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. **43.** 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 41), there are a countable number of bit strings. **45.** 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 41 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 36, it is itself a countable set. **47.** Exercise 45 shows that there are only a countable number of computer programs. Consequently, there are only a countable number of computable functions. Because, as Exercise 46 shows, there are an uncountable number of functions, not all functions are computable.

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)** $|\emptyset| \leq |A \cap B| \leq |A| \leq |A \cup B| \leq |U|$ **b)** $|\emptyset| \leq |A - B| \leq |A \oplus B| \leq |A \cup B| \leq |A| + |B|$ **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.** Let $f(a) = f(b) = 1$, $f(c) = f(d) = 2$, $S = \{a, c\}$, $T = \{b, d\}$. Then $f(S \cap T) = f(\emptyset) = \emptyset$, but $f(S) \cap f(T) = \{1, 2\} \cap \{1, 2\} = \{1, 2\}$. **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 $0 \leq \epsilon < 1/m$. 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.

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 *sum*($a_1, \ldots, a_n$: integers)
  $sum := a_1$
  for i := 2 **to** n
    $sum := sum + a_i$
  {*sum* has desired value}

5. procedure *duplicates* ($a_1, a_2, \ldots, a_n$: integers in nondecreasing order)
  $k := 0$ {this counts the duplicates}
  $j := 2$
  while $j \leq n$
  begin
    if $a_j = a_{j-1}$ **then**
    begin
      $k := k + 1$
      $c_k := a_j$
      while ($j \leq n$ and $a_j = c_k$)
        $j := j + 1$
    end
  $j := j + 1$
  end {$c_1, c_2, \ldots, c_k$ 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** $k := i$
  end {k is the desired location (or 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 $a_i \neq a_{n+1-i}$ **then** *answer* := **false**
  end {*answer* is true iff string is a palindrome}

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: $a_1 \leq a_2 \leq \cdots \leq a_n$}
  $a_{n+1} := x + 1$
  $i := 1$

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
begin
  if *max* < a_i **then**
  begin
    max := a_i
    location := i
  end
end

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 $\geq$ will be handled separately}
if $a > b$ **then**
begin
  if $b > c$ **then**
  median := b; *max* := a; *min* := c
end
...
(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**
  begin
    hit($f(a_j)$) := 1
    count := *count* + 1
  end
if *count* = m **then** *onto* := **true**
else *onto* := **false**

25. **procedure** *ones*(a: bit string, $a = a_1 a_2 \ldots a_n$)
ones:= 0
for $i := 1$ **to** n
begin
  if $a_i := 1$ **then**
    ones := *ones* + 1
  end {*ones* is the number of ones in the bit strings a}

27. **procedure** *ternary search*(s: integer, $a_1, a_2, \ldots, a_n$: increasing integers)
$i := 1$
$j := n$
while $i < j - 1$
begin
  $l = \lfloor (i + j)/3 \rfloor$
  $u = \lfloor 2(i + j)/3 \rfloor$
  if $x > a_u$ **then** $i := u + 1$
  else if $x > a_l$ **then**
  begin
    $i := l + 1$
    $j := u$
  end
  else $j := l$
end
if $x = a_i$ **then** *location* := i
else if $x = a_j$ **then** *location* := j
else *location* := 0
{*location* is the subscript of the term equal to x (0 if not found)}

29. **procedure** *find a mode*($a_1, a_2, \ldots, a_n$: nondecreasing integers)
modecount := 0
$i := 1$
while $i \leq n$
begin
  value := a_i
  count := 1
  while $i \leq n$ and a_i = *value*
  begin
    count := *count* + 1
    $i := i + 1$
  end
  if *count* > *modecount* **then**
  begin
    modecount := *count*
    mode := *value*
  end
end
{*mode* is the first value occurring most often}

