ONLINE INSTRUCTOR'S SOLUTIONS MANUAL

ELEMENTARY NUMBER THEORY AND ITS APPLICATIONS

SIXTH EDITION

Kenneth Rosen
Monmouth University

Addison-Wesley
is an imprint of
PEARSON

Reproduced by Pearson Addison-Wesley from electronic files supplied by the author.

Publishing as Addison-Wesley, 75 Arlington Street, Boston, MA 02116.

ISBN-13: 978-0-321-53801-7
ISBN-10: 0-321-53801-3

Contents

1

CHAPTER 1

The Integers

1.1. Numbers and Sequences

1.1.1. a. The set of integers greater than 3 is well-ordered. Every subset of this set is also a subset of the set of positive integers, and hence must have a least element.

b. The set of even positive integers is well-ordered. Every subset of this set is also a subset of the set of positive integers, and hence must have a least element.

c. The set of positive rational numbers is not well-ordered. This set does not have a least element. If a/b were the least positive rational number then $a/(b+a)$ would be a smaller positive rational number, which is a contradiction.

d. The set of positive rational numbers of the form $a/2$ is well-ordered. Consider a subset of numbers of this form. The set of numerators of the numbers in this subset is a subset of the set of positive integers, so it must have a least element b. Then $b/2$ is the least element of the subset.

e. The set of nonnegative rational numbers is not well-ordered. The set of positive rational numbers is a subset with no least element, as shown in part c.

1.1.2. Let S be the set of all positive integers of the form $a - bk$. S is not empty because $a - b(-1) = a + b$ is a positive integer. Then the well-ordering principle implies that S has a least element, which is the number we're looking for.

1.1.3. Suppose that x and y are rational numbers. Then $x = a/b$ and $y = c/d$, where a, b, c, and d are integers with $b \neq 0$ and $d \neq 0$. Then $xy = (a/b) \cdot (c/d) = ac/bd$ and $x + y = a/b + c/d = (ad + bc)/bd$ where $bd \neq 0$. Because both $x + y$ and xy are ratios of integers, they are both rational.

1.1.4. a. Suppose that x is rational and y is irrational. Then there exist integers a and b such that $x = \frac{a}{b}$ where a and b are integers with $b \neq 0$. Suppose that $x + y$ is rational. Then there exist integers c and d with $d \neq 0$ such that $x + y = \frac{c}{d}$. This implies that $y = (x + y) - x = (a/b) - (c/d) = (ad - bc)/bd$, which means that y is rational, a contradiction. Hence $x + y$ is irrational.

b. This is false. A counterexample is given by $\sqrt{2} + (-\sqrt{2}) = 0$.

c. This is false. A counterexample is given by $0 \cdot \sqrt{2} = 0$.

d. This is false. A counterexample is given by $\sqrt{2} \cdot \sqrt{2} = 2$.

1.1.5. Suppose that $\sqrt{3}$ were rational. Then there would exist positive integers a and b with $\sqrt{3} = a/b$. Consequently, the set $S = \{k\sqrt{3} \mid k \text{ and } k\sqrt{3} \text{ are positive integers}\}$ is nonempty because $a = b\sqrt{3}$. Therefore, by the well-ordering property, S has a smallest element, say $s = t\sqrt{3}$. We have $s\sqrt{3} - s = s\sqrt{3} - t\sqrt{3} = (s - t)\sqrt{3}$. Because $s\sqrt{3} = 3t$ and s are both integers, $s\sqrt{3} - s = (s - t)\sqrt{3}$ must also be an integer. Furthermore, it is positive, because $s\sqrt{3} - s = s(\sqrt{3} - 1)$ and $\sqrt{3} > 1$. It is less than s because $s = t\sqrt{3}$, $s\sqrt{3} = 3t$, and $\sqrt{3} < 3$. This contradicts the choice of s as the smallest positive integer in S. It follows that $\sqrt{3}$ is irrational.

1.1.6. Let S be a set of negative integers. Then the set $T = \{-s : s \in S\}$ is a set of positive integers. By the well-ordering principle, T has a least element t_0. We prove that $-t_0$ is a greatest element of S. First note that because $t_0 \in S$, then $t_0 = -s_0$ for some $s_0 \in S$. Then $-t_0 = s_0 \in S$. Second, if $s \in S$, then $-s \in T$, so $t_0 \leq -s$. Multiplying by -1 yields $s \leq -t_0$. Because the choice of s was arbitrary, we see that $-t_0$ is greater than or equal to every element of S.

1.1.7. a. Because $0 \leq 1/4 < 1$, we have $[1/4] = 0$.

b. Because $-1 \leq -3/4 < 0$, we have $[-3/4] = -1$.

c. Because $3 \leq 22/7 < 4$, we have $[22/7] = 3$.

d. Because $-2 \leq -2 < -1$, we have $[-2] = -2$.

e. We compute $[1/2 + [1/2]] = [1/2 + 0] = [1/2] = 0$.

f. We compute $[-3 + [-1/2]] = [-3 - 1] = [-4] = -4$.

1.1.8. a. Because $-1 \leq -1/4 < 0$, we have $[-1/4] = -1$.

b. Because $-4 \leq -22/7 < -3$, we have $[-22/7] = -4$.

c. Because $1 \leq 5/4 < 2$, we have $[5/4] = 1$.

d. We compute $[[1/2]] = [0] = 0$.

e. We compute $[[3/2] + [-3/2]] = [1 + (-2)] = [-1] = -1$.

f. We compute $[3 - [1/2]] = [3 - 0] = [3] = 3$.

1.1.9. a. Because $[8/5] = 1$, we have $\{8/5\} = 8/5 - [8/5] = 8/5 - 1 = 3/5$.

b. Because $[1/7] = 0$, we have $\{1/7\} = 1/7 - [1/7] = 1/7 - 0 = 1/7$.

c. Because $[-11/4] = -3$, we have $\{-11/4\} = -11/4 - [-11/4] = -11/4 - (-3) = 1/4$.

d. Because $[7] = 7$, we have $\{7\} = 7 - [7] = 7 - 7 = 0$.

1.1.10. a. Because $[-8/5] = -2$, we have $\{-8/5\} = -8/5 - [-8/5] = -8/5 - (-2) = 2/5$.

b. Because $[22/7] = 3$, we have $\{22/7\} = 22/7 - [22/7] = 22/7 - 3 = 1/7$.

c. Because $[-1] = -1$, we have $\{-1\} = -1 - [-1] = -1 - 1 = 0$.

d. Because $[-1/3] = -1$, we have $\{-1/3\} = -1/3 - [-1/3] = -1/3 - (-1) = 2/3$.

1.1.11. If x is an integer, then $[x] + [-x] = x - x = 0$. Otherwise, $x = z + r$, where z is an integer and r is a real number with $0 < r < 1$. In this case, $[x] + [-x] = [z + r] + [-z - r] = z + (-z - 1) = -1$.

1.1.12. Let $x = [x] + r$ where $0 \leq r < 1$. We consider two cases. First suppose that $r < \frac{1}{2}$. Then $x + \frac{1}{2} = [x] + (r + \frac{1}{2}) < [x] + 1$ because $r + \frac{1}{2} < 1$. It follows that $[x + \frac{1}{2}] = [x]$. Also $2x = 2[x] + 2r < 2[x] + 1$ because $2r < 1$. Hence $[2x] = 2[x]$. It follows that $[x] + [x + \frac{1}{2}] = [2x]$. Next suppose that $\frac{1}{2} \leq r < 1$. Then $[x] + 1 \leq x + (r + \frac{1}{2}) < [x] + 2$, so that $[x + \frac{1}{2}] = [x] + 1$. Also $2[x] + 1 \leq 2[x] + 2r = 2([x] + r) = 2x < 2[x] + 2$ so that $[2x] = 2[x] + 1$. It follows that $[x] + [x + \frac{1}{2}] = [x] + [x] + 1 = 2[x] + 1 = [2x]$.

1.1.13. We have $[x] \leq x$ and $[y] \leq y$. Adding these two inequalities gives $[x] + [y] \leq x + y$. Hence $[x + y] \geq [[x] + [y]] = [x] + [y]$.

1.1.14. Let $x = a+r$ and $y = b+s$, where a and b are integers and r and s are real numbers such that $0 \leq r, s < 1$. By Exercise 14, $[2x] + [2y] = [x] + [x + \frac{1}{2}] + [y] + [y + \frac{1}{2}]$. We now need to show that $[x + \frac{1}{2}] + [y + \frac{1}{2}] \geq [x + y]$. Suppose $0 \leq r, s < \frac{1}{2}$. Then $[x + \frac{1}{2}] + [y + \frac{1}{2}] = a + b + [r + \frac{1}{2}] + [s + \frac{1}{2}] = a + b$, and $[x + y] = a+b+[r+s] = a+b$, as desired. Suppose that $\frac{1}{2} \leq r, s < 1$. Then $[x+\frac{1}{2}]+[y+\frac{1}{2}] = a+b+[r+\frac{1}{2}]+[s+\frac{1}{2}] = a + b + 2$, and $[x + y] = a + b + [r + s] = a + b + 1$, as desired. Suppose that $0 \leq r < \frac{1}{2} \leq s < 1$. Then $[x + \frac{1}{2}] + [y + \frac{1}{2}] = a + b + 1$, and $[x + y] \leq a + b + 1$.

1.1.15. Let $x = a + r$ and $y = b + s$, where a and b are integers and r and s are real numbers such that $0 \leq r, s < 1$. Then $[xy] = [ab + as + br + sr] = ab + [as + br + sr]$, whereas $[x][y] = ab$. Thus we have $[xy] \geq [x][y]$ when x and y are both positive. If x and y are both negative, then $[xy] \leq [x][y]$. If one of x and y is positive and the other negative, then the inequality could go either direction. For examples take $x = -1.5, y = 5$ and $x = -1, y = 5.5$. In the first case we have $[-1.5 \cdot 5] = [-7.5] = -8 > [-1.5][5] = -2 \cdot 5 = -10$. In the second case we have $[-1 \cdot 5.5] = [-5.5] = -6 < [-1][5.5] = -1 \cdot 5 = -5$.

1.1.16. If x is an integer then $-[-x] = -(-x) = x$, which certainly is the least integer greater than or equal to x. Let $x = a + r$, where a is an integer and $0 < r < 1$. Then $-[-x] = -[-a - r] = -(-a + [-r]) = a - [-r] = a + 1$, as desired.

1.1.17. Let $x = [x] + r$. Because $0 \leq r < 1$, $x + \frac{1}{2} = [x] + r + \frac{1}{2}$. If $r < \frac{1}{2}$, then $[x]$ is the integer nearest to x and $[x + \frac{1}{2}] = [x]$ because $[x] \leq x + \frac{1}{2} = [x] + r + \frac{1}{2} < [x] + 1$. If $r \geq \frac{1}{2}$, then $[x] + 1$ is the integer nearest to x (choosing this integer if x is midway between $[x]$ and $[x + 1]$) and $[x + \frac{1}{2}] = [x] + 1$ because $[x] + 1 \leq x + r + \frac{1}{2} < [x] + 2$.

1.1.18. Let $y = x + n$. Then $[y] = [x] + n$, because n is an integer. Therefore the problem is equivalent to proving that $[y/m] = [[y]/m]$ which was done in Example 1.34.

1.1.19. Let $x = k + \epsilon$ where k is an integer and $0 \leq \epsilon < 1$. Further, let $k = a^2 + b$, where a is the largest integer such that $a^2 \leq k$. Then $a^2 \leq k = a^2 + b \leq x = a^2 + b + \epsilon < (a + 1)^2$. Then $[\sqrt{x}] = a$ and $[\sqrt{[x]}] = [\sqrt{k}] = a$ also, proving the theorem.

