ **33.** $J(1) = 1$, $J(2) = 1$, $J(3) = 3$, $J(4) = 1$, $J(5) = 3$, $J(6) = 5$, $J(7) = 7$, $J(8) = 1$, $J(9) = 3$, $J(10) = 5$, $J(11) = 7$, $J(12) = 9$, $J(13) = 11$, $J(14) = 13$, $J(15) = 15$, $J(16) = 1$ **35.** First, suppose that the number of people is even, say $2n$. After going around the circle once and returning to the first person, because the people at locations with even numbers have been eliminated, there are exactly n people left and the person currently at location i is the person who was originally at location $2i - 1$. Therefore, the survivor [originally in location $J(2n)$] is now in location $J(n)$; this was the person who was at location $2J(n) - 1$. Hence, $J(2n) = 2J(n) - 1$. Similarly, when there are an odd number of people, say $2n + 1$, then after going around the circle once and then eliminating person 1, there are n people left and the person currently at location i is the person who was at location $2i + 1$. Therefore, the survivor will be the player currently occupying location $J(n)$, namely, the person who was originally at location $2J(n) + 1$. Hence, $J(2n + 1) = 2J(n) + 1$. The basis step is $J(1) = 1$. **37.** 73, 977, 3617 **39.** These nine moves solve the puzzle: Move disk 1 from peg 1 to peg 2; move disk 2 from peg 1 to peg 3; move disk 1 from peg 2 to peg 3; move disk 3 from peg 1 to peg 2; move disk 4 from peg 1 to peg 4; move disk 3 from peg 2 to peg 4; move disk 1 from peg 3 to peg 2; move disk 2 from peg 3 to peg 4; move disk 1 from peg 2 to peg 4. To see that at least nine moves are required, first note that at least seven moves are required no matter how many pegs are present: three to unstack the disks, one to move the largest disk 4, and three more moves to restack them. At least two other moves are needed, because to move disk 4 from peg 1 to peg 4 the other three disks must be on pegs 2 and 3, so at least one move is needed to restack them and one move to unstack them. **41.** The base cases are obvious. If $n > 1$, the algorithm consists of three stages. In the first stage, by the inductive hypothesis, $R(n - k)$ moves are used to transfer the smallest $n - k$ disks to peg 2. Then using the usual three-peg Tower of Hanoi algorithm, it takes $2^k - 1$ moves to transfer the rest of the disks (the largest k disks) to peg 4, avoiding peg 2. Then again by the inductive hypothesis, it takes $R(n - k)$ moves to transfer the smallest $n - k$ disks to peg 4; all the pegs are available for this, because the largest disks, now on peg 4, do not interfere. This establishes the recurrence relation. **43.** First note that $R(n) = \sum_{j=1}^{n} [R(j) - R(j - 1)]$ [which follows because the sum is telescoping and $R(0) = 0$]. By Exercise 42, this is the sum of $2^{k'-1}$ for this range of values of j. Therefore, the sum is $\sum_{i=1}^{k} i2^{i-1}$, except that if n is not a triangular number, then the last few values when $i = k$ are missing, and that is what the final term in the given expression accounts for. **45.** By Exercise 43, $R(n)$ is no larger than $\sum_{i=1}^{k} i2^{i-1}$. It can be shown that this sum equals $(k+1)2^k - 2^{k+1} + 1$, so it is no greater than $(k+1)2^k$. Because $n > k(k-1)/2$, the quadratic formula can be used to show that