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

33. **procedure** *find decrease*($a_1, a_2, \ldots, a_n$: positive integers)
location := 0
$i := 2$
while $i \leq n$ and *location* = 0

if $a_i < a_{i-1}$ **then** *location* := i
else $i := i + 1$
{*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* ($a_1, \ldots, a_n$: integers)
$i := 1$; *done* := **false**
while ($i < n$ and *done* = **false**)
begin
done := **true**
for $j := 1$ **to** $n - i$
if $a_j > a_{j+1}$ **then**
begin
interchange a_j and a_{j+1}
done := **false**
end
$i := i + 1$
end {$a_1, \ldots, a_n$ 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*($a_1, a_2, \ldots, a_n$: real numbers with $n \geq 2$)
for $j := 2$ **to** n
begin
{binary search for insertion location i}
left := 1
right := $j - 1$
while *left* < *right*
begin
middle := $\lfloor (left + right)/2 \rfloor$
if $a_j > a_{middle}$ **then** *left* := *middle* + 1
else *right* := *middle*
end
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** $j - i - 1$
$a_{j-k} := a_{j-k-1}$
$a_i := m$
end {$a_1, a_2, \ldots, a_n$ 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. a)** The variable f will give the finishing time of the talk last selected, starting out with f equal to the time the hall becomes available. Order the talks in increasing order of the ending times, and start at the top of the list. At each stage of the algorithm, go down the list of talks from where it left off, and find the first one whose starting time is not less than f. Schedule that talk and update f to record its finishing time. **b)** 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)** Here we assume that the men are the suitors and the women the suitees.
procedure *stable*($M_1, M_2, \ldots, M_s, W_1, W_2, \ldots, W_s$: 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
begin
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
end
for $j := 1$ **to** s
match j with the one man on j's proposal list
{This matching is stable.}

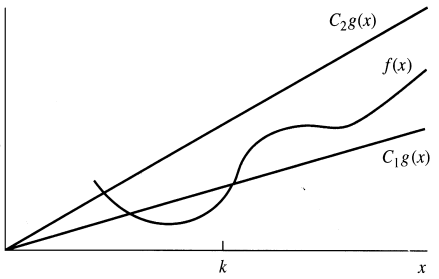
b) There are at most s^2 iterations of the **while** loop, so the algorithm must terminate. Indeed, if at the conclusion of the **while** loop rejected men remain, then some man must have been rejected and so his rejection list grew. Thus, each pass through the **while** loop, at least one more of the s^2 possible rejections will have been recorded, unless the loop is about to terminate. Furthermore, when the **while** loop terminates, each man will have one pending proposal, and each woman will have at most one pending proposal, so the assignment must be one-to-one. **c)** 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. **61.** 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.** $x^4 + 9x^3 + 4x + 7 \leq 4x^4$ 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.** $x^2 + 4x + 17 \leq 3x^3$ 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 $x^3 \leq C(x^2 + 4x + 17) \leq 3Cx^2$ for some C, for all sufficiently large x, which implies that $x \leq 3C$ for all sufficiently large x, which is impossible. Hence, x^3 is not $O(x^2 + 4x + 17)$. **11.** $3x^4 + 1 \leq 4x^4 = 8(x^4/2)$ for all $x > 1$, so $3x^4 + 1$ is $O(x^4/2)$, with witnesses $C = 8$, $k = 1$. Also $x^4/2 \leq 3x^4 + 1$ for all $x > 0$, so $x^4/2$ is $O(3x^4 + 1)$, with witnesses $C = 1$, $k = 0$. **13.** Because $2^n \leq 3^n$ 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, $3^n \leq C \cdot 2^n$ for all sufficiently large n. This says that $C \geq (3/2)^n$ 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 $|f(x)| \leq C$ 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 $|f(x)| \leq C_1|g(x)|$ for all $x > k_1$ and $|g(x)| \leq C_2|h(x)|$ for all $x > k_2$. Hence, for $x > \max(k_1, k_2)$ it follows that $|f(x)| \leq C_1|g(x)| \leq C_1C_2|h(x)|$. This shows that $f(x)$ is $O(h(x))$. **19. a)** $O(n^3)$ **b)** $O(n^5)$ **c)** $O(n^3 \cdot n!)$ **21. a)** $O(n^2 \log n)$ **b)** $O(n^2(\log n)^2)$ **c)** $O(n^{2^n})$ **23. 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 $\Theta(x^2)$ **25.** If $f(x)$ is $\Theta(g(x))$, then there exist constants C_1 and C_2 with $C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$. It follows that $|f(x)| \leq C_2|g(x)|$ and $|g(x)| \leq (1/C_1)|f(x)|$ 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 $|f(x)| \leq C_1|g(x)|$ for $x > k_1$ and $|g(x)| \leq C_2|f(x)|$ for $x > k_2$. We can assume that $C_2 > 0$ (we can always make C_2 larger). Then we have $(1/C_2)|g(x)| \leq |f(x)| \leq C_1|g(x)|$ for $x > \max(k_1, k_2)$. Hence, $f(x)$ is $\Theta(g(x))$. **27.** 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 $|f(x)| \leq C_2|g(x)|$ for all $x > k_2$ and $|f(x)| \geq C_1|g(x)|$ for all $x > k_1$. It follows that $C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$ whenever $x > k$, where $k = \max(k_1, k_2)$. Conversely, if there are positive constants C_1, C_2, and k such that $C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$ for $x > k$, then taking $k_1 = k_2 = k$ shows that $f(x)$ is both $O(g(x))$ and $\Theta(g(x))$.