1.1.20. Let $x = k + \epsilon$ where k is an integer and $0 \leq \epsilon < 1$. Choose w from $0, 1, 2, \ldots, m - 1$ such that $w/m \leq \epsilon < (w + 1)/m$. Then $w \leq m\epsilon < w + 1$. Then $[mx] = [mk + m\epsilon] = mk + [m\epsilon] = mk + w$. On the other hand, the same inequality gives us $(w + j)/m \leq \epsilon + j/m < (w + 1 + j)/m$, for any integer $j = 0, 1, 2, \ldots, m - 1$. Note that this implies $[\epsilon + j/m] = [(w + j)/m]$ which is either 0 or 1 for j in this range. Indeed, it equals 1 precisely when $w+j \geq m$, which happens for exactly w values of j in this range. Now we compute $\sum_{j=0}^{m-1}[x + j/m] = \sum_{j=0}^{m-1}[k + \epsilon + j/m] = \sum_{j=0}^{m-1} k + [\epsilon + j/m] = mk + \sum_{j=0}^{m-1}[(w + j)/m] = mk + \sum_{j=m-w}^{m-1} 1 = mk + w$ which is the same as the value above.

1.1.21. a. Because the difference between any two consecutive terms of this sequence is 8, we may compute the nth term by adding 8 to the first term $n - 1$ times. That is, $a_n = 3 + (n - 1)8 = 8n - 5$.

b. For each n, we have $a_n - a_{n-1} = 2^{n-1}$, so we may compute the nth term of this sequence by adding all the powers of 2, up to the $(n - 1)$th, to the first term. Hence $a_n = 5 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 5 + 2^n - 2 = 2^n + 3$.

c. The nth term of this sequence appears to be zero, unless n is a perfect square, in which case the term is 1. If n is not a perfect square, then $[\sqrt{n}] < \sqrt{n}$, where $[x]$ represents the greatest integer function. If n is a perfect square, then $[\sqrt{n}] = \sqrt{n}$. Therefore, $[[\sqrt{n}]/\sqrt{n}]$ equals 1 if n is a perfect square and 0 otherwise, as desired.

d. This is a Fibonacci-like sequence, with $a_n = a_{n-1} + a_{n-2}$, for $n \geq 3$, and $a_1 = 1$, and $a_2 = 3$.

1.1.22. a. Each term given is 3 times the preceding term, so we conjecture that the nth term is the first term multiplied by 3, $n-1$ times. So $a_n = 2 \cdot 3^{n-1}$.

b. In this sequence, $a_n = 0$ if n is a multiple of 3, and equals 1 otherwise. Let $[x]$ represent the greatest integer function. Because $[n/3] < n/3$ when n is not a multiple of 3 and $[n/3] = n/3$ when n is a multiple of 3, we have that $a_n = 1 - [[n/3]/(n/3)]$.

c. If we look at the difference of successive terms, we have the sequence $1, 1, 2, 2, 3, 3, \ldots$. So if n is odd, say $n = 2k+1$, then a_n is obtained by adding $1+1+2+2+3+3+\cdots+k+k = 2t_k$ to the first term, which is 1. (Here t_k stands for the kth triangular number.) So if n is odd, then $a_n = 1 + 2t_k$ where $k = (n-1)/2$. If n is even, say $n = 2k$, then $a_n = a_{2k+1} - k = 1 - k + 2t_k$.

d. This is a Fibonacci-like sequence, with $a_n = a_{n-1} + 2a_{n-2}$, for $n \geq 3$, and $a_1 = 3$, and $a_2 = 5$.

1.1.23. Three possible answers are $a_n = 2^{n-1}$, $a_n = (n^2 - n + 2)/2$, and $a_n = a_{n-1} + 2a_{n-2}$.

1.1.24. Three possible answers are $a_n = a_{n-1}a_{n-2}$, $a_n = a_{n-1} + 2n - 3$, and $a_n =$ the number of letters in the nth word of the sentence "If our answer is correct we will join the Antidisestablishmentarianism Society and boldly state that 'If our answer is correct we will join the Antidisestablishmentarianism Society and boldly state....' "

1.1.25. This set is exactly the sequence $a_n = n - 100$, and hence is countable.

1.1.26. The function $f(n) = 5n$ is a one-to-one correspondence between this set and the set of integers, which is known to be countable.

1.1.27. One way to show this is to imitate the proof that the set of rational numbers is countable, replacing a/b with $a + b\sqrt{2}$. Another way is to consider the function $f(a + b\sqrt{2}) = 2^a 3^b$ which is a one-to-one map of this set into the rational numbers, which is known to be countable.

1.1.28. Let A and B be two countable sets. If one or both of the sets are finite, say A is finite, then the listing $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots$, where any b_i which is also in A is deleted from the list, demonstrates the countability of $A \cup B$. If both sets are infinite, then each can be represented as a sequence: $A = \{a_1, a_2, \ldots\}$, and $B = \{b_1, b_2, \ldots\}$. Consider the listing $a_1, b_1, a_2, b_2, a_3, b_3, \ldots$ and form a new sequence c_i as follows. Let $c_1 = a_1$. Given that c_n is determined, let c_{n+1} be the next element in the listing which is different from each c_i with $i = 1, 2, \ldots, n$. Then this sequence is exactly the elements of $A \cup B$, which is therefore countable.

1.1.29. Suppose $\{A_i\}$ is a countable collection of countable sets. Then each A_i can be represented by a sequence, as follows:

$$\begin{array}{lcllll} A_1 & = & a_{11} & a_{12} & a_{13} & \ldots \\ A_2 & = & a_{21} & a_{22} & a_{23} & \ldots \\ A_3 & = & a_{31} & a_{32} & a_{33} & \ldots \\ & \vdots & & & & \end{array}$$

Consider the listing $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \ldots$, in which we first list the elements with subscripts adding to 2, then the elements with subscripts adding to 3 and so on. Further, we order the elements with subscripts adding to k in order of the first subscript. Form a new sequence c_i as follows. Let $c_1 = a_1$. Given that c_n is determined, let c_{n+1} be the next element in the listing which is different from each c_i with $i = 1, 2, \ldots, n$. Then this sequence is exactly the elements of $\bigcup_{i=1}^{\infty} A_i$, which is therefore countable.

1.1.30. a. Note that $\sqrt{2} \approx 1.4 = 7/5$, so we might guess that $\sqrt{2} - 7/5 \approx 0$. If we multiply through by 5 we expect that $5\sqrt{2} - 7$ should be small, and its value is approximately 0.071 which is much less than $1/8 = 0.125$. So we may take $a = 5 \leq 8$ and $b = 7$.

b. As in part a., note that $\sqrt[3]{2} = 1.2599\ldots \approx 1.25 = 5/4$, so we investigate $4\sqrt[3]{2} - 5 = 0.039\ldots \leq 1/8$. So we may take $a = 4 \leq 8$ and $b = 5$.

c. Because we know that $\pi \approx 22/7$ we investigate $|7\pi - 22| = 0.0088\ldots \leq 1/8$. So we may take $a = 7 \leq 8$ and $b = 22$.

d. Because $e \approx 2.75 = 11/4$ we investigate $|4e - 11| = 0.126\ldots$, which is too large. A closer approximation to e is 2.718. We consider the decimal expansions of the multiples of $1/7$ and find that $5/7 = .714\ldots$, so $e \approx 19/7$. Therefore we investigate $|7e - 19| = 0.027 \leq 1/8$. So we may take $a = 7 \leq 8$ and $b = 19$.

1.1.31. a. Note that $\sqrt{3} = 1.73 \approx 7/4$, so we might guess that $\sqrt{3} - 7/4 \approx 0$. If we multiply through by 4 we find that $|4\sqrt{3} - 7| = 0.07\ldots < 1/10$. So we may take $a = 4 \leq 10$ and $b = 7$.

b. It is helpful to keep the decimal expansions of the multiples of $1/7$ in mind in these exercises. Here $\sqrt[3]{3} = 1.442\ldots$ and $3/7 = 0.428\ldots$ so that we have $\sqrt[3]{3} \approx 10/7$. Then, as in part a., we investigate $|7\sqrt[3]{3} - 10| = 0.095\ldots < 1/10$. So we may take $a = 7 \leq 10$ and $b = 10$.

c. Because $\pi^2 = 9.869\ldots$ and $6/7 = 0.857\ldots$, we have that $\pi^2 \approx 69/7$, so we compute $|7\pi^2 - 69| = 0.087\ldots < 1/10$. So we may take $a = 7 \leq 10$ and $b = 69$.

d. Because $e^3 = 20.0855\ldots$ we may take $a = 1$ and $b = 20$ to get $|1e^3 - 20| = 0.855\ldots < 1/10$.

1.1.32. For $j = 0, 1, 2, \ldots, n+1$, consider the $n+2$ numbers $\{j\alpha\}$, which all lie in the interval $0 \leq \{j\alpha\} < 1$. We can partition this interval into the $n+1$ subintervals $(k-1)/(n+1) \leq x < k/(n+1)$ for $k = 1, \ldots, n+1$. Because we have $n+2$ numbers and only $n+1$ intervals, by the pigeonhole principle, some interval must contain at least two of the numbers. So there exist integers r and s such that $0 \leq r < s \leq n+1$ and $|\{r\alpha\} - \{s\alpha\}| \leq 1/(n+1)$. Let $a = s - r$ and $b = [s\alpha] - [r\alpha]$. Because $0 \leq r < s \leq n+1$, we have $1 \leq a \leq n$. Also, $|a\alpha - b| = |(s-r)\alpha - ([s\alpha] - [r\alpha])| = |(s\alpha - [s\alpha]) - (r\alpha - [r\alpha]a)| = |\{s\alpha\} - \{r\alpha\}| < 1/(n+1)$. Therefore, a and b have the desired properties.

1.1.33. The number α must lie in some interval of the form $r/k \leq \alpha < (r+1)/k$. If we divide this interval into equal halves, then α must lie in one of the halves, so either $r/k \leq \alpha < (2r+1)/2k$ or $(2r+1)/2k \leq \alpha < (r+1)/k$. In the first case we have $|\alpha - r/k| < 1/2k$, so we take $u = r$. In the second case we have $|\alpha - (r+1)/k| < 1/2k$, so we take $u = r + 1$.

1.1.34. Suppose that there are only finitely many positive integers $q_1, q_2, \ldots, q_n$ with corresponding integers $p_1, p_2, \ldots, p_n$ such that $|\alpha - p_i/q_i| < 1/q_i^2$. Because α is irrational, $|\alpha - p_i/q_i|$ is positive for every i, and so is $|q_i\alpha - p_i|$ so we may choose an integer N so large that $|q_i\alpha - p_i| > 1/N$ for all i. By Dirichlet's Approximation Theorem, there exist integers r and s with $1 \leq s \leq N$ such that $|s\alpha - r| < 1/N < 1/s$, so that $|\alpha - r/s| < 1/s^2$, and s is not one of the q_i. Therefore, we have another solution to the inequality. So no finite list of solutions can be complete, and we conclude that there must be an infinite number of solutions.

1.1.35. First we have $|\sqrt{2} - 1/1| = 0.414\ldots < 1/1^2$. Second, Exercise 30, part a., gives us $|\sqrt{2} - 7/5| < 1/50 < 1/5^2$. Third, observing that $3/7 = 0.428\ldots$ leads us to try $|\sqrt{2} - 10/7| = 0.014\ldots < 1/7^2 = 0.0204\ldots$. Fourth, observing that $5/12 = 0.4166\ldots$ leads us to try $|\sqrt{2} - 17/12| = 0.00245\ldots < 1/12^2 = 0.00694\ldots$.

1.1.36. First we have $|\sqrt[3]{5} - 1/1| = 0.7099\ldots < 1/1^2$. Second, $|\sqrt[3]{5} - 5/3| = 0.04\ldots < 1/3^2$. Third, because $\sqrt[3]{5} = 1.7099\ldots$, we try $|\sqrt[3]{5} - 17/10| = 0.0099\ldots < 1/10^2$. Likewise, we get a fourth rational number with $|\sqrt[3]{5} - 171/100| = 0.000024\ldots < 1/100^2$. Fifth, consideration of multiples of $1/7$ leads to $|\sqrt[3]{5} - 12/7| = 0.0043\ldots < 1/7^2$.

1.1.37. We may assume that b and q are positive. Note that if $q > b$, we have $|p/q - a/b| = |pb - aq|/qb \geq 1/qb > 1/q^2$. Therefore, solutions to the inequality must have $1 \leq q \leq b$. For a given q, there can be only finitely many p such that the distance between the rational numbers a/b and p/q is less than $1/q^2$

(indeed there is at most one.) Therefore there are only finitely many p/q satisfying the inequality.