$k < 1+\sqrt{2n}$ for all $n > 1$. Therefore, $R(n)$ is bounded above by $(1+\sqrt{2n}+1)2^{1+\sqrt{2n}} < 8\sqrt{n}2^{\sqrt{2n}}$ for all $n > 2$. Hence, $R(n)$ is $O(\sqrt{n}2^{\sqrt{2n}})$. **47. a)** 0 **b)** 0 **c)** 2 **d)** $2^{n-1} - 2^{n-2}$ **49.** $a_n - 2\nabla a_n + \nabla^2 a_n = a_n - 2(a_n - a_{n-1}) + (\nabla a_n - \nabla a_{n-1}) = -a_n + 2a_{n-1} + [(a_n - a_{n-1}) - (a_{n-1} - a_{n-2})] = -a_n + 2a_{n-1} + (a_n - 2a_{n-1} + a_{n-2}) = a_{n-2}$ **51.** $a_n = a_{n-1} + a_{n-2} = (a_n - \nabla a_n) + (a_n - 2\nabla a_n + \nabla^2 a_n) = 2a_n - 3\nabla a_n + \nabla^2 a_n$, or $a_n = 3\nabla a_n - \nabla^2 a_n$ **53.** Insert $S(0) := \emptyset$ after $T(0) := 0$ (where $S(j)$ will record the optimal set of talks among the first j talks), and replace the statement $T(j) := \max(w_j + T(p(j)), T(j-1))$ with the following code:

if $w_j + T(p(j)) > T(j-1)$ **then**
  $T(j) := w_j + T(p(j))$
  $S(j) := S(p(j)) \cup \{j\}$
else
  $T(j) := T(j-1)$
  $S(j) := S(j-1)$

55. a) Talks 1, 3, and 7 **b)** Talks 1 and 6, or talks 1, 3, and 7 **c)** Talks 1, 3, and 7 **d)** Talks 1 and 6 **57. a)** This follows immediately from Example 5 and Exercise 41c in Section 8.4. **b)** The last step in computing $\mathbf{A}_{ij}$ is to multiply $\mathbf{A}_{ik}$ by $\mathbf{A}_{k+1,j}$ for some k between i and $j-1$ inclusive, which will require $m_i m_{k+1} m_{j+1}$ integer multiplications, independent of the manner in which $\mathbf{A}_{ik}$ and $\mathbf{A}_{k+1,j}$ are computed. Therefore to minimize the total number of integer multiplications, each of those two factors must be computed in the most efficient manner. **c)** This follows immediately from part (b) and the definition of $M(i, j)$. **d) procedure** *matrix order*$(m_1, \ldots, m_{n+1}$: positive integers)

for $i := 1$ **to** n
  $M(i, i) := 0$
for $d := 1$ **to** $n - 1$
  for $i := 1$ **to** $n - d$
    min $:= 0$
    for $k := i$ **to** $i + d$
      new $:= M(i, k) + M(k+1, i+d) + m_i m_{k+1} m_{i+d+1}$
      if *new* $<$ *min* **then**
        min := *new*
        where$(i, i+d) := k$
    $M(i, i+d) :=$ *min*

e) The algorithm has three nested loops, each of which is indexed over at most n values.