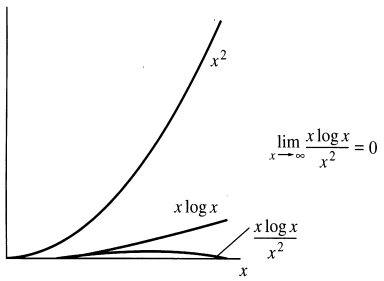
29.



31. 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. **33.** Because $f(x)$ is $O(g(x))$, there are constants C and l such that $|f(x)| \leq C|g(x)|$ for $x > l$. Hence, $|f^k(x)| \leq C^k|g^k(x)|$ for $x > l$, so $f^k(x)$ is $O(g^k(x))$ by taking the constant to be C^k. **35.** Because $f(x)$ and $g(x)$ are increasing and unbounded, we can assume $f(x) \geq 1$ and $g(x) \geq 1$ for sufficiently large x. There are constants C and k with $f(x) \leq Cg(x)$ for $x > k$. This implies that $\log f(x) \leq \log C + \log g(x) < 2 \log g(x)$ for sufficiently large x. Hence, $\log f(x)$ is $O(\log g(x))$. **37.** 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 $f_1(x) \geq C_1|g(x)|$ for all $x > k_1$, $f_1(x) \leq C_1'|g(x)|$ for all $x > k_1'$, $f_2(x) \geq C_2|g(x)|$ for all $x > k_2$, and $f_2(x) \leq C_2'|g(x)|$ for all $x > k_2'$. Adding the first and third inequalities shows that $f_1(x) + f_2(x) \geq (C_1 + C_2)|g(x)|$ for all $x > k$ where $k = \max(k_1, k_2)$. Adding the second and fourth inequalities shows that $f_1(x) + f_2(x) \leq (C_1' + C_2')|g(x)|$ 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. **39.** 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. **41.** 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. **43.** There are positive constants C_1, C_2, C_1', C_2', k_1, k_1', k_2, and k_2' such that $|f_1(x)| \geq C_1|g_1(x)|$ for all $x > k_1$, $|f_1(x)| \leq C_1'|g_1(x)|$ for all $x \geq k_1'$, $|f_2(x)| > C_2|g_2(x)|$ for all $x > k_2$, and $|f_2(x)| \leq C_2'|g_2(x)|$ for all $x > k_2'$. Because f_2 and g_2 are never zero, the last two inequalities can be rewritten as $|1/f_2(x)| \leq (1/C_2)|1/g_2(x)|$ for all $x > k_2$ and $|1/f_2(x)| \geq (1/C_2')|1/g_2(x)|$ for all $x > k_2'$. Multiplying the first and rewritten fourth inequalities shows that $|f_1(x)/f_2(x)| \geq (C_1/C_2')|g_1(x)/g_2(x)|$ for all $x > \max(k_1, k_2')$, and multiplying the second and rewritten third inequalities gives $|f_1(x)/f_2(x)| \leq (C_1'/C_2)|g_1(x)/g_2(x)|$ for all $x > \max(k_1', k_2)$. It follows that f_1/f_2 is big-Theta of g_1/g_2. **45.** There exist positive constants $C_1, C_2, k_1, k_2, k_1', k_2'$ such that $|f(x, y)| \leq C_1|g(x, y)|$ for