1.1.38. a. Because $n2$ is an integer for all n, so is $[n2]$, so the first ten terms of the spectrum sequence are 2, 4, 6, 8, 10, 12, 14, 16, 18, 20.

b. The sequence for $n\sqrt{2}$, rounded, is 1.414, 2.828, 4.242, 5.656, 7.071, 8.485, 9.899, 11.314, 12.728, 14.142. When we apply the floor function to these numbers we get 1, 2, 4, 5, 7, 8, 9, 11, 12, 14 for the spectrum sequence.

c. The sequence for $n(2+\sqrt{2})$, rounded, is 3.414, 6.828, 10.24, 13.66, 17.07, 20.48, 23.90, 27.31, 30.73, 34.14. When we apply the floor function to these numbers we get 3, 6, 10, 13, 17, 20, 23, 27, 30, 34, for the spectrum sequence.

d. The sequence for ne, rounded is 2.718, 5.436, 8.155, 10.87, 13.59, 16.31, 19.03, 21.75, 24.46, 27.18. When we apply the floor function to these numbers we get 2, 5, 8, 10, 13, 16, 19, 21, 24, 27, for the spectrum sequence.

e. The sequence for $n(1+\sqrt{5})/2$, rounded, is 1.618, 3.236, 4.854, 6.472, 8.090, 9.708, 11.33, 12.94, 14.56, 16.18. When we apply the floor function to these numbers we get 1, 3, 4, 6, 8, 9, 11, 12, 14, 16 for the spectrum sequence.

1.1.39. a. Because $n3$ is an integer for all n, so is $[n3]$, so the first ten terms of the spectrum sequence are 3, 6, 9, 12, 15, 18, 21, 24, 27, 30.

b. The sequence for $n\sqrt{3}$, rounded, is 1.732, 3.464, 5.196, 6.928, 8.660, 10.39, 12.12, 13.86, 15.59, 17.32. When we apply the floor function to these numbers we get 1, 3, 5, 6, 8, 10, 12, 13, 15, 17 for the spectrum sequence.

c. The sequence for $n(3+\sqrt{3})/2$, rounded, is 2.366, 4.732, 7.098, 9.464, 11.83, 14.20, 16.56, 18.93, 21.29, 23.66. When we apply the floor function to these numbers we get 2, 4, 7, 9, 11, 14, 16, 18, 21, 23 for the spectrum sequence.

d. The sequence for $n\pi$, rounded is 3.142, 6.283, 9.425, 12.57, 15.71, 18.85, 21.99, 25.13, 28.27, 31.42. When we apply the floor function to these numbers we get 3, 6, 9, 12, 15, 18, 21, 25, 28, 31, for the spectrum sequence.

1.1.40. Because $\alpha \neq \beta$, their decimal expansions must be different. If they differ in digits that are to the left of the decimal point, then $[\alpha] \neq [\beta]$, so certainly the spectrum sequences are different. Otherwise, suppose that they differ in the kth position to the right of the decimal. Then $[10^k\alpha] \neq [10^k\beta]$, and so the spectrum sequences will again differ.

1.1.41. Assume that $1/\alpha + 1/\beta = 1$. Note first that for all integers n and m, $m\alpha \neq n\beta$, for otherwise, we solve the equations $m\alpha = n\beta$ and $1/\alpha + 1/\beta = 1$ and get rational solutions for α and β, a contradiction. Therefore the sequences $m\alpha$ and $n\beta$ are disjoint.

For an integer k, define $N(k)$ to be the number of elements of the sequences $m\alpha$ and $n\beta$ which are less than k. Now $m\alpha < k$ if and only if $m < k/\alpha$, so there are exactly $[k/\alpha]$ members of the sequence $m\alpha$ less than k. Likewise, there are exactly $[k/\beta]$ members of the sequence $n\beta$ less than k. So we have $N(k) = [k/\alpha] + [k/\beta]$. By definition of the greatest integer function, we have $k/\alpha - 1 < [k/\alpha] < k/\alpha$ and $k/\beta - 1 < [k/\beta] < k/\beta$, where the inequalities are strict because the numbers are irrational. If we add these inequalities we get $k/\alpha + k/\beta - 2 < N(k) < k/\alpha + k/\beta$ which simplifies to $k - 2 < N(k) < k$. Because $N(k)$ is an integer, we conclude that $N(k) = k - 1$. This shows that there is exactly one member of the union of the sequences $m\alpha$ and $n\beta$ in each interval of the form $k - 1 \leq x < k$, and therefore, when we apply the floor function to each member, exactly one will take on the value k.

Conversely, suppose that α and β are irrational numbers such that $1/\alpha + 1/\beta \neq 1$. If $1/\alpha + 1/\gamma = 1$ then we know from the first part of the theorem that the spectrum sequences for α and γ partition the positive integers. By Exercise 40, we know that the spectrum sequences for β and γ are different, so the

sequences for α and β can not partition the positive integers.

1.1.42. The first two Ulam numbers are 1 and 2. Because $3 = 1 + 2$, it is the third Ulam number and because $4 = 1 + 3$, it is the fourth Ulam number. Note that 5 is not an Ulam number because $5 = 1 + 4 = 2 + 3$. The fifth Ulam number is 6 because $6 = 4 + 2$ and no other two Ulam numbers have 6 as their sum. We have $7 = 4 + 3 = 6 + 1$, so 7 is not an Ulam number. The sixth Ulam number is $8 = 6 + 2$. Note that $9 = 8 + 1 = 6 + 3$ and $10 = 8 + 2 = 4 + 6$ so neither 9 nor 10 is an Ulam number. The seventh Ulam number is 11 because $11 = 8 + 3$ is the unique way to write 11 as the sum of two distinct Ulam numbers. Next note that $12 = 8 + 4 = 1 + 11$ so that 12 is not an Ulam number. Note that $13 = 11 + 2$ is the unique way to write 13 as the eighth Ulam number. We see that $14 = 13 + 1 = 11 + 3$ and $15 = 2 + 13 = 4 + 11$, so that neither 14 nor 15 are Ulam numbers. We note that $16 = 3 + 13$ is the unique way to write 16 as the sum of two Ulam numbers, so that the ninth Ulam number is 16. Note that $17 = 1 + 16 = 4 + 13$ so that 17 is not an Ulam number. Note that $18 = 2 + 16$ is the unique way to write 18 as the sum of two Ulam numbers so that 18 is the tenth Ulam number. In summary, the first ten Ulam numbers are: 1, 2, 3, 4, 6, 8, 11, 13, 16, 18.

1.1.43. Assume that there are only finitely many Ulam numbers. Let the two largest Ulam numbers be u_{n-1} and u_n. Then the integer $u_n + u_{n-1}$ is an Ulam number larger than u_n. It is the unique sum of two Ulam numbers because $u_i + u_j < u_n + u_{n-1}$ if $j < n$ or $j = n$ and $i < n - 1$.

1.1.44. Suppose that e is rational so that $e = a/b$ where a and b are integers and $b \neq 0$. Let $k \geq b$ be an integer and set $c = k!(e - 1 - 1/1! - 1/2! - 1/3! - \cdots - 1/k!)$. Because every denominator in the expression divides evenly into $k!$, we see that c is an integer. Because $e = 1 + 1/1! + 1/2! + \cdots$, we have $0 < c = k!(1/(k+1)! + 1/(k+2)! + \cdots) = 1/(k+1) + 1/(k+1)(k+2) + \cdots < 1/(k+1) + 1/(k+1)^2 + \cdots$. This last geometric series is equal to $1/k$, so we have that $0 < c < 1/k$, which is impossible because c is an integer. Therefore e must be irrational.

1.1.45. To get a contradiction, suppose that the set of real numbers is countable. Then the subset of real numbers strictly between 0 and 1 is also countable. Then there is a one-to-one correspondence $f : \mathbb{Z}^+ \to (0, 1)$. Each real number $b \in (0, 1)$ has a decimal representation of the form $b = 0.b_1b_2b_3\ldots$, where b_i is the ith digit after the decimal point. For each $k = 1, 2, 3, \ldots$, Let $f(k) = a_k \in (0, 1)$. Then each a_k has a decimal representation of the form $a_k = a_{k1}a_{k2}a_{k3}\ldots$. Form the real number $c = c_1c_2c_3\ldots$ as follows: If $a_{kk} = 5$, then let $c_k = 4$. If $a_{kk} \neq 5$, then let $c_k = 5$. Then $c \neq a_k$ for every k because it differs in the kth decimal place. Therefore $f(k) \neq c$ for all k, and so f is not a one-to-one correspondence. This gives us our contradiction, and so we conclude that the real numbers are uncountable.

1.2. Sums and Products

1.2.1. a. We have $\displaystyle\sum_{j=1}^{5} j^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$.

b. We have $\displaystyle\sum_{j=1}^{5} (-3) = (-3) + (-3) + (-3) + (-3) + (-3) = -15$.

c. We have $\displaystyle\sum_{j=1}^{5} 1/(j+1) = 1/2 + 1/3 + 1/4 + 1/5 + 1/6 = 29/20$.

1.2.2. a. We have $\displaystyle\sum_{j=0}^{4} 3 = 3 + 3 + 3 + 3 + 3 = 15$.

b. We have $\displaystyle\sum_{j=0}^{4} (j - 3) = (-3) + (-2) + (-1) + 0 + 1 = -5$.

c. We have $\displaystyle\sum_{j=0}^{4} (j+1)/(j+2) = 1/2 + 2/3 + 3/4 + 4/5 + 5/6 = 71/20$.

1.2.3. a. We use the formula from Example 1.15 as follows. We evaluate the sum $\sum_{j=0^8 2^j} = 2^9 - 1 = 511$ as in Example 1.17. Then we have $\sum_{j=1^8 2^j} = \sum_{j=0^8 2^j} -2^0 = 510$.

b. We could proceed as in part (a), or we may do the following: $\sum_{j=1}^{8} 5(-3)^j = \sum_{j=0}^{7} 5(-3)^{j+1}$ $= \sum_{j=0}^{7} -15(-3)^j$. We may apply the formula in Example 1.15 to this last sum, with $a = -15, n = 7$ and $r = -3$, to get the sum equal to $\dfrac{-15(-3)^8 - (-15)}{-3-1} = 24600$.

c. We manipulate the sum as in part b., so we can apply the formula from Example 1.15. $\sum_{j=1}^{8} 3(-1/2)^j = \sum_{j=0}^{7} 3(-1/2)^{j+1} = \sum_{j=0}^{7} (-3/2)(-1/2)^j = \dfrac{(-3/2)(-1/2)^8 - (-3/2)}{-1/2-1} = -\dfrac{255}{256}$.

1.2.4. a. We have $\sum_{j=0}^{10} 8 \cdot 3^j = \dfrac{8 \cdot 3^{11} - 8}{3-1} = 708584$, using the formula from Example 1.15 with $a = 8, n = 10$ and $r = 3$.

b. We have $\sum_{j=0}^{10} (-2)^{j+1} = \sum_{j=0}^{10} (-2)(-2)^j = \dfrac{(-2) \cdot (-2)^{11} - (-2)}{(-2)-1} = -1366$, using the formula from Example 1.15 with $a = -2, n = 10$ and $r = -2$.

c. We have $\sum_{j=0}^{10} (1/3)^j = \dfrac{(1/3)^{11} - 1}{(1/3)-1} = \dfrac{88573}{59049}$, using the formula from Example 1.15 with $a = 1, n = 10$ and $r = (1/3)$.

1.2.5. The sum $\sum_{k=1}^{n} [\sqrt{k}]$ counts 1 for every value of k with $\sqrt{k} \geq 1$. There are n such values of k in the range $k = 1, 2, 3, \ldots, n$. It counts another 1 for every value of k with $\sqrt{k} \geq 2$. There are $n-3$ such values in the range. The sum counts another 1 for each value of k with $\sqrt{k} \geq 3$. There are $n-8$ such values in the range. In general, for $m = 1, 2, 3, \ldots, [\sqrt{n}]$ the sum counts a 1 for each value of k with $\sqrt{k} \geq m$, and there are $n - (m^2 - 1)$ values in the range. Therefore $\sum_{k=1}^{n} [\sqrt{k}] = \sum_{m=1}^{[\sqrt{n}]} n - (m^2 - 1) = [\sqrt{n}](n+1) - \sum_{m=1}^{[\sqrt{n}]} m^2 = [\sqrt{n}](n+1) - ([\sqrt{n}]([\sqrt{n}]+1)(2[\sqrt{n}]+1))/6$.