Section 8.2

1. a) Degree 3 **b)** No **c)** Degree 4 **d)** No **e)** No **f)** Degree 2 **g)** No **3. a)** $a_n = 3 \cdot 2^n$ **b)** $a_n = 2$ **c)** $a_n = 3 \cdot 2^n - 2 \cdot 3^n$ **d)** $a_n = 6 \cdot 2^n - 2 \cdot n2^n$ **e)** $a_n = n(-2)^{n-1}$ **f)** $a_n = 2^n - (-2)^n$ **g)** $a_n = (1/2)^{n+1} - (-1/2)^{n+1}$ **5.** $a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$ **7.** $[2^{n+1} + (-1)^n]/3$ **9. a)** $P_n = 1.2P_{n-1} + 0.45P_{n-2}$, $P_0 = 100{,}000$, $P_1 = 120{,}000$ **b)** $P_n = (250{,}000/3)(3/2)^n + (50{,}000/3)(-3/10)^n$ **11. a)** *Basis step:* For $n = 1$ we have $1 = 0 + 1$, and for $n = 2$ we have $3 = 1 + 2$. *Inductive step:* Assume true for $k \le n$. Then $L_{n+1} = L_n + L_{n-1} = f_{n-1} + f_{n+1} + f_{n-2} + f_n = (f_{n-1} + f_{n-2}) + (f_{n+1} + f_n) = f_n + f_{n+2}$. **b)** $L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$ **13.** $a_n = 8(-1)^n - 3(-2)^n + 4 \cdot 3^n$ **15.** $a_n = 5 + 3(-2)^n - 3^n$ **17.** Let $a_n = C(n, 0) + C(n-1, 1) + \cdots + C(n-k, k)$ where $k = \lfloor n/2 \rfloor$. First, assume that n is even, so that $k = n/2$, and the last term is $C(k, k)$. By Pascal's identity we have $a_n = 1 + C(n-2, 0) + C(n-2, 1) + C(n-3, 1) + C(n-3, 2) + \cdots + C(n-k, k-2) + C(n-k, k-1) + 1 = 1 + C(n-2, 1) + C(n-3, 2) + \cdots + C(n-k, k-1) + C(n-2, 0) + C(n-3, 1) + \cdots + C(n-k, k-2) + 1 = a_{n-1} + a_{n-2}$ because $\lfloor (n-1)/2 \rfloor = k - 1 = \lfloor (n-2)/2 \rfloor$. A similar calculation works when n is odd. Hence, $\{a_n\}$ satisfies the recurrence relation $a_n = a_{n-1} + a_{n-2}$ for all positive integers n, $n \ge 2$. Also, $a_1 = C(1, 0) = 1$ and $a_2 = C(2, 0) + C(1, 1) = 2$, which are f_2 and f_3. It follows that $a_n = f_{n+1}$ for all positive integers n. **19.** $a_n = (n^2 + 3n + 5)(-1)^n$ **21.** $(a_{1,0} + a_{1,1}n + a_{1,2}n^2 + a_{1,3}n^3) + (a_{2,0} + a_{2,1}n + a_{2,2}n^2)(-2)^n + (a_{3,0} + a_{3,1}n)3^n + a_{4,0}(-4)^n$ **23. a)** $3a_{n-1} + 2^n = 3(-2)^n + 2^n = 2^n(-3 + 1) = -2^{n+1} = a_n$ **b)** $a_n = \alpha 3^n - 2^{n+1}$ **c)** $a_n = 3^{n+1} - 2^{n+1}$ **25. a)** $A = -1$, $B = -7$ **b)** $a_n = \alpha 2^n - n - 7$ **c)** $a_n = 11 \cdot 2^n - n - 7$ **27. a)** $p_3 n^3 + p_2 n^2 + p_1 n + p_0$ **b)** $n^2 p_0 (-2)^n$ **c)** $n^2(p_1 n + p_0)2^n$ **d)** $(p_2 n^2 + p_1 n + p_0)4^n$ **e)** $n^2(p_2 n^2 + p_1 n + p_0)(-2)^n$ **f)** $n^2(p_4 n^4 + p_3 n^3 + p_2 n^2 + p_1 n + p_0)2^n$ **g)** p_0 **29. a)** $a_n = \alpha 2^n + 3^{n+1}$ **b)** $a_n = -2 \cdot 2^n + 3^{n+1}$ **31.** $a_n = \alpha 2^n + \beta 3^n - n \cdot 2^{n+1} + 3n/2 + 21/4$ **33.** $a_n = (\alpha + \beta n + n^2 + n^3/6)2^n$ **35.** $a_n = -4 \cdot 2^n - n^2/4 - 5n/2 + 1/8 + (39/8)3^n$ **37.** $a_n = n(n+1)(n+2)/6$ **39. a)** $1, -1, i, -i$ **b)** $a_n = \frac{1}{4} - \frac{1}{4}(-1)^n + \frac{2+i}{4}i^n + \frac{2-i}{4}(-i)^n$ **41. a)** Using the formula for f_n, we see that $\left| f_n - \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n \right| = \left| \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \right| < 1/\sqrt{5} < 1/2$. This means that f_n is the integer closest to $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$. **b)** Less when n is even; greater when n is odd **43.** $a_n = f_{n-1} + 2f_n - 1$ **45. a)** $a_n = 3a_{n-1} + 4a_{n-2}$, $a_0 = 2$, $a_1 = 6$ **b)** $a_n = [4^{n+1} + (-1)^n]/5$ **47. a)** $a_n = 2a_{n+1} + (n-1)10{,}000$ **b)** $a_n = 70{,}000 \cdot 2^{n-1} - 10{,}000n - 10{,}000$ **49.** $a_n = 5n^2/12 + 13n/12 + 1$ **51.** See Chapter 11, Section 5 in [Ma93]. **53.** $6^n \cdot 4^{n-1}/n$