all $x > k_1$ and $y > k_2$ and $|f(x, y)| \geq C_2|g(x, y)|$ for all $x > k_1'$ and $y > k_2'$. **47.** $(x^2 + xy + x\log y)^3 < (3x^2y^3) = 27x^6y^3$ 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 $O(x^6y^3)$. **49.** For all positive real numbers x and y, $\lfloor xy \rfloor \leq xy$. Hence, $\lfloor xy \rfloor$ is $O(xy)$ from the definition, taking $C = 1$ and $k_1 = k_2 = 0$. **51.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)** $\lim_{x\to\infty} \frac{x^2+x+1}{x^2} = \lim_{x\to\infty} \left(1 + \frac{1}{x} + \frac{1}{x^2}\right) = 1 \neq 0$

53.



55. No. Take $f(x) = 1/x^2$ and $g(x) = 1/x$. **57. 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 $f(x)/g(x) = 1$. **59.** Because $f_2(x)$ is $o(g(x))$, from Exercise 57(a) it follows that $f_2(x)$ is $O(g(x))$. By Corollary 1, we have $f_1(x) + f_2(x)$ is $O(g(x))$. **61.** We can easily show that $(n - i)(i + 1) \geq n$ for $i = 0, 1, \ldots, n - 1$. Hence, $(n!)^2 = (n \cdot 1)((n - 1) \cdot 2) \cdot ((n - 2) \cdot 3) \cdots (2 \cdot (n - 1)) \cdot (1 \cdot n) \geq n^n$. Therefore, $2 \log n! \geq n \log n$. **63.** Compute that $\log 5! \approx 6.9$ and $(5 \log 5)/4 \approx 2.9$, so the inequality holds for $n = 5$. Assume $n \geq 6$. 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 $\log n - 1 > (\log n)/2$. **65.** All are not asymptotic.

Section 3.3

1. $2n - 1$ **3.** Linear **5.** $O(n)$ **7. a)** *power* := 1, y := 1; i := 1, *power* := 2, y := 3; i := 2, *power* := 4, y := 15 **b)** $2n$ multiplications and n additions **9. 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 **11. a)** 36 years **b)** 13 days **c)** 19 minutes **13.** The average number of comparisons is $(3n + 4)/2$. **15.** $O(\log n)$ **17.** $O(n)$ **19.** $O(n^2)$ **21.** $O(n)$ **23.** $O(n)$ **25.** $O(\log n)$ comparisons; $O(n^2)$ swaps **27. a)** doubles **b)** increases by 1