1.2.6. We see that $t_n = \sum_{j=1}^{n} j$, and $t_{n-1} = \sum_{j=1}^{n-1} j = \sum_{j=1}^{n-1} (n-j)$. Now, $t_{n-1} + t_n = \sum_{j=1}^{n-1} (n-j+j) + n = n(n-1) + n = n^2$.

1.2.7. The total number of dots in the n by $n+1$ rectangle, namely $n(n+1)$ is $2t_n$ because the rectangle is made from two triangular arrays. Dividing both sides by 2 gives the desired formula.

1.2.8. From the closed formula for the nth triangular number, we have $3t_n + t_{n-1} = 3(n(n+1)/2) + (n-1)(n-1+1)/2 = 3n(n+1)/2 + n(n-1)/2 = (3n^2+3n+n^2-n)/2 = (4n^2+2n)/2 = 2n(2n+1)/2 = t_{2n}$ as desired.

1.2.9. From the closed formula for the nth triangular number, we have $t_{n+1}^2 - t_n^2 = ((n+1)(n+1+1)/2)^2 - (n(n+1)/2)^2 = (n+1)^2((n+2)^2/4 - n^2/4) = (n+1)^2(n^2+4n+4-n^2)/4 = (n+1)^2(4n+4)/4 = (n+1)^3$, as desired.

1.2.10. It is clear that $p_1 = 1$. Suppose we know p_{k-1}. To compute p_k we consider k nested pentagons as in the figure. Note that $p_k - p_{k-1}$ counts the number of dots on three sides of the outer pentagon. Each side consists of k dots, but two of the dots belong to two sides. Therefore $p_k - p_{k-1} = 3k - 2$, which is the

formula desired. Then $p_n = 3n-2+p_{n-1} = 3n-2+3(n-1)-2+p_{n-2} = 3n-2+3(n-1)-2+3(n-2)-2+p_{n-3} = \cdots = 3n-2+3(n-1)-2+\cdots+3(1)-2 = \sum_{k=1}^{n}(3k-2)$. Evaluating this sums gives us $p_n = \sum_{k=1}^{n}(3k-2) = 3\sum_{k=1}^{n}-2\sum_{k=1}^{n}1 = 3t_n-2n = 3n(n+1)/2-2n = (3n^2+3n-4n)/2 = (3n^2-n)/2$.

1.2.11. From Exercise 10, we have $p_n = (3n^2-n)/2$. On the other hand, $t_{n-1}+n^2 = (n-1)n/2+n^2 = (3n^2-n)/2$, which is the same as above.

1.2.12. a. Consider a regular hexagon which we border successively by hexagons with $3, 4, 5, \ldots$ on each side. Define the *hexagonal number* h_k to be the number of dots contained in the k nested hexagons.

b. First note that $h_1 = 1$. To get a recursive relationship we consider $h_k - h_{k-1}$, which counts the dots added to the $(k-1)$st hexagon to obtain the kth hexagon. To do this, we must add 4 sides of k dots each, but 3 of the dots belong to two sides. Therefore $h_k - h_{k-1} = 4k-3$. A closed formula is then given by adding these differences together: $h_k = \sum_{i=1}^{k}(4i-3) = 4t_k - 3k = 4k(k+1)/2 - 3k = 2k^2-k$.

1.2.13. a. Consider a regular heptagon which we border successively by heptagons with $3, 4, 5, \ldots$ on each side. Define the *heptagonal numbers* $s_1, s_2, s_3, \ldots, s_k, \ldots$ to be the number of dots contained in the k nested heptagons.

b. First note that $s_1 = 1$. To get a recursive relationship we consider $s_k - s_{k-1}$, which counts the dots added to the $(k-1)$st heptagon to obtain the kth heptagon. To do this, we must add 5 sides of k dots each, but 4 of the dots belong to two sides. Therefore $s_k - s_{k-1} = 5k-4$. A closed formula is then given by adding these differences together: $s_k = \sum_{i=1}^{k}(5i-4) = 5t_k - 4k = 5k(k+1)/2-4k = (5k^2-3k)/2$.

1.2.14. From Exercise 12 we have $h_n = 2n^2-n$. Also, $t_{2n-1} = (2n-1)(2n-1+1)/2 = n(2n-1) = 2n^2-n = h_n$.

1.2.15. From Exercise 10 we have $p_n = (3n^2-n)/2$. Also, $t_{3n-1}/3 = (1/3)(3n-1)(3n)/2 = (3n-1)(n)/2 = (3n^2-n)/2 = p_n$.

1.2.16. First consider the difference $T_k - T_{k-1}$. This counts the number of dots on one face of the kth tetrahedron. But this is simply the kth nested triangle used to define the triangular numbers. Therefore, $T_k - T_{k-1} = t_k$. Hence, because $T_1 = t_1 = 1$, it follows that $T_n = \sum_{k=1}^{n} t_k$.

1.2.17. We continue with the formula from Exercise 16. $T_n = \sum_{k=1}^{n} t_k = \sum_{k=1}^{n} k(k+1)/2$. Exploiting the same technique as in Example 1.19, we consider $(k+1)^3 - k^3 = 3k^2+3k+1 = 3(k^2+k)+1$ and solve for k^2+k to get $k^2+k = ((k+1)^3-k^3)/3-(1/3)$. Then $T_n = (1/2)\sum_{k=1}^{n} k(k+1) = (1/6)\sum_{k=1}^{n}((k+1)^3-k^3) - (1/6)\sum_{k=1}^{n}1$. The first sum is telescoping and the second sum is trivial, so we have $T_n = (1/6)((n+1)^3-1^3)-(n/6) = (n^3+3n^2+2n)/6$.

1.2.18. Using the fact $n! = n\cdot(n-1)!$, we find that $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$, $7! = 5040$, $8! = 40320$, $9! = 362880$, and $10! = 3628800$.

1.2.19. Each of these four quantities are products of 100 integers. The largest product is 100^{100}, because it is the product of 100 factors of 100. The second largest is $100!$ which is the product of the integers $1, 2, \ldots, 100$, and each of these terms is less or equal to 100. The third largest is $(50!)^2$ which is the product of $1^2, 2^2, \ldots, 50^2$, and each of these factors j^2 is less than $j(50+j)$, whose product is $100!$. The smallest is 2^{100} which is the product of 100 2's.

1.2.20. a. $\displaystyle\prod_{i=1}^{n} ka_i = k^n \prod_{i=1}^{n} a_i$.

b. $\displaystyle\prod_{i=1}^{n} ia_i = (a_1)(2a_2)\cdots(na_n) = (1\cdot 2\cdots n)(a_1a_2\cdots a_n) = n!\prod_{i=1}^{n} a_i$.

c. $\displaystyle\prod_{i=1}^{n} a_i^k = \left(\prod_{i=1}^{n} a_i\right)^k$.

1.2.21. $\displaystyle\sum_{k=1}^{n}\left(\frac{1}{k(k+1)}\right) = \sum_{k=1}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right)$. Let $a_j = 1/(j+1)$. Notice that this is a telescoping sum, and using the notation in the text preceding Example 1.15, we have $\displaystyle\sum_{k=1}^{n}\left(\frac{1}{k(k+1)}\right) = \sum_{j=1}^{n}(a_{j-1} - a_j) = a_0 - a_n = 1 - 1/(n+1) = n/(n+1)$.

1.2.22. $\displaystyle\sum_{k=2}^{n}\frac{1}{k^2-1} = \frac{1}{2}\sum_{k=2}^{n}\left(\frac{1}{k-1} - \frac{1}{k+1}\right) = \frac{1}{2}\sum_{k=2}^{n}\left(\left(\frac{1}{k-1} - \frac{1}{k}\right) + \left(\frac{1}{k} - \frac{1}{k+1}\right)\right) =$
$\displaystyle\frac{1}{2}\sum_{k=2}^{n}(\frac{1}{k-1} - \frac{1}{k}) + \frac{1}{2}\sum_{k=2}^{n}(\frac{1}{k} - \frac{1}{k+1}) = \frac{1}{2}(1 - \frac{1}{n}) + \frac{1}{2}(\frac{1}{2} - \frac{1}{n+1}) = \frac{3}{4} - \frac{2n+1}{2n(n+1)}$.

1.2.23. We sum both sides of the identity $(k+1)^3 - k^3 = 3k^2 + 3k + 1$ from $k = 1$ to $k = n$. $\sum_{k=1}^{n}((k+1)^3 - k^3) = (n+1)^3 - 1$, because the sum is telescoping. $\sum_{k=1}^{n}(3k^2 + 3k + 1) = 3(\sum_{k=1}^{n} k^2) + 3(\sum_{k=1}^{n} k) + \sum_{k=1}^{n} 1 = 3(\sum_{k=1}^{n} k^2) + 3n(n+1)/2 + n$. As these two expressions are equal, solving for $\sum_{k=1}^{n} k^2$, we find that $\sum_{k=1}^{n} k^2 = (n/6)(2n+1)(n+1)$.

1.2.24. We sum both sides of the identity $(k+1)^4 - k^4 = 4k^3 + 6k^2 + 4k + 1$ from $k = 1$ to $k = n$. Using Exercise 19 we find that $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$.

1.2.25. a. $10! = (7!)(8 \cdot 9 \cdot 10) = (7!)(720) = (7!)(6!)$.

b. $10! = (7!)(6!) = (7!)(5!) \cdot 6 = (7!)(5!)(3!)$.

c. $16! = (14!)(15 \cdot 16) = (14!)(240) = (14!)(5!)(2!)$.

d. $9! = (7!)(8 \cdot 9) = (7!)(6 \cdot 6 \cdot 2) = (7!)(3!)(3!)(2!)$

1.2.26. Because $c = a_1!a_2!\cdots a_n!$ and $b = (a_1!a_2!\cdots a_n!) - 1$, it follows that $c! = c \cdot (c-1)! = c \cdot b! = a_1!a_2!\cdots a_n! \cdot b!$.

1.2.27. Assume that $x \le y$. Then $z! = x! + y! \le y! + y! = 2(y!)$. Because $z > y$ we have $z! \ge (y+1)y!$. This implies that $y + 1 \le 2$. Hence the only solution with x, y, and z positive integers is $x = y = 1$ and $z = 2$.

1.2.28. a. $\displaystyle\prod_{j=2}^{n}(1 - \frac{1}{j}) = (1 - 1/2)(1 - 1/3)\cdots(1 - 1/n) = \frac{1}{2}\frac{2}{3}\frac{3}{4}\cdots\frac{n-1}{n} = \frac{1}{n}$.

b. $\displaystyle\prod_{j=2}^{n}(1 - \frac{1}{j^2}) = \prod_{j=2}^{n}(1 - 1/j)\prod_{j=2}^{n}(1 + 1/j) = \left(\frac{1}{n}\right)\left(\frac{3}{2}\frac{4}{3}\frac{5}{4}\cdots\frac{n+1}{n}\right) = \frac{n+1}{2n}$.

1.3. Mathematical Induction

1.3.1. For $n = 1$ we have $1 < 2^1 = 2$. This is the basis step. Now assume $n < 2^n$. We then have $n + 1 < 2^n + 1 < 2^n + 2^n = 2^{n+1}$. This completes the inductive step and the proof by mathematical induction.

1.3.2. We have $2 = 2$, $2 + 4 = 6$, $2 + 4 + 6 = 12$, $2 + 4 + 6 + 8 = 20$, and $2 + 4 + 6 + 8 + 10 = 30$. We conjecture that $\sum_{j=1}^{n} 2j = n(n+1)$ because this formula holds for small values of n. To prove this by mathematical induction we have $\sum_{j=1}^{1} 2j = 2 = 2 \cdot (1+1)$ so the result is true for 1. Now assume that the formula holds for n. Then $\sum_{j=1}^{n+1} 2j = (\sum_{j=1}^{n} 2j) + 2(n+1) = n(n+1) + 2(n+1) = (n+1)(n+2)$. This completes the proof.