Section 8.3

1. 14 **3.** The first step is $(1110)_2(1010)_2 = (2^4 + 2^2)(11)_2\ (10)_2 + 2^2[(11)_2 - (10)_2][(10)_2 - (10)_2] + (2^2 + 1)(10)_2 \cdot (10)_2$. The product is $(10001100)_2$. **5.** $C = 50{,}665C + 729 = 33{,}979$ **7. a)** 2 **b)** 4 **c)** 7 **9. a)** 79 **b)** 48,829 **c)** 30,517,579 **11.** $O(\log n)$ **13.** $O(n^{\log_3 2})$ **15.** 5 **17. a)** *Basis step:* If the sequence has just one element, then the one person on the list is the winner. *Recursive step:* Divide the list into two parts—the first half and the second half—as equally as possible. Apply the algorithm recursively to each half to come up with at most two names. Then run through the entire list to count the number of occurrences of each of those names to decide which, if either, is the winner. **b)** $O(n \log n)$ 19. **a)** $f(n) = f(n/2) + 2$ **b)** $O(\log n)$ 21. **a)** 7 **b)** $O(\log n)$

23. **a)**

```
procedure largest sum(a_1, ..., a_n)
best := 0 {empty subsequence has sum 0}
for i := 1 to n
  sum := 0
  for j := i + 1 to n
    sum := sum + a_j
    if sum > best then best := sum
{best is the maximum possible sum of numbers
   in the list}
```

b) $O(n^2)$ **c)** We divide the list into a first half and a second half and apply the algorithm recursively to find the largest sum of consecutive terms for each half. The largest sum of consecutive terms in the entire sequence is either one of these two numbers or the sum of a sequence of consecutive terms that crosses the middle of the list. To find the largest possible sum of a sequence of consecutive terms that crosses the middle of the list, we start at the middle and move forward to find the largest possible sum in the second half of the list, and move backward to find the largest possible sum in the first half of the list; the desired sum is the sum of these two quantities. The final answer is then the largest of this sum and the two answers obtained recursively. The base case is that the largest sum of a sequence of one term is the larger of that number and 0. **d)** 11, 9, 14 **e)** $S(n) = 2S(n/2) + n$, $C(n) = 2C(n/2) + n + 2$, $S(1) = 0$, $C(1) = 1$ **f)** $O(n \log n)$, better than $O(n^2)$ 25. (1, 6) and (3, 6) at distance 2 27. The algorithm is essentially the same as the algorithm given in Example 12. The central strip still has width $2d$ but we need to consider just two boxes of size $d \times d$ rather than eight boxes of size $(d/2) \times (d/2)$. The recurrence relation is the same as the recurrence relation in Example 12, except that the coefficient 7 is replaced by 1. 29. With $k = \log_b n$, it follows that $f(n) = a^k f(1) + \sum_{j=0}^{k-1} a^j c(n/b^j)^d = a^k f(1) + \sum_{j=0}^{k-1} cn^d = a^k f(1) + kcn^d = a^{\log_b n} f(1) + c(\log_b n)n^d = n^{\log_b a} f(1) + cn^d \log_b n = n^d f(1) + cn^d \log_b n$. 31. Let $k = \log_b n$ where n is a power of b. *Basis step:* If $n = 1$ and $k = 0$, then $c_1 n^d + c_2 n^{\log_b a} = c_1 + c_2 = b^d c/(b^d - a) + f(1) + b^d c/(a - b^d) = f(1)$. *Inductive step:* Assume true for k, where $n = b^k$. Then for $n = b^{k+1}$, $f(n) = af(n/b) + cn^d = a\{[b^d c/(b^d - a)](n/b)^d + [f(1) + b^d c/(a - b^d)] \cdot (n/b)^{\log_b a})\} + cn^d = b^d c/(b^d - a)n^d a/b^d + [f(1) + b^d c/(a - b^d)]n^{\log_b a} + cn^d = n^d[ac/(b^d - a) + c(b^d - a)/(b^d - a)] + [f(1) + b^d c/(a - b^d c)]n^{\log_b a} = [b^d c/(b^d - a)]n^d + [f(1) + b^d c/(a - b^d)]n^{\log_b a}$. 33. If $a > b^d$, then $\log_b a > d$, so the second term dominates, giving $O(n^{\log_b a})$. 35. $O(n^{\log_4 5})$ 37. $O(n^3)$