Section 3.4

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.** If a **mod** $m = b$ **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 $0 \leq r < m$. It follows that $a - b = (q_1 - q_2)m$, so $m \mid (a - b)$. It follows that $a \equiv b \pmod m$. **13.** There is some b with $(b - 1)k < n \leq bk$. Hence, $(b - 1)k \leq n - 1 < bk$. Divide by k to obtain $b - 1 < n/k \leq b$ and $b - 1 \leq (n - 1)/k < b$. Hence, $\lceil n/k \rceil = b$ and $\lfloor (n - 1)/k \rfloor = b - 1$. **15.** x **mod** m if x **mod** $m \leq \lceil m/2 \rceil$ and $(x$ **mod** $m) - m$ if x **mod** $m > \lceil m/2 \rceil$ **17. a)** 1 **b)** 2 **c)** 3 **d)** 9 **19. a)** No **b)** No **c)** Yes **d)** No **21.** 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 $a \equiv b \pmod n$. **23. 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 $3^1 = 3 \not\equiv 4 \equiv 729 = 3^6 \pmod 5$. **25.** Because $a \equiv b \pmod m$, there exists an integer s such that $a = b + sm$, so $a - b = sm$. Then $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$, $k \geq 2$, is also a multiple of m. It follows that $a^k \equiv b^k \pmod m$. **27. a)** 7, 19, 7, 7, 18, 0 **b)** Take the next available space **mod** 31. **29.** 2, 6, 7, 10, 8, 2, 6, 7, 10, 8, ... **31. a)** GR QRW SDVV JR **b)** QB ABG CNFF TB **c)** QX UXM AHJJ ZX **33.** 4 **35.** The check digit of the ISBN for this book is valid because $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 + 10 \cdot 2 \equiv 0 \pmod{11}$.

Section 3.5

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.** 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. **9.** 3, 5, and 7 are primes of the desired form. **11.** 1, 7, 11, 13, 17, 19, 23, 29 **13. a)** Yes **b)** No **c)** Yes **d)** Yes **15.** 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. **17. a)** 2 **b)** 4 **c)** 12 **19.** $\phi(p^k) = p^k - p^{k-1}$ **21. a)** $3^5 \cdot 5^3$ **b)** 1 **c)** 23^{17} **d)** $41 \cdot 43 \cdot 53$ **e)** 1

f) 1111 **23. 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 **25.** gcd (92928, 123552) = 1056; lcm(92928, 123552) = 10,872,576; both products are 11,481,440,256. **27.** 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. **29. 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. **31.** 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 $3 \cdot 2 = 6$. **33.** $n = 1601$ is a counterexample. **35.** 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. **37.** 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 3.6

1. a) 1110 0111 **b)** 1 0001 1011 0100 **c)** 1 0111 1101 0110 1100 **3. a)** 31 **b)** 513 **c)** 341 **d)** 26,896 **5. a)** 1000 0000 1110 **b)** 1 0011 0101 1010 1011 **c)** 1010 1011 1011 1010 **d)** 1101 1110 1111 1010 11001110 1101 **7.** 1010 1011 1100 1101 1110 1111 **9.** $(B7B)_{16}$ **11.** 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 $(\ldots h_1h_1h_0)_{16}$. **13.** Group together blocks of three binary digits, adding up to two initial 0s if necessary, and translate each block of three binary digits into a single octal digit. **15.** $(1110111001010111010001)_2$, $(1273)_8$ **17.** Convert the given octal numeral to binary using Exercise 14, then convert from binary to hexadecimal using Example 6. **19.** 436 **21.** 27 **23. a)** 6 **b)** 3 **c)** 11 **d)** 3 **e)** 40 **f)** 12 **25.** 8 **27.** The binary expansion of the integer is the unique such sum. **29.** 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. **31.** 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. **33. a)** -6 **b)** 13 **c)** -14 **d)** 0 **35.** 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. **37.** 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 $a_{n-1} = 1$. **39. a)** -7 **b)** 13 **c)** -15 **d)** -1 **41.** 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. **43.** 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 $a_{n-1} = 1$. **45.** $4n$

47. procedure *Cantor*(x: positive integer)
  $n := 1$; $f := 1$
  while $(n + 1) \cdot f \leq x$
  begin
    $n := n + 1$
    $f := f \cdot n$
  end
  $y := x$
  while $n > 0$
  begin

$a_n := \lfloor y/f \rfloor$
$y := y - a_n \cdot f$
$f := f/n$
$n := n - 1$
end $\{x = a_n n! + a_{n-1}(n-1)! + \cdots + a_1 1!\}$