1.3.3. For the basis step we have $\sum_{k=1}^{1} \frac{1}{k^2} = 1 \le 2 - \frac{1}{1} = 1$. For the inductive step, we assume that $\sum_{k=1}^{n} \frac{1}{k^2} \le 2 - \frac{1}{n}$. Then, $\sum_{k=1}^{n+1} \frac{1}{k^2} = \sum_{k=1}^{n} \frac{1}{k^2} + \frac{1}{(n+1)^2} \le 2 - \frac{1}{n} + \frac{1}{(n+1)^2}$ by the induction hypothesis. This is less than $2 - \frac{1}{n+1} + \frac{1}{(n+1)^2} = 2 - \frac{1}{n+1}(1 - \frac{1}{n+1}) \le 2 - \frac{1}{n+1}$, as desired.

1.3.4. For the basis step, we have $\sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{2}$. For the inductive step, we assume that $\sum_{k+1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$. Then, $\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n+1}{n+2}$, as desired.

1.3.5. We see that $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \mathbf{A}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \mathbf{A}^3 = \mathbf{A}^2\mathbf{A} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ and so on. We conjecture that $\mathbf{A}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. To prove this by mathematical induction we first note that the basis step follows because $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Next, we assume that $\mathbf{A}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Then $\mathbf{A}^{n+1} = \mathbf{A}^n\mathbf{A} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$.

1.3.6. The basis step holds because $1 = 1 \cdot (1+1)/2$. For the inductive step assume that $\sum_{j=1}^{n} j = n(n+1)/2$. It follows that

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)(\frac{n}{2} + 1) = \frac{(n+1)(n+2)}{2}.$$

This finishes the inductive proof.

1.3.7. For the basis step, we have $\sum_{j=1}^{1} j^2 = 1 = 1(1+1)(2 \cdot 1 + 1)/6$. For the inductive step, we assume that $\sum_{j=1}^{n} j^2 = n(n+1)(2n+1)/6$. Then, $\sum_{j=1}^{n+1} j^2 = \sum_{j=1}^{n} j^2 + (n+1)^2 = n(n+1)(2n+1)/6 + (n+1)^2 = (n+1)\left(n(2n+1)/6 + n + 1\right) = (n+1)(2n^2 + 7n + 6)/6 = (n+1)(n+2)[2(n+1)+1]/6$, as desired.

1.3.8. For the basis step, we have $\sum_{j=1}^{1} j^3 = 1$, and $(1(1+1)/2)^2 = 1$ also. For the inductive step, we assume that $\sum_{j=1}^{n} j^3 = (n(n+1)/2)^2$. Then, $\sum_{j=1}^{n+1} j^3 = \sum_{j=1}^{n} j^3 + (n+1)^3 = (n(n+1)/2)^2 + n^3 + 3n^2 + 3n + 1 = ((n+1)(n+2)/2)^2$, as desired.

1.3.9. For the basis step, we have $\sum_{j=1}^{1} j(j+1) = 2 = 1(2)(3)/3$. Assume it is true for n. Then $\sum_{j=1}^{n+1} j(j+1) = n(n+1)(n+2)/3 + (n+1)(n+2) = (n+1)(n+2)(n/3+1) = (n+1)(n+2)(n+3)/3$.

1.3.10. For the basis step, we have $\sum_{j=1}^{1}(-1)^{j-1}j^2 = 1 = (-1)^{1-1}1(1+1)/2$. For the inductive step, we assume that $\sum_{j=1}^{n}(-1)^{j-1}j^2 = (-1)^{n-1}n(n+1)/2$. Then, $\sum_{j=1}^{n+1}(-1)^{j-1}j^2 = \sum_{j=1}^{n}(-1)^{j-1}j^2 + (-1)^n(n+1)^2 = (-1)^{n-1}n(n+1)/2 + (-1)^n(n+1)^2 = (-1)^n\frac{1}{2}(n+1)[2(n+1) - n] = (-1)^{(n+1)-1}(n+1)(n+2)/2$, as desired.

1.3.11. We have $\prod_{j=1}^{n} 2^j = 2^{\sum_{j=1}^{n} j} = 2^{n(n+1)/2}$ because $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$.

1.3.12. We use mathematical induction. For $n = 1$ we have $\sum_{j=1}^{1} j \cdot j! = 1 \cdot 1! = 1 = (1+1)! - 1 = 1$. Now assume that $\sum_{j=1}^{n} j \cdot j! = (n+1)! - 1$. Then $\sum_{j=1}^{n+1} j \cdot j! = (n+1)! - 1 + (n+1) \cdot (n+1)! = (n+1)!(1 + n + 1) - 1 = (n+2)! - 1$. This completes the proof.

1.3.13. We will prove this using mathematical induction. We see that $12 = 4 \cdot 3$. Now assume that postage of n cents can be formed, with $n = 4a + 5b$, where a and b are nonnegative integers. To form $n+1$ cents postage, if $a > 0$ we can replace a 4-cent stamp with a 5-cent stamp; that is, $n + 1 = 4(a-1) + 5(b+1)$.

If no 4-cent stamps are present, then all 5-cent stamps were used. It follows that there must be at least three 5-cent stamps and these can be replaced by four 4-cent stamps; that is, $n+1 = 4(a+4) + 5(b-3)$.

1.3.14. We prove this using mathematical induction. We see that $54 = 4 \cdot 10 + 2 \cdot 7$. Now assume that postage of n cents can be formed, with $n = 10a + 7b$, where a and b are positive integers. To form $n+1$ cents postage, if $a > 1$ we can replace 2 ten-cent stamps with 3 seven-cent stamps, that is, $n+1 = 10(a-2) + 7(b+3)$. If $a < 2$, then notice that $b \geq 7$. We can replace 7 seven-cent stamps with 5 ten-cent stamps, that is, $n+1 = 10(a+5) + 7(b-7)$.

1.3.15. We use mathematical induction. The inequality is true for $n = 0$ because $H_{2^0} = H_1 = 1 \geq 1 = 1 + 0/2$. Now assume that the inequality is true for n, that is, $H_{2^n} \geq 1 + n/2$. Then $H_{2^{n+1}} = \sum_{j=1}^{2^n} 1/j + \sum_{j=2^n+1}^{2^{n+1}} 1/j \geq H_{2^n} + \sum_{j=2^n+1}^{2^{n+1}} 1/2^{n+1} \geq 1 + n/2 + 2^n \cdot 1/2^{n+1} = 1 + n/2 + 1/2 = 1 + (n+1)/2$. This completes the inductive proof.

1.3.16. For the basis step, we have $H_{2^0} = H_1 = 1 \leq 1 + 0 = 1$. For the inductive step, we assume that $H_{2^n} \leq 1 + n$. Then,

$$H_{2^{n+1}} = H_{2^n} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} < 1 + n + 2^n \frac{1}{2^n} = 1 + (n+1),$$

as desired.

1.3.17. For the basis step, we have $(2 \cdot 1)! = 2 < 2^{2 \cdot 1}(1!)^2 = 4$. For the inductive step, we assume that $(2n)! < 2^{2n}(n!)^2$. Then $[2(n+1)]! = (2n)!(2n+1)(2n+2) < 2^{2n}(n!)^2(2n+1)(2n+2) < 2^{2n}(n!)^2(2n+2)^2 = 2^{2(n+1)}[(n+1)!]^2$, as desired.

1.3.18. We will use the second principle of mathematical induction to prove this. For the basis step, we have $x - y$ is a factor of $x^1 - y^1$. For the inductive step, we assume that $x - y$ is a factor of $x^n - y^n$ and $x^{n-1} - y^{n-1}$. Then, $x^{n+1} - y^{n+1} = (x^n - y^n)(x + y) + xy(x^{n-1} - y^{n-1})$. Because $x - y$ is a factor of both $(x^n - y^n)(x + y)$ and $xy(x^{n-1} - y^{n-1})$, it is a factor of $x^{n+1} - y^{n+1}$.

1.3.19. Let A be such a set. Define B as $B = \{x - k + 1 \mid x \in A \text{ and } x \geq k\}$. Because $x \geq k, B$ is a set of positive integers. Because $k \in A$ and $k \geq k$, $k - k + 1 = 1$ is in B. Because $n + 1$ is in A whenever n is, $n + 1 - k + 1$ is in B whenever $n - k + 1$ is. Thus B satisfies the hypothesis for mathematical induction, i.e. B is the set of positive integers. Mapping B back to A in the natural manner, we find that A contains the set of integers greater than or equal to k.

1.3.20. The basis step holds because $2^4 = 16 < 4! = 24$. Now assume that $2^n < n!$. Then $2^{n+1} = 2 \cdot 2^n < 2 \cdot n! < (n+1) \cdot n! = (n+1)!$.

1.3.21. For the basis step, we have $4^2 = 16 < 24 = 4!$. For the inductive step, we assume that $n^2 < n!$. Then, $(n+1)^2 = n^2 + 2n + 1 < n! + 2n + 1 < n! + 3n < n! + n! = 2n! < (n+1)n! = (n+1)!$, as desired.

1.3.22. The basis step is clear when $n = 0$. For the inductive step, we assume that $1 + hn \leq (1+h)^n$. Then, $(1+h)^{n+1} = (1+h)^n(1+h) \geq (1+hn)(1+h) = 1 + nh + h + nh^2 \geq 1 + h(n+1)$ because nh^2 is positive. This last inequality proves the induction hypothesis.

1.3.23. We use the second principle of mathematical induction. For the basis step, if the puzzle has only one piece, then it is assembled with exactly 0 moves. For the induction step, assume that all puzzles with $k \leq n$ pieces require $k - 1$ moves to assemble. Suppose it takes m moves to assemble a puzzle with $n + 1$ pieces. Then the m move consists of joining two blocks of size a and b, respectively, with $a + b = n + 1$. But by the induction hypothesis, it requires exactly $a - 1$ and $b - 1$ moves to assemble each of these blocks. Thus, $m = (a-1) + (b-1) + 1 = a + b + 1 = n + 1$. This completes the induction.

1.3.24. The $n = 2$ case does not follow from the $n = 1$ case, because, when $n = 2$, the set of horses labelled 1 to $n - 1$ (which is just the set containing horse 1) does not have any common elements with the set of

horses labelled from 2 to n (which is just the set containing horse 2.)

1.3.25. Suppose that $f(n)$ is defined recursively by specifying the value of $f(1)$ and a rule for finding $f(n+1)$ from $f(n)$. We will prove by mathematical induction that such a function is well-defined. First, note that $f(1)$ is well-defined because this value is explicitly stated. Now assume that $f(n)$ is well-defined. Then $f(n+1)$ also is well-defined because a rule is given for determining this value from $f(n)$.

1.3.26. The function is $f(n) = 2^n$. For the basis step, we have $f(1) = 2 = 2^1$. For the inductive step, we assume that $f(n) = 2^n$. Then, $f(n+1) = 2f(n) = 2 \cdot 2^n = 2^{n+1}$, as desired.

1.3.27. We have $g(1) = 2, g(2) = 2^{g(1)} = 4, g(3) = 2^{g(2)} = 2^4 = 16$, and $g(4) = 2^{g(3)} = 2^{16} = 65536$.

1.3.28. The basis step is given. For the inductive step, we assume that the value of f at the first n positive integers are uniquely determined. Then $f(n+1)$ is uniquely determined from the rule. Therefore, by mathematical induction, $f(n)$ is determined for every positive integer n.

1.3.29. We use the second principle of mathematical induction. The basis step consists of verifying the formula for $n = 1$ and $n = 2$. For $n = 1$ we have $f(1) = 1 = 2^1 + (-1)^1$ and for $n = 2$ we have $f(2) = 5 = 2^2 + (-1)^2$. Now assume that $f(k) = 2^k + (-1)^k$ for all positive integers k with $k < n$ where $n > 2$. By the induction hypothesis it follows that $f(n) = f(n-1) + 2f(n-2) = (2^{n-1} + (-1)^{n-1}) + 2(2^{n-2} + (-1)^{n-2}) = (2^{n-1} + 2^{n-1}) + (-1)^{n-2}(-1+2) = 2^n + (-1)^n$. This finishes the proof.

1.3.30. Because $2^5 = 32 > 25 = 5^2$, the basis step holds. Assume that $2^n > n^2$. Note that for $n > 4$, $2n^2 = n^2 + n^2 > n^2 + 3n = n^2 + 2n + n > n^2 + 2n + 1 = (n+1)^2$. Then we have $(n+1)^2 < 2n^2 < 2 \cdot 2^n = 2^{n+1}$, which completes the induction.