Section 8.4

1. $f(x) = 2(x^6 - 1)/(x - 1)$ 3. **a)** $f(x) = 2x(1 - x^6)/(1 - x)$ **b)** $x^3/(1 - x)$ **c)** $x/(1 - x^3)$ **d)** $2/(1 - 2x)$ **e)** $(1 + x)^7$ **f)** $2/(1+x)$ **g)** $[1/(1-x)] - x^2$ **h)** $x^3/(1-x)^2$ 5. **a)** $5/(1-x)$ **b)** $1/(1-3x)$ **c)** $2x^3/(1-x)$ **d)** $(3-x)/(1-x)^2$ **e)** $(1+x)^8$ 7. **a)** $a_0 = -64$, $a_1 = 144$, $a_2 = -108$, $a_3 = 27$, and $a_n = 0$ for all $n \geq 4$ **b)** The only nonzero coefficients are $a_0 = 1$, $a_3 = 3$, $a_6 = 3$, $a_9 = 1$. **c)** $a_n = 5^n$ **d)** $a_n = (-3)^{n-3}$ for $n \geq 3$, and $a_0 = a_1 = a_2 = 0$ **e)** $a_0 = 8$, $a_1 = 3$, $a_2 = 2$, $a_n = 0$ for odd n greater than 2 and $a_n = 1$ for even n greater than 2 **f)** $a_n = 1$ if n is a positive multiple 4, $a_n = -1$ if $n < 4$, and $a_n = 0$ otherwise **g)** $a_n = n - 1$ for $n \geq 2$ and $a_0 = a_1 = 0$ **h)** $a_n = 2^{n+1}/n!$ 9. **a)** 6 **b)** 3 **c)** 9 **d)** 0 **e)** 5 11. **a)** 1024 **b)** 11 **c)** 66 **d)** 292,864 **e)** 20,412 13. 10 15. 50 17. 20 19. $f(x) = 1/[(1 - x)(1 - x^2)(1 - x^5)(1 - x^{10})]$ 21. 15 23. **a)** $x^4(1 + x + x^2 + x^3)^2/(1 - x)$ **b)** 6 25. **a)** The coefficient of x^r in the power series expansion of $1/[(1-x^3)(1-x^4)(1-x^{20})]$ **b)** $1/(1 - x^3 - x^4 - x^{20})$ **c)** 7 **d)** 3224 27. **a)** 3 **b)** 29 **c)** 29 **d)** 242 29. **a)** 10 **b)** 49 **c)** 2 **d)** 4 31. **a)** $G(x) - a_0 - a_1 x - a_2 x^2$ **b)** $G(x^2)$ **c)** $x^4 G(x)$ **d)** $G(2x)$ **e)** $\int_0^x G(t)dt$ **f)** $G(x)/(1-x)$ 33. $a_k = 2 \cdot 3^k - 1$ 35. $a_k = 18 \cdot 3^k - 12 \cdot 2^k$ 37. $a_k = k^2 + 8k + 20 + (6k - 18)2^k$ 39. Let $G(x) = \sum_{k=0}^{\infty} f_k x^k$. After shifting indices of summation and adding series, we see that $G(x) - xG(x) - x^2 G(x) = f_0 + (f_1 - f_0)x + \sum_{k=2}^{\infty}(f_k - f_{k-1} - f_{k-2})x^k = 0 + x + \sum_{k=2}^{\infty} 0x^k$. Hence, $G(x) - xG(x) - x^2G(x) = x$. Solving for $G(x)$ gives $G(x) = x/(1 - x - x^2)$. By the method of partial fractions, it can be shown that $x/(1 - x - x^2) = (1/\sqrt{5})[1/(1 - \alpha x) - 1/(1 - \beta x)]$, where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Using the fact that $1/(1 - \alpha x) = \sum_{k=0}^{\infty} \alpha^k x^k$, it follows that $G(x) = (1/\sqrt{5}) \cdot \sum_{k=0}^{\infty}(\alpha^k - \beta^k)x^k$. Hence, $f_k = (1/\sqrt{5}) \cdot (\alpha^k - \beta^k)$. 41. **a)** Let $G(x) = \sum_{n=0}^{\infty} C_n x^n$ be the generating function for $\{C_n\}$. Then $G(x)^2 = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} C_k C_{n-k})\, x^n = \sum_{n=1}^{\infty}(\sum_{k=0}^{n-1} C_k C_{n-1-k})x^{n-1} = \sum_{n=1}^{\infty} C_n x^{n-1}$. Hence, $xG(x)^2 = \sum_{n=1}^{\infty} C_n x^n$, which implies that $xG(x)^2 - G(x) + 1 = 0$. Applying the quadratic formula shows that $G(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$. We choose the minus sign in this formula because the choice of the plus sign leads to a division by zero. **b)** By Exercise 40, $(1 - 4x)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} x^n$. Integrating term by term (which is valid by a theorem from calculus) shows that $\int_0^x (1 - 4t)^{-1/2} dt = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^{n+1} = x \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^n$. Because $\int_0^x (1-4t)^{-1/2} dt = \frac{1 - \sqrt{1-4x}}{2} = xG(x)$, equating coefficients shows that $C_n = \frac{1}{n+1}\binom{2n}{n}$. **c)** Verify the basis step for $n = 1, 2, 3, 4, 5$. Assume the inductive hypothesis that $C_j \geq 2^{j-1}$ for $1 \leq j < n$, where $n \geq 6$. Then $C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1} \geq \sum_{k=1}^{n-2} C_k C_{n-k-1} \geq (n-2)2^{k-1}2^{n-k-2} = (n-2)2^{n-1}/4 \geq 2^{n-1}$. 43. Applying the binomial theorem to the equality $(1 + x)^{m+n} = (1 + x)^m (1 + x)^n$, shows that $\sum_{r=0}^{m+n} C(m + n, r)x^r = \sum_{r=0}^{m} C(m, r)x^r \cdot \sum_{r=0} C(n, r)\, x^r = \sum_{r=0}^{m+n} \left[\sum_{k=0}^{r} C(m, r - k)\, C(n, k)\right] x^r$. Comparing coefficients gives the desired identity. 45. **a)** $2e^x$ **b)** e^{-x} **c)** e^{3x} **d)** $xe^x + e^x$ 47. **a)** $a_n = (-1)^n$ **b)** $a_n = 3 \cdot 2^n$