49. 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: $c = 1, s_5 = 1$

51. procedure *subtract*(a, b: positive integers, $a > b$,
$a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$,
$b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$)
$B := 0$ {B is the borrow}
for $j := 0$ **to** $n - 1$
begin
if $a_j \geq b_j + B$ **then**
begin
$s_j := a_j - b_j - B$
$B := 0$
end
else
begin
$s_j := a_j + 2 - b_j - B$
$B := 1$
end
end {$(s_{n-1}s_{n-2}\ldots s_1s_0)_2$ is the difference}

53. procedure *compare*(a, b: positive integers,
$a = (a_n a_{n-1}\ldots a_1a_0)_2$,
$b = (b_n b_{n-1}\ldots b_1b_0)_2$)
$k := n$
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"

55. $O(\log n)$ **57.** 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 8.

Section 3.7

1. 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)** $1 = 2468 \cdot 9999 + (-2221) \cdot 11111$ **3.** $15 \cdot 7 = 105 \equiv 1 \pmod{26}$ **5.** 7 **7.** 52 **9.** 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 2 that $b \equiv c \pmod{m}$. **11.** $x \equiv 8 \pmod{9}$ **13.** 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 1, we see that m' divides $a - b$, so $a \equiv b \pmod{m'}$. **15.** 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 $x \equiv 1 \pmod{p}$. **17. 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 $a^p \equiv a \pmod{p}$. **19.** All integers of the form $323 + 330k$, where k is an integer **21.** All integers of the form $16 + 252k$, where k is an integer **23.** Suppose that p is a prime appearing in the prime factorization of $m_1m_2\cdots m_n$. 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 $m_1m_2\cdots m_n$ divides $a - b$, so $a \equiv b \pmod{m_1m_2\cdots m_n}$. **25.** $x \equiv 1 \pmod{6}$ **27. 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 23 that $2^{340} \equiv 1 \pmod{341}$. **29. a)** 3, 4, 8 **b)** 983 **31.** 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. **33.** 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 23 (or the Chinese Remainder Theorem) it follows that $b^{2820} \equiv 1 \pmod{2821}$, as desired. **35. 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 34 are met, and we conclude that n is a Carmichael number. **b)** Letting $m = 51$ gives $n = 172{,}947{,}529$. **37.** $0 = (0, 0)$, $1 = (1, 1)$, $2 = (2, 2)$, $3 = (0, 3)$, $4 = (1, 4)$, $5 = (2, 0)$, $6 = (0, 1)$, $7 = (1, 2)$, $8 = (2, 3)$, $9 = (0, 4)$, $10 = (1, 0)$, $11 = (2, 1)$, $12 = (0, 2)$, $13 = (1, 3)$, $14 = (2, 4)$ **39.** 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 $65 \cdot 903{,}070 \cdot 37 + 2 \cdot 912{,}285 \cdot 33 + 51 \cdot 921{,}690 \cdot 24 + 10 \cdot 941{,}094 \cdot 4 = 3{,}397{,}886{,}480 \equiv 537{,}140 \pmod{89{,}403{,}930}$. **41.** By Exercise 40 it follows that $\gcd(2^b - 1, (2^a - 1) \bmod (2^b - 1)) = \gcd(2^b - 1, 2^{a \bmod b} - 1)$. Because the exponents involved in the calculation are b and $a \bmod b$, 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 $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. **43.** 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 41, $\gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p,q-1)} - 1$. 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. **45.** 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 $q = n/p$. **47.** SILVER **49.** $34 \cdot 144 + (-55) \cdot 89 = 1$

51. **procedure** *extended Euclidean* (a, b: positive integers)
$x := a$
$y := b$
$oldolds := 1$
$olds := 0$
$oldoldt := 0$
$oldt := 1$
while $y \neq 0$
begin
$q := x$ **div** y
$r := x$ **mod** y
$x := y$
$y := r$
$s := oldolds - q \cdot olds$
$t := oldoldt - q \cdot oldt$
$oldolds := olds$
$oldoldt := oldt$
$olds := s$
$oldt := t$
end {$\gcd(a, b)$ is x, and $(oldolds)a + (oldoldt)b = x$}