1.3.31. We use the second principle of mathematical induction. We see that $a_0 = 1 \leq 3^0 = 1$, $a_1 = 3 \leq 3^i = 3$, and $a_2 = 9 \leq 3^2 = 9$. These are the basis steps. Now assume that $a_k \leq 3^k$ for all integers k with $0 \leq k < n$. It follows that $a_n = a_{n-1} + a_{n-2} + a_{n-3} \leq 3^{n-1} + 3^{n-2} + 3^{n-3} = 3^{n-3}(1 + 3 + 9) = 13 \cdot 3^{n-3} < 27 \cdot 3^{n-3} = 3^n$. The induction argument is complete.

1.3.32. a. For the basis step notice that for 1 ring only, $1 = 2^1 - 1$ moves are needed. For the inductive step we assume that it takes $2^n - 1$ steps to transfer n rings. To make the inductive step, first transfer n of $n+1$ rings to the third peg. This takes $2^n - 1$ steps. Now transfer the bottom ring to the second peg. This is one step. Then transfer the n rings on the third peg to the second peg. This is $2^n - 1$ more steps. Altogether, this takes $2^n - 1 + 1 + 2^n - 1 = 2^{n+1} - 1$ steps.

b. The world will last, according to this legend, $2^{64} - 1 = 18,446,744,073,709,551,615$ seconds $= 3.07445 \cdot 10^{17}$ minutes $= 5.12409 \cdot 10^{15}$ hours $= 2.13503 \cdot 10^{14}$ days $= 5.84942 \cdot 10^{11}$ years, that is more than 580 billion years.

1.3.33. Let P_n be the statement for n. Then P_2 is true, because we have $((a_1 + a_2)/2)^2 - a_1 a_2 = ((a_1 - a_2)/2)^2 \geq 0$. Assume P_n is true. Then by P_2, for $2n$ positive real numbers $a_1, \ldots, a_{2n}$ we have $a_1 + \cdots + a_{2n} \geq 2(\sqrt{a_1 a_2} + \sqrt{a_3 a_4} + \cdots + \sqrt{a_{2n-1} a_{2n}})$. Apply P_n to this last expression to get $a_1 + \cdots + a_{2n} \geq 2n(a_1 a_2 \cdots a_{2n})^{1/2n}$ which establishes P_n for $n = 2^k$ for all k. Again, assume P_n is true. Let $g = (a_1 a_2 \cdots a_{n-1})^{1/(n-1)}$. Applying P_n, we have $a_1 + a_2 + \cdots + a_{n-1} + g \geq n(a_1 a_2 \cdots a_{n-1} g)^{1/n} = n(g^{n-1} g)^{1/n} = ng$. Therefore, $a_1 + a_2 + \cdots + a_{n-1} \geq (n-1)g$ which establishes P_{n-1}. Thus P_{2^k} is true and P_n implies P_{n-1}. This establishes P_n for all n.

1.3.34. There are four 2×2 chess boards with one square missing. Each can be covered with exactly one L-shaped piece. This is the basis step. Now assume that any $2^n \times 2^n$ chess board can be covered with L-shaped pieces. Consider a $2^{n+1} \times 2^{n+1}$ chess board with one square missing. Split this into four $2^n \times 2^n$ chess boards three of which contain every square and the fourth has one square missing. By the inductive hypothesis we can cover the fourth $2^n \times 2^n$ chess board because it is missing one square. Now use one L-shaped piece to cover the three squares in the other three chess boards that touch at the center of the larger $2^{n+1} \times 2^{n+1}$ chess board. What is left to cover is all the rest of the squares in each of the three

$2^n \times 2^n$ chess boards. The inductive hypothesis says that we can cover all the remaining squares in each of these chess boards. This completes the proof.

1.3.35. Note that because $0 < p < q$ we have $0 < p/q < 1$. The proposition is trivially true if $p = 1$. We proceed by strong induction on p. Let p and q be given and assume the proposition is true for all rational numbers between 0 and 1 with numerators less than p. To apply the algorithm, we find the unit fraction $1/s$ such that $1/(s-1) > p/q > 1/s$. When we subtract, the remaining fraction is $p/q - 1/s = (ps-q)/qs$. On the other hand, if we multiply the first inequality by $q(s-1)$ we have $q > p(s-1)$ which leads to $p > ps - q$, which shows that the numerator of p/q is strictly greater than the numerator of the remainder $(ps-q)/qs$ after one step of the algorithm. By the induction hypothesis, this remainder is expressible as a sum of unit fractions, $1/u_1 + \cdots + 1/u_k$. Therefore $p/q = 1/s + 1/u_1 + \cdots + 1/u_k$ which completes the induction step.

1.3.36. a. Because $1/2 < 2/3$, we subtract to get $2/3 = 1/2 + 1/6$.

b. Because $1/2 < 5/8$, we subtract to get $5/8 = 1/2 + 1/8$.

c. Because $1/2 < 11/17$ we subtract to get $11/17 = 1/2 + 5/34$. The largest unit fraction less than $5/34$ is $1/7$ so we subtract to get $11/17 = 1/2 + 1/7 + 1/238$.

d. The largest unit fraction less than $44/101$ is $1/3$ so we subtract and get $44/101 = 1/3 + 31/303$. The largest unit fraction less than $31/303$ is $1/10$, so we subtract to get $44/101 = 1/3 + 1/10 + 7/3030$. The largest unit fraction less than $7/3030$ is $1/433$, so we subtract to get $44/101 = 1/3 + 1/10 + 1/433 + 1/1311990$. (Note that this is the result of the "greedy algorithm." Other representations are possible, such as $44/101 = 1/3 + 1/10 + 1/440 + 1/26664$.)

1.4. The Fibonacci Numbers

1.4.1. a. We have $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Hence $f_3 = f_2 + f_1 = 1 + 1 = 2$, $f_4 = f_3 + f_2 = 2 + 1 = 3$, $f_5 = 3 + 2 = 5$, $f_6 = 5 + 3 = 8$, $f_7 = 8 + 5 = 13$, $f_8 = 13 + 8 = 21$, $f_9 = 21 + 13 = 34$, and $f_{10} = 34 + 21 = 55$.

b. We continue beyond part (a) finding that $f_{11} = f_{10} + f_9 = 55 + 34 = 89$, $f_{12} = 89 + 55 = 144$, and $f_{13} = 144 + 89 = 233$.

c. We continue beyond part (b) finding that $f_{14} = f_{13} + f_{12} = 233 + 144 = 377$, and $f_{15} = 377 + 233 = 610$.

d. We continue beyond part (c) finding that $f_{16} = 610 + 377 = 987$, $f_{17} = 987 + 610 = 1597$, and $f_{18} = 1597 + 987 = 2584$.

e. We continue beyond part (d) finding that $f_{19} = 2584 + 1597 = 4181$, $f_{20} = 4181 + 2584 = 6765$.

f. We continue beyond part (e) finding that $f_{21} = 6765 + 4181 = 10946$, $f_{22} = 10946 + 6765 = 17711$, $f_{23} = 17711 + 10946 = 28657$, $f_{24} = 28657 + 17711 = 46368$, and $f_{25} = 46368 + 28657 = 75025$.

1.4.2. a. We continue from Exercise 1 part (a), finding that $f_{11} = 55 + 34 = 89$ and $f_{12} = 89 + 55 = 144$.

b. We continue from Exercise 1 part (c), finding that $f_{16} = 610 + 377 = 987$.

c. We computed $f_{24} = 46368$ in Exercise 1 part (f).

d. We continue from Exercise 1 part (f), finding that $f_{26} = 75025 + 46368 = 121393$, $f_{27} = 121393 + 75025 = 196418$, $f_{28} = 196418 + 121393 = 317811$, $f_{29} = 317811 + 196418 = 514229$, and $f_{30} = 514229 + 317811 = 832040$.

e. We continue from part (d), finding $f_{31} = 832040 + 514229 = 1346269$, and $f_{32} = 1346269 + 832040 = 2178309$.

f. We continue from part (e), finding $f_{33} = 2178309 + 1346269 = 3524578$, $f_{34} = 3524578 + 2178309 = 5702887$, $f_{35} = 5702887 + 3524578 = 9227465$ and $f_{36} = 9227465 + 5702887 = 14930352$.

1.4.3. Note that from the Fibonacci identity, whenever n is a positive integer, $f_{n+2} - f_n = f_{n+1}$. Then we have $2f_{n+2} - f_n = f_{n+2} + (f_{n+2} - f_n) = f_{n+2} + f_{n+1} = f_{n+3}$. If we add f_n to both sides of this equation, we have the desired identity.

1.4.4. Assuming n is a positive integer, we have compute $2f_{n+1} + f_n = f_{n+1} + (f_{n+1} + f_n) = f_{n+1} + f_{n+2} = f_{n+3}$. If we subtract f_n from both sides of this equation, we have the desired identity.

1.4.5. For $n = 1$ we have $f_{2\cdot 1} = 1 = 1^2 + 2 \cdot 1 \cdot 0 = f_1^2 + 2f_0 f_1$, and for $n = 2$, we have $f_{2\cdot 2} = 3 = 1^2 + 2 \cdot 1 \cdot 1 = f_2^2 + 2f_1 f_2$. So the basis step holds for strong induction. Assume, then that $f_{2n-4} = f_{n-2}^2 + 2f_{n-3}f_{n-2}$ and $f_{2n-2} = f_{n-1}^2 + 2f_{n-2}f_{n-1}$. Now compute $f_{2n} = f_{2n-1} + f_{2n-2} = 2f_{2n-2} + f_{2n-3} = 3f_{2n-2} - f_{2n-4}$. Now we may substitute in our induction hypotheses to set this last expression equal to $3f_{n-1}^2 + 6f_{n-2}f_{n-1} - f_{n-2}^2 - 2f_{n-3}f_{n-2} = 3f_{n-1}^2 + 6(f_n - f_{n-1})f_{n-1} - (f_n - f_{n-1})^2 - 2(f_{n-1} - f_{n-2})(f_n - f_{n-1}) = -2f_{n-1}^2 + 6f_n f_{n-1} - f_n^2 + 2f_n(f_n - f_{n-1}) - 2f_{n-1}(f_n - f_{n-1}) = f_n^2 + 2f_{n-1}f_n$ which completes the induction step.

1.4.6. For n a positive integer greater than 1, we have $f_{n+2} = f_{n+1} + f_n = (f_n + f_{n-1}) + f_n = (f_n + (f_n - f_{n-2})) + f_n = 3f_n - f_{n-2}$. Adding f_{n-2} to both sides yields the desired identity.

1.4.7. Note that $f_1 = 1 = f_2$, $f_1 + f_3 = 3 = f_4$, and $f_1 + f_3 + f_5 = 8 = f_6$ so we conjecture that $f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}$. We prove this by induction. The basis step is checked above. Assume that our formula is true for n, and consider $f_1 + f_3 + f_5 + \cdots + f_{2n-1} + f_{2n+1} = f_{2n} + f_{2n+1} = f_{2n+2}$, which is the induction step. Therefore the formula is correct.

1.4.8. Note that $f_2 = 1 = f_3 - 1$, $f_2 + f_4 = 4 = f_5 - 1$, and $f_2 + f_4 + f_6 = 12 = f_7 - 1$, so we conjecture that $f_2 + f_4 + f_6 + \cdots + f_{2n} = f_{2n+1} - 1$. We prove this by induction. The basis step is checked above. Assume that our formula is true for n, and consider $f_2 + f_4 + f_6 + \cdots + f_{2n} + f_{2n+2} = f_{2n+1} - 1 + f_{2n+2} = f_{2n+3} - 1$, which is the induction step. Therefore the formula is correct. Another solution is to subtract the formula in Exercise 7 from the formula in Example 1.27, as follows: $\sum_{i=1}^{n} f_{2i} = \sum_{i=1}^{2n} f_i - \sum_{i=1}^{n} f_{2i-1} = (f_{2n+2} - 1) - f_{2n} = f_{2n+1} - 1$.