c) $a_n = 3^n - 3 \cdot 2^n$ **d)** $a_n = (-2)^n$ for $n \geq 2$, $a_1 = -3$, $a_0 = 2$ **e)** $a_n = (-2)^n + n!$ **f)** $a_n = (-3)^n + n! \cdot 2^n$ for $n \geq 2$, $a_0 = 1$, $a_1 = -2$ **g)** $a_n = 0$ if n is odd and $a_n = n!/(n/2)!$ if n is even 49. **a)** $a_n = 6a_{n-1} + 8^{n-1}$ for $n \geq 1$, $a_0 = 1$ **b)** The general solution of the associated linear homogeneous recurrence relation is $a_n^{(h)} = \alpha 6^n$. A particular solution is $a_n^{(p)} = \frac{1}{2} \cdot 8^n$. Hence, the general solution is $a_n = \alpha 6^n + \frac{1}{2} \cdot 8^n$. Using the initial condition, it follows that $\alpha = \frac{1}{2}$. Hence, $a_n = (6^n + 8^n)/2$. **c)** Let $G(x) = \sum_{k=0}^{\infty} a_k x^k$. Using the recurrence relation for $\{a_k\}$, it can be shown that $G(x) - 6xG(x) = (1-7x)/(1-8x)$. Hence, $G(x) = (1-7x)/[(1-6x)(1-8x)]$. Using partial fractions, it follows that $G(x) = (1/2)/(1-6x) + (1/2)/(1-8x)$. With the help of Table 1, it follows that $a_n = (6^n + 8^n)/2$. 51. $\frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots$ 53. $(1+x)(1+x)^2(1+x)^3 \cdots$ 55. The generating functions obtained in Exercises 52 and 53 are equal because $(1+x)(1+x^2)(1+x^3)\cdots = \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^6}{1-x^3} \cdots = \frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \frac{1}{1-x^5} \cdots$. 57. **a)** $G_X(1) = \sum_{k=0}^{\infty} p(X=k) \cdot 1^k = \sum_{k=0}^{\infty} P(X=k) = 1$ **b)** $G'_X(1) = \frac{d}{dx} \sum_{k=0}^{\infty} p(X=k) \cdot x^k |_{x=1} = \sum_{k=0}^{\infty} p(X=k) \cdot k \cdot x^{k-1} |_{x=1} = \sum_{k=0}^{\infty} p(X=k) \cdot k = E(X)$ **c)** $G''_X(1) = \frac{d^2}{dx^2} \sum_{k=0}^{\infty} p(X=k) \cdot x^k |_{x=1} = \sum_{k=0}^{\infty} p(X=k) \cdot k(k-1) \cdot x^{k-2} |_{x=1} = \sum_{k=0}^{\infty} p(X=k) \cdot (k^2 - k) = V(X) + E(X)^2 - E(X)$. Combining this with part (b) gives the desired results. 59. **a)** $G(x) = p^m/(1-qx)^m$ **b)** $V(x) = mq/p^2$