53. 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 2, $p \mid (s - t)$ or $p \mid (s + t)$, so $s \equiv t \pmod p$ or $s \equiv -t \pmod p$. Hence, there are at most two solutions. **55.** 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 $a \equiv b \pmod p$. **57.** By Exercise 56, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod p$. **59.** $x \equiv 8, 13, 22,$ or $27 \pmod{35}$ **61.** Suppose that we use a prime for n. To find a private decryption key from the corresponding public encryption key e, one would need to find a number d that is an inverse for e modulo $n - 1$ so that the calculation shown before Example 12 can go through. But finding such a d is easy using the Euclidean algorithm, because the person doing this would already know $n - 1$. In particular, to find d, one can work backward through the steps of the Euclidean algorithm to express 1 as a linear combination of e and $n - 1$; then d is the coefficient of e in this linear combination.

Section 3.8

1. a) 3×4 **b)** $\begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}$ **c)** $[2 \quad 0 \quad 4 \quad 6]$ **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.** $\mathbf{A}^n(\mathbf{A}^{-1})^n = \mathbf{A}(\mathbf{A} \cdots (\mathbf{A}(\mathbf{AA}^{-1})\mathbf{A}^{-1}) \cdots \mathbf{A}^{-1})\mathbf{A}^{-1}$ 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.** There are m_2 multiplications used to find each of the m_1m_3 entries of the product. Hence, $m_1m_2m_3$ multiplications are used. **25.** $\mathbf{A}_1((\mathbf{A}_2\mathbf{A}_3)\mathbf{A}_4)$ **27.** $x_1 = 1$, $x_2 = -1, x_3 = -2$

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

31. 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)** $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

33. a) $\mathbf{A} \vee \mathbf{B} = [a_{ij} \vee b_{ij}] = [b_{ij} \vee a_{ij}] = \mathbf{B} \vee \mathbf{A}$ **b)** $\mathbf{A} \wedge \mathbf{B} = [a_{ij} \wedge b_{ij}] = [b_{ij} \wedge a_{ij}] = \mathbf{B} \wedge \mathbf{A}$ **35. 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)** $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = [a_{ij}] \wedge [b_{ij} \vee c_{ij}] = [a_{ij} \wedge (b_{ij} \vee c_{ij})] = [(a_{ij} \wedge b_{ij}) \vee (a_{ij} \wedge c_{ij})] = [a_{ij} \wedge b_{ij}] \vee [a_{ij} \wedge c_{ij}] = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$ **37.** $\mathbf{A} \odot (\mathbf{B} \odot \mathbf{C}) = \left[\bigvee_q a_{iq} \wedge \left(\bigvee_r (b_{qr} \wedge c_{rl})\right)\right] = \left[\bigvee_q \bigvee_r (a_{iq} \wedge b_{qr} \wedge c_{rl})\right] = \left[\bigvee_r \bigvee_q (a_{iq} \wedge b_{qr} \wedge c_{rl})\right] = \left[\bigvee_r \left(\bigvee_q (a_{iq} \wedge b_{qr})\right) \wedge c_{rl}\right] = (\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C}$

Supplementary Exercises

1. a) **procedure** *last max*($a_1, \ldots, a_n$: integers)
  $max := a_1$
  $last := 1$
  $i := 2$
  while $i \leq n$
  begin
    if $a_i \geq max$ **then**
    begin
      $max := a_i$
      $last := i$
    end
    $i := i + 1$
  end {*last* is the location of final occurrence of largest integer in list}