1.4.9. First suppose $n = 2k$ is even. Then $f_n - f_{n-1} + \cdots + (-1)^{n+1} f_1 = (f_{2k} + f_{2k-1} + \cdots + f_1) - 2(f_{2k-1} + f_{2k-3} + \cdots + f_1) = (f_{2k+2} - 1) - 2(f_{2k})$ by the formulas in Example 1.27 and Exercise 7. This last equals $(f_{2k+2} - f_{2k}) - f_{2k} - 1 = f_{2k+1} - f_{2k} - 1 = f_{2k-1} - 1 = f_{n-1} - 1$. Now suppose $n = 2k + 1$ is odd. Then $f_n - f_{n-1} + \cdots + (-1)^{n+1} = f_{2k+1} - (f_{2k} - f_{2k-1} + \cdots - (-1)^{n+1} f_1) = f_{2k+1} - (f_{2k-1} - 1)$ by the formula just proved for the even case. This last equals $(f_{2k+1} - f_{2k-1}) + 1 = f_{2k} + 1 = f_{n-1} + 1$. We can unite the formulas for the odd and even cases by writing the formula as $f_{n-1} - (-1)^n$.

1.4.10. For $n = 1$ we have $f_3 = 2 = f_2^2 + f_1^2 = 1^2 + 1^2$. And when $n = 2$ we have $f_5 = 5 = 2^2 + 1^2 = f_3^2 + f_2^2$, so the basis steps hold for mathematical induction. Now assume, for the strong form of induction, that the identity holds for all values of n up to $n = k$. Then $f_{2k-3} = f_{k-1}^2 + f_{k-2}^2$ and $f_{2k-1} = f_k^2 + f_{k-1}^2$. Now we calculate $f_{2k+1} = f_{2k} + f_{2k-1} = f_{2k-1} + f_{2k-2} + f_{2k-1} = 2f_{2k-1} + (f_{2k-1} - f_{2k-3}) = 3f_{2k-1} - f_{2k-3}$. Now substituting in the induction hypothesis, makes this last expression equal to $3(f_k^2 + f_{k-1}^2) - f_{k-1}^2 - f_{k-2}^2 = 3f_k^2 + 2f_{k-2}^2 - (f_k - f_{k-1})^2 = 2f_k^2 + f_{k-1}^2 + 2f_k f_{k-1} = 2f_k^2 + (f_{k+1} - f_k)^2 + 2f_k(f_{k+1} - f_k) = f_{k+1}^2 + f_k^2$, which completes the induction step.

1.4.11. We can construct an induction proof similar to the ones in Exercises 5 and 10, or we may proceed as follows. From Exercise 5, we have $f_{2n} = f_n^2 + 2f_{n-1}f_n = f_n(f_n + f_{n-1} + f_{n-1}) = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) = f_{n+1}^2 - f_{n-1}^2$, which is the desired identity.

1.4.12. Let $S_n = f_n + f_{n-1} + f_{n-2} + 2f_{n-3} + \cdots + 2^{n-4} f_2 + 2^{n-3} f_1$. We proceed by induction. If $n = 3$ we have $S_3 = f_3 + f_2 + f_1 = 2 + 1 + 1 = 4 = 2^{3-1}$, and when $n = 4$ we have $S_4 = f_4 + f_3 + f_2 + 2f_1 = 3 + 2 + 1 + 2 \cdot 1 =$

$8 = 2^{4-1}$, so the basis steps hold. Now assume the identity holds for all values less or equal to n and consider $S_{n+1} = f_{n+1} + f_n + f_{n-1} + 2f_{n-2} + 4f_{n-3} + \cdots + 2^{n-4}f_3 + 2^{n-3}f_2 + 2^{n-2}f_1$. We use the Fibonacci identity to expand every term except the last two to get $S_{n+1} = (f_n + f_{n-1}) + (f_{n-1} + f_{n-2}) + (f_{n-2} + f_{n-3}) + 2(f_{n-3} + f_{n-4}) + 4(f_{n-4} + f_{n-5}) + \cdots + 2^{n-4}(f_2 + f_1) + 2^{n-3}f_2 + 2^{n-2}f_1$. Next we regroup, taking the first term from each set of parentheses, plus the second last term together in one group, the last term from each set of parentheses together in another group, and leaving the last term by itself to get $S_{n+1} = (f_n + f_{n-1} + f_{n-2} + 2f_{n-3} + 4f_{n-4} + \cdots + 2^{n-4}f_2 + 2^{n-3}f_2) + (f_{n-1} + f_{n-2} + f_{n-3} + 2f_{n-4} + 4f_{n-5} + \cdots + 2^{n-4}f_1) + 2^{n-2}f_1$. The first group is seen to be equal to S_n when we realize that the last $f_2 = f_1$. The second group is equal to S_{n-1}, so we have $S_{n+1} = S_n + S_{n-1} + 2^{n-1} = 2^{n-2} + 2^{n-2} + 2^{n-1} = 2^n$ by the induction hypothesis. Therefore, by mathematical induction, the proposition is proved.

1.4.13. We proceed by mathematical induction. For the basis step, $\sum_{j=1}^{1} f_j^2 = f_1^2 = f_1 f_2$. To make the inductive step we assume that $\sum_{j=1}^{n} f_j^2 = f_n f_{n+1}$. Then $\sum_{j=1}^{n+1} f_j^2 = \sum_{j=1}^{n} f_j^2 + f_{n+1}^2 = f_n f_{n+1} + f_{n+1}^2 = f_{n+1} f_{n+2}$.

1.4.14. We use mathematical induction. We will use the recursive definition $f_n = f_{n-1} + f_{n-2}$, with $f_0 = 0$ and $f_1 = 1$. For $n = 1$ we have $f_2 f_0 - f_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1$. Hence the basis step holds. Now assume that $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$. Then $f_{n+2} f_n - f_{n+1}^2 = (f_{n+1} + f_n) f_n - f_{n+1}(f_n + f_{n-1}) = f_n^2 - f_{n+1} f_{n-1} = -(-1)^n = (-1)^{n+1}$. This completes the proof.

1.4.15. From Exercise 13, we have $f_{n+1} f_n - f_{n-1} f_{n-2} = (f_1^2 + \cdots + f_n^2) - (f_1^2 + \cdots f_{n-2}^2) = f_n^2 + f_{n-1}^2$. The identity in Exercise 10 shows that this is equal to f_{2n-1} when n is a positive integer, and in particular when n is greater than 2.

1.4.16. Because $f_1 f_2 = 1 \cdot 1 = 1^2 = f_2^2$, the basis step holds. By the induction hypothesis we have $f_1 f_2 + \cdots + f_{2n-1} f_{2n} + f_{2n} f_{2n+1} + f_{2n+1} f_{2(n+1)} = f_{2n}^2 + f_{2n} f_{2n+1} + f_{2n+1} f_{2(n+1)} = f_{2n}(f_{2n} + f_{2n+1}) + f_{2n+1} f_{2(n+1)} = f_{2n} f_{2(n+1)} + f_{2n+1} f_{2(n+1)} = (f_{2n} + f_{2n+1}) f_{2(n+1)} = f_{2(n+1)}^2$.

1.4.17. For fixed m, we proceed by induction on n. The basis step is $f_{m+1} = f_m f_2 + f_{m-1} f_1 = f_m \cdot 1 + f_{m-1} \cdot 1$ which is true. Assume the identity holds for $1, 2, \ldots, k$. Then $f_{m+k} = f_m f_{k+1} + f_{m-1} f_k$ and $f_{m+k-1} = f_m f_k + f_{m-1} f_{k-1}$. Adding these equations gives us $f_{m+k} + f_{m+k-1} = f_m(f_{k+1} + f_k) + f_{m-1}(f_k + f_{k-1})$. Applying the recursive definition yields $f_{m+k+1} = f_m f_{k+2} + f_{m-1} f_{k+1}$, which is precisely the identity.

1.4.18. We're given that $L_1 = 1$ and $L_2 = 3$. Adding each consecutive pair to generate the next Lucas number yields the sequence $1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, \ldots$.

1.4.19. A few trial cases lead us to conjecture that $\sum_{i=1}^{n} L_i = L_{n+2} - 3$. We prove that this formula is correct by induction. The basis step is $L_1 = 1$ and $L_3 - 3 = 4 - 3 = 1$, which checks. Assume that the formula holds for n and compute $\sum_{i=1}^{n+1} L_i = \sum_{i=1}^{n} L_i + L_{n+1} = L_{n+2} - 3 + L_{n+1}$ by the induction hypothesis. This last equals $(L_{n+2} + L_{n+1}) - 3 = L_{n+3} - 3$, which completes the induction step.

1.4.20. A few trial cases lead us to conjecture that $\sum_{i=1}^{n} L_{2i-1} = L_{2n} - 2$. We prove that this formula is correct by induction. The basis step is $L_1 = 1 = L_2 - 2$. Assume that the formula holds for n and compute $\sum_{i=1}^{n+1} L_{2i-1} = \sum_{i=1}^{n} L_{2i-1} + L_{2n+1} = L_{2n} - 2 + L_{2n+1} = L_{2n+2} - 2$, which completes the induction step.

1.4.21. A few trial cases lead us to conjecture that $\sum_{i=1}^{n} L_{2i} = L_{2n+1} - 1$. We prove that this formula is correct by induction. The basis step is $L_2 = 3 = L_3 - 1$. Assume that the formula holds for n and compute $\sum_{i=1}^{n+1} L_{2i} = \sum_{i=1}^{n} L_{2i} + L_{2n+2} = L_{2n+1} - 1 + L_{2n+2} = L_{2n+3} - 1$, which completes the induction step.

1.4.22. We proceed by induction. The basis step is when $n = 2$, and we have $L_2^2 - L_3 L_1 = 3^2 - 4 \cdot 1 = 5 = 5(-1)^2$. Now assume the identity holds for n. Then for $n + 1$ we have $L_{n+1}^2 - L_{n+2} L_n = (L_n + L_{n-1}) L_{n+1} - (L_{n+1} + L_n) L_n = L_n L_{n+1} + L_{n-1} L_{n+1} - L_{n+1} L_n - L_n^2 = -(L_n^2 - L_{n-1} L_{n+1}) = -(5(-1)^n) = 5(-1)^{n+1}$, where we apply the induction hypothesis at the penultimate step.

1.4.23. We proceed by induction. The basis step is $L_1^2 = 1 = L_1L_2 - 2 = 1 \cdot 3 - 2$. Assume the formula holds for n and consider $\sum_{i=1}^{n+1} L_i^2 = \sum_{i=1}^{n} L_i^2 + L_{n+1}^2 = L_nL_{n+1} - 2 + L_{n+1}^2 = L_{n+1}(L_n + L_{n+1}) - 2 = L_{n+1}L_{n+2} - 2$, which completes the induction step.

1.4.24. For $n = 2$, we have $L_2 = 3 = 1 + 2 = f_1 + f_3$. For $n = 3$, we have $L_3 = 4 = 1 + 3 = f_2 + f_4$. This serves as the basis step. Now assume that the statement is true for $k = 2, 3, 4, \ldots, n$. Then $L_{n+1} = L_n + L_{n-1} = (f_{n+1} + f_{n-1}) + (f_n + f_{n-2}) = (f_{n+1} + f_n) + (f_{n-1} + f_{n-2}) = f_{n+2} + f_n$, which completes the induction.

1.4.25. For the basis step, we check that $L_1f_1 = 1 \cdot 1 = 1 = f_2$ and $L_2f_2 = 3 \cdot 1 = 3 = f_4$. Assume the identity is true for all positive integers up to n. Then we have $f_{n+1}L_{n+1} = (f_{n+2} - f_n)(f_{n+2} + f_n)$ from Exercise 24. This equals $f_{n+2}^2 - f_n^2 = (f_{n+1} + f_n)^2 - (f_{n-1} + f_{n-2})^2 = f_{n+1}^2 + 2f_{n+1}f_n + f_n^2 - f_{n-1}^2 - 2f_{n-1}f_{n-2} - f_{n-2}^2 = (f_{n+1}^2 - f_{n-1}^2) + (f_n^2 - f_{n-2}^2) + 2(f_{n+1}f_n - f_{n-1}f_{n-2}) = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) + (f_n - f_{n-2})(f_n + f_{n-2}) + 2(f_{2n-1})$, where the last parenthetical expression is obtained from Exercise 15. This equals $f_nL_n + f_{n-1}L_{n-1} + 2f_{2n-1}$. Applying the induction hypothesis yields $f_{2n} + f_{2n-2} + 2f_{2n-1} = (f_{2n} + f_{2n-1}) + (f_{2n-1} + f_{2n-2}) = f_{2n+1} + f_{2n} = f_{2n+2}$, which completes the induction.