Section 8.5

1. **a)** 30 **b)** 29 **c)** 24 **d)** 18 3. 1% 5. **a)** 300 **b)** 150 **c)** 175 **d)** 100 7. 492 9. 974 11. 55 13. 248 15. 50,138 17. 234 19. $|A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5| = |A_1| + |A_2| + |A_3| + |A_4| + |A_5| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_1 \cap A_5| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_2 \cap A_5| - |A_3 \cap A_4| - |A_3 \cap A_5| - |A_4 \cap A_5| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_2 \cap A_5| + |A_1 \cap A_3 \cap A_4| + |A_1 \cap A_3 \cap A_5| + |A_1 \cap A_4 \cap A_5| + |A_2 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_5| + |A_2 \cap A_4 \cap A_5| + |A_3 \cap A_4 \cap A_5| - |A_1 \cap A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_5| - |A_1 \cap A_2 \cap A_4 \cap A_5| - |A_1 \cap A_3 \cap A_4 \cap A_5| - |A_2 \cap A_3 \cap A_4 \cap A_5| + |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5|$ 21. $|A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6| = |A_1| + |A_2| + |A_3| + |A_4| + |A_5| + |A_6| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_1 \cap A_5| - |A_1 \cap A_6| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_2 \cap A_5| - |A_2 \cap A_6| - |A_3 \cap A_4| - |A_3 \cap A_5| - |A_3 \cap A_6| - |A_4 \cap A_5| - |A_4 \cap A_6| - |A_5 \cap A_6|$ 23. $p(E_1 \cup E_2 \cup E_3) = p(E_1) + p(E_2) + p(E_3) - p(E_1 \cap E_2) - p(E_1 \cap E_3) - p(E_2 \cap E_3) + p(E_1 \cap E_2 \cap E_3)$ 25. 4972/71,295 27. $p(E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5) = p(E_1) + p(E_2) + p(E_3) + p(E_4) + p(E_5) - p(E_1 \cap E_2) - p(E_1 \cap E_3) - p(E_1 \cap E_4) - p(E_1 \cap E_5) - p(E_2 \cap E_3) - p(E_2 \cap E_4) - p(E_2 \cap E_5) - p(E_3 \cap E_4) - p(E_3 \cap E_5) - p(E_4 \cap E_5) + p(E_1 \cap E_2 \cap E_3) + p(E_1 \cap E_2 \cap E_4) + p(E_1 \cap E_2 \cap E_5) + p(E_1 \cap E_3 \cap E_4) + p(E_1 \cap E_3 \cap E_5) + p(E_1 \cap E_4 \cap E_5) + p(E_2 \cap E_3 \cap E_4) + P(E_2 \cap E_3 \cap E_5) + p(E_2 \cap E_4 \cap E_5) + p(E_3 \cap E_4 \cap E_5)$ 29. $p\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{1 \leq i \leq n} p(E_i) - \sum_{1 \leq i < j \leq n} p(E_i \cap E_j) + \sum_{1 \leq i < j < k \leq n} p(E_i \cap E_j \cap E_k) - \cdots + (-1)^{n+1} p\left(\bigcap_{i=1}^{n} E_i\right)$