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

3. a) **procedure** *pair zeros*($b_1b_2 \ldots b_n$: bit string, $n \geq 2$)
  $x := b_1$
  $y := b_2$
  $k := 2$
  while ($k < n$ and ($x \neq 0$ or $y \neq 0$))
  begin
    $k := k + 1$
    $x := y$
    $y := b_k$
  end
  if ($x = 0$ and $y = 0$) **then** print "YES"
  else print "NO"

b) $O(n)$ comparisons

5. a) and **b)**
  procedure *smallest and largest*($a_1, a_2, \ldots, a_n$: integers)
  $min := a_1$
  $max := a_1$
  for $i := 2$ **to** n
  begin
    if $a_i < min$ **then** $min := a_i$
    if $a_i > max$ **then** $max := a_i$
  end {*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.** 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 **11.** 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. **13.** Because $\log n < n$, we have $(n \log n + n^2)^3 \leq (n^2 + n^2)^3 \leq (2n^2)^3 = 8n^6$ for all $n > 0$. This proves that $(n \log n + n^2)^3$ is $O(n^6)$, with witnesses $C = 8$ and $k = 0$. **15.** $O(x^2 2^x)$ **17.** Note that $\frac{n!}{2^n} = \frac{n}{2} \cdot \frac{n-1}{2} \cdots \frac{3}{2} \cdot \frac{2}{2} \cdot \frac{1}{2} > \frac{n}{2} \cdot 1 \cdot 1 \cdots 1 \cdot \frac{1}{2} = \frac{n}{4}$. **19.** 5, 22, −12, −29 **21.** 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 $a \equiv b \pmod{m/d}$. **23.** 1 **25.** 1 **27.** $(a_n a_{n-1} \ldots a_1 a_0)_{10} = \sum_{k=0}^{n} 10^k a_k \equiv \sum_{k=0}^{n} a_k \pmod 9$ because $10^k \equiv 1 \pmod 9$ for every nonnegative integer k. **29.** If not, then suppose that $q_1, q_2, \ldots, q_n$ are all the primes of the form $6k + 5$. Let $Q = 6q_1q_2 \cdots q_n - 1$. Note that Q is of the form $6k + 5$, where $k = q_1q_2 \cdots q_n - 1$. Let $Q = p_1p_2 \cdots p_t$ 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. a)** Not mutually relatively prime **b)** Mutually relatively prime **c)** Mutually relatively prime **d)** Mutually relatively prime **33. a)** The decryption function is $g(q) = \bar{a}(q - b)$ **mod** 26, where $\bar{a}$ is an inverse of a modulo 26. **b)** PLEASE SEND MONEY **35.** $x \equiv 28 \pmod{30}$ **37.** 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. **39.** 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 $n = p + q$. **41.** $\mathbf{A}^{4n} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{A}^{4n+1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\mathbf{A}^{4n+2} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $\mathbf{A}^{4n+3} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, for $n \geq 0$ **43.** 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, $\mathbf{A} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = a\mathbf{I}$.

45. procedure *triangular matrix multiplication*(**A**, **B**: upper triangular $n \times n$ matrices, $\mathbf{A} = [a_{ij}]$, $\mathbf{B} = [b_{ij}]$)
  for $i := 1$ **to** n
  for $j := i$ **to** n
  begin
    $c_{ij} := 0$
    for $k := i$ **to** j
      $c_{ij} := c_{ij} + a_{ik}b_{kj}$
  end

47. $(\mathbf{AB})(\mathbf{B}^{-1}\mathbf{A}^{-1}) = \mathbf{A}(\mathbf{BB}^{-1})\mathbf{A}^{-1} = \mathbf{AIA}^{-1} = \mathbf{AA}^{-1} = \mathbf{I}$. Similarly, $(\mathbf{B}^{-1}\mathbf{A}^{-1})(\mathbf{AB}) = \mathbf{I}$. Hence, $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$. **49. 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 $\mathbf{0} \wedge \mathbf{A} = \mathbf{0}$. **51.** 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.

CHAPTER 4

Section 4.1

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)** $\sum_{j=1}^{n} 1/2^j =$