Section 8.6

1. 75 3. 6 5. 46 7. 9875 9. 540 11. 2100 13. 1854 15. **a)** $D_{100}/100!$ **b)** $100D_{99}/100!$ **c)** $C(100,2)/100!$ **d)** 0 **e)** $1/100!$ 17. 2,170,680 19. By Exercise 18 we have $D_n - nD_{n-1} = -[D_{n-1} - (n-1)D_{n-2}]$. Iterating, we have $D_n - nD_{n-1} = -[D_{n-1} - (n-1)D_{n-2}] = -[-(D_{n-2} - (n-2)D_{n-3})] = D_{n-2} - (n-2)D_{n-3} = \cdots = (-1)^n(D_2 - 2D_1) = (-1)^n$ because $D_2 = 1$ and $D_1 = 0$. 21. When n is odd 23. $\phi(n) = n - \sum_{i=1}^{m} \frac{n}{p_i} + \sum_{1 \leq i < j \leq m} \frac{n}{p_i p_j} - \cdots \pm \frac{n}{p_1 p_2 \cdots p_m} = n \prod_{i=1}^{m} \left(a - \frac{1}{p_i}\right)$ 25. 4 27. There are n^m functions from a set with m elements to a set with n elements, $C(n, 1)(n-1)^m$ functions from a set with m elements to a set with n elements that miss exactly one element, $C(n, 2)(n-2)^m$ functions from a set with m elements to a set with n elements that miss exactly two elements, and so on, with $C(n, n-1) \cdot 1^m$ functions from a set with m elements to a set with n elements that miss exactly $n-1$ elements. Hence, by the principle of inclusion–exclusion, there are $n^m - C(n, 1)(n-1)^m + C(n, 2)(n-2)^m - \cdots + (-1)^{n-1}C(n, n-1) \cdot 1^m$ onto functions.

Supplementary Exercises

1. **a)** $A_n = 4A_{n-1}$ **b)** $A_1 = 40$ **c)** $A_n = 10 \cdot 4^n$ 3. **a)** $M_n = M_{n-1} + 160{,}000$ **b)** $M_1 = 186{,}000$ **c)** $M_n = 160{,}000n + 26{,}000$ **d)** $T_n = T_{n-1} + 160{,}000n + 26{,}000$ **e)** $T_n = 80{,}000n^2 + 106{,}000n$ 5. **a)** $a_n = a_{n-2} + a_{n-3}$ **b)** $a_1 = 0, a_2 = 1, a_3 = 1$ **c)** $a_{12} = 12$ 7. **a)** 2 **b)** 5 **c)** 8 **d)** 16 9. $a_n = 2^n$ 11. $a_n = 2 + 4n/3 + n^2/2 + n^3/6$ 13. $a_n = a_{n-2} + a_{n-3}$ 15. **a)** Under the given conditions, one longest common subsequence clearly ends at the last term in each sequence, so $a_m = b_n = c_p$. Furthermore, a longest common subsequence of what is left of the a-sequence and the b-sequence after those last terms are deleted has to form the beginning of a longest common subsequence of the original sequences. **b)** If $c_p \neq a_m$, then the longest common subsequence's appearance in the a-sequence must terminate before the end; therefore the c-sequence must be a longest common subsequence of $a_1, a_2, \ldots, a_{m-1}$ and $b_1, b_2, \ldots, b_n$. The other half is similar.

17.
```
procedure howlong(a_1, ..., a_m, b_1, ..., b_n: sequences)
for i := 1 to m
    L(i, 0) := 0
for j := 1 to n
    L(0, j) := 0
for i := 1 to m
    for j := 1 to n
        if a_i = b_j then L(i, j) := L(i − 1, j − 1) + 1
        else L(i, j) := max(L(i, j − 1), L(i − 1, j))
return L(m, n)
```