1.4.26. For the basis step, we check that when $n = 1$, $5f_2 = 5 \cdot 1 = 1 + 4 = L_1 + L_3$ and when $n = 2$, $5f_3 = 10 = 3 + 7 = L_2 + L_4$. Now assume the identity holds for integers less than n, and compute $5f_{n+1} = 5f_n + 5f_{n-1} = (L_{n-1} + L_{n+1}) + (L_{n-2} + L_n) = (L_{n-1} + L_{n-2}) + (L_{n+1} + L_n) = L_n + L_{n+1}$, which completes the induction step.

1.4.27. We prove this by induction on n. Fix m a positive integer. If $n = 2$, then for the basis step we need to show that $L_{m+2} = f_{m+1}L_2 + f_mL_1 = 3f_{m+1} + f_m$, for which we will use induction on m. For $m = 1$ we have $L_3 = 4 = 3 \cdot f_2 + f_1$ and for $m = 2$ we have $L_4 = 7 = 3 \cdot f_3 + f_2$, so the basis step for m holds. Now assume that the basis step for n holds for all values of m less than and equal to m. Then $L_{m+3} = L_{m+2} + L_{m+1} = 3f_{m+1} + f_m + 3f_m + f_{m-1} = 3f_{m+2} + f_{m+1}$, which completes the induction step on m and proves the basis step for n. To prove the induction step on n, we compute $L_{m+n+1} = L_{m+n} + L_{m+n-1} = (f_{m+1}L_n + f_mL_{n-1}) + (f_{m+1}L_{n-1} + f_mL_{n-2}) = f_{m+1}(L_n + L_{n-1}) + f_m(L_{n-1} + L_{n-2}) = f_{m+1}L_{n+1} + f_mL_n$, which completes the induction on n and proves the identity.

1.4.28. First check that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. We proceed by induction. The basis steps are $\alpha + \beta = (1 + \sqrt{5})/2 + (1 - \sqrt{5})/2 = 1 = L_1$ and $\alpha^2 + \beta^2 = (1 + \alpha) + (1 + \beta) = 2 + L_1 = 3 = L_2$. Assume the identity is true for all positive integers up to n. Then $L_{n+1} = L_n + L_{n-1} = \alpha^n + \beta^n + \alpha^{n-1} + \beta^{n-1} = \alpha^{n-1}(\alpha + 1) + \beta^{n-1}(\beta + 1) = \alpha^{n-1}(\alpha^2) + \beta^{n-1}(\beta^2) = \alpha^{n+1} + \beta^{n+1}$, which completes the induction.

1.4.29. We find that $50 = 34 + 13 + 3 = f_9 + f_7 + f_4$, $85 = 55 + 21 + 8 + 1 = f_{10} + f_8 + f_6 + f_2$, $110 = 89 + 21 = f_{11} + f_8$ and $200 = 144 + 55 + 1 = f_{12} + f_{10} + f_2$. In each case, we used the "greedy" algorithm, always subtracting the largest possible Fibonacci number from the remainder.

1.4.30. Suppose there is a positive integer that has no Zeckendorf representation. Then by the well-ordering property, there is a smallest such integer, n. Let f_k be the largest Fibonacci number less than or equal to n. Note that if $n = f_k$, then n has a Zeckendorf representation, contrary to our assumption. Then $n - f_k$ is a positive integer less than n, so it has a Zeckendorf representation $n - f_k = \sum_{i=1}^{m} f_{a_i}$. Because n has no Zeckendorf representation, it must be that one of the f_{a_i}'s is equal to or consecutive to f_k. That is, one of f_{k-1}, f_k, or f_{k+1} appears in the summation for $n - f_k$. Then $n = \sum_{i=1}^{m} f_{a_i} + f_k \geq f_{k-1} + f_k = f_{k+1}$. But this contradicts the choice of f_k as the largest Fibonacci number less than n. This establishes existence. To establish uniqueness of the Zeckendorf representation, suppose that there is a positive integer that has two distinct representations. Then the well-ordering property gives us a smallest such integer, n. Suppose $n = \sum_{i=1}^{m} f_{a_i} = \sum_{j=1}^{l} f_{b_l}$ are two distinct representations for n. Then no $f_{a_i} = f_{b_j}$, else we could cancel this term from each side and have a smaller integer with two distinct representations. Without loss of generality, assume that $f_{a_1} > f_{a_2} > \cdots > f_{a_m}$ and $f_{b_1} > f_{b_2} > \cdots > f_{b_l}$ and that $f_{a_1} > f_{b_1}$. If b_1 is even, we compute $n = \sum_{i=1}^{l} f_{b_i} \leq f_{b_1} + f_{b_1-2} + f_{b_1-4} + \cdots + f_2 = f_{b_1+1} - 1$ by Exercise 4. But this last is less than or equal to $f_{a_1} - 1 < n$, a contradiction. If b_1 is odd, we compute, now using Exercise 3, $n = \sum_{i=1}^{l} f_{b_i} \leq f_{b_1} + f_{b_1-2} + f_{b_1-4} + \cdots + f_3 = f_{b_1+1} - f_1 \leq f_{a_1} - 1 < n$, which is also a contradiction. This proves uniqueness.

1.4.31. We proceed by mathematical induction. The basis steps ($n = 2$ and 3) are easily seen to hold. For the inductive step, we assume that $f_n \le \alpha^{n-1}$ and $f_{n-1} \le \alpha_{n-2}$. Now, $f_{n+1} = f_n + f_{n-1} \le \alpha^{n-1} + \alpha^{n-2} = \alpha^n$, because α satisfies $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$.

1.4.32. We proceed by the second principle of mathematical induction on n. For the basis step, we observe that $\binom{0}{0} = f_{0+1} = 1$. For the inductive step, we assume that $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots = f_{n+1}$, and that $\binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots = f_n$. Now, $\binom{n+1}{0} + \binom{n}{1} + \binom{n-1}{2} + \cdots = \binom{n}{0} + [\binom{n-1}{1} + \binom{n-1}{0}] + [\binom{n-2}{2} + \binom{n-2}{1}] + \cdots = \binom{n}{0} + \binom{n-1}{1}\binom{n-2}{2} + \cdots + \binom{n-1}{0} + \binom{n-2}{1} + \cdots = f_{n+1} + f_n = f_{n+2}$.

1.4.33. Using Theorem 1.3 and the notation therein, we have $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$, because they are roots of $x^2 - x - 1 = 0$. Then we have $f_{2n} = (\alpha^{2n} - \beta^{2n})/\sqrt{5} = (1/\sqrt{5})((\alpha+1)^n - (\beta+1)^n) = (1/\sqrt{5})\left(\sum_{j=0}^n \binom{n}{j}\alpha^j - \sum_{j=0}^n \binom{n}{j}\beta^j\right) = (1/\sqrt{5})\sum_{j=0}^n \binom{n}{j}(\alpha^j - \beta^j) = \sum_{j=1}^n \binom{n}{j} f_j$ because the first term is zero in the penultimate sum.

1.4.34. We prove this using mathematical induction. For $n = 1$ we have

$$\mathbf{F}^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}$$

where $f_0 = 0$. Now assume that this formula is true for n. Then

$$\mathbf{F}^{n+1} = \mathbf{F}^n\mathbf{F} = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_{n+1}+f_n & f_{n+1} \\ f_n + f_{n-1} & f_n \end{pmatrix} = \begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix}.$$

1.4.35. On one hand, $\det(\mathbf{F}^n) = \det(\mathbf{F})^n = (-1)^n$. On the other hand,

$$\det\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = f_{n+1}f_{n-1} - f_n^2.$$

1.4.36. We proceed by induction. Clearly the basis step holds. For the inductive step, we assume that $g_n = af_{n-2} + bf_{n-1}$. Then, $g_{n+1} = g_n + g_{n-1} = af_{n-2} + bf_{n-1} + af_{n-3} + bf_{n-2} = af_{n-1} + bf_n$.

1.4.37. We use the relationship $f_n = f_{n+2} - f_{n+1}$ to extend the definition to include negative indices. Thus, $f_0 = 0, f_{-1} = 1, f_{-2} = -1, f_{-3} = 2, f_{-4} = -3, f_{-5} = 5, f_{-6} = -8, f_{-7} = 13, f_{-8} = -21, f_{-9} = 34, f_{-10} = -55$.

1.4.38. We conjecture that $f_{-n} = (-1)^{n+1}f_n$. The basis step is given in Exercise 55. Assume the conjecture is true for n. Then $f_{-(n+1)} = f_{-(n-1)} - f_{-n} = (-1)^n f_{n-1} - (-1)^{n+1}f_n = (-1)^n(f_{n-1} + f_n) = (-1)^{n+2}f_{n+1}$, which completes the induction step.

1.4.39. The square has area 64 square units, while the rectangle has area 65 square units. This corresponds to the identity in Exercise 14, which tells us that $f_7f_5 - f_6^2 = 1$. Notice that the slope of the hypotenuse of the triangular piece is $3/8$, while the slope of the top of the trapezoidal piece is $2/5$. We have $2/5 - 3/8 = 1/40$. Thus, the "diagonal" of the rectangle is really a very skinny parallelogram of area 1, hidden visually by the fact that the two slopes are nearly equal.

1.4.40. First check that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$ as in the solution to Exercise 18. We compute $a_1 = (1/\sqrt{5})(\alpha - \beta) = (1/\sqrt{5})\left((1+\sqrt{5}/2 - (1-\sqrt{5}/2)\right) = (1/\sqrt{5})\left(2\sqrt{5}/2\right) = 1$ and $a_2 = (1/\sqrt{5})(\alpha^2 - \beta^2) = (1/\sqrt{5})(\alpha + 1 - \beta - 1) = (1/\sqrt{5})(\alpha - \beta) = 1$. Finally, we check that $a_{n-1} + a_{n-2} = (1/\sqrt{5})(\alpha^{n-1} - \beta^{n-1}) + (1/\sqrt{5})(\alpha^{n-2} - \beta^{n-2}) = (1/\sqrt{5})(\alpha^{n-1} + \alpha^{n-2} - \beta^{n-1} - \beta^{n-2}) = (1/\sqrt{5})(\alpha^{n-2}(\alpha+1) - \beta^{n-2}(\beta+1)) = (1/\sqrt{5})(\alpha^{n-2}\alpha^2 - \beta^{n-2}\beta^2) = (1/\sqrt{5})(\alpha^n - \beta^n) = a_n$. Because these a_n satisfy the defining relationships of the Fibonacci numbers, we can conclude that $a_n = f_n$ for $n = 1, 2, \ldots$.

1.4.41. We solve the equation $r^2 - r - 1 = 0$ to discover the roots $r_1 = (1+\sqrt{5})/2$ and $r_2 = (1-\sqrt{5})/2$. Then according to the theory in the paragraph above, $f_n = C_1r_1^n + C_2r_2^n$. For $n = 0$ we have $0 = C_1r_1^0 + C_2r_2^0 = C_1 + C_2$. For $n = 1$ we have $1 = C_1r_1 + C_2r_2 = C_1(1+\sqrt{5})/2 + C_2(1-\sqrt{5})/2$. Solving

these two equations simultaneously yields $C_1 = 1/\sqrt{5}$ and $C_2 = -1/\sqrt{5}$. So the explicit formula is $f_n = (1/\sqrt{5})r_1^n - (1/\sqrt{5})r_2^n = (r_1^n - r_2^n)/\sqrt{5}$.

1.4.42. First note that $G(x) - xG(x) - x^2G(x) = \sum_{k=0}^{\infty} f_k x^k - \sum_{k=0}^{\infty} f_k x^{k+1} - \sum_{k=0}^{\infty} f_k x^{k+2} = \sum_{k=0}^{\infty} f_k x^k - \sum_{k=1}^{\infty} f_{k-1}x^k - \sum_{k=2}^{\infty} f_{k-2}x^k = f_0x^0 + f_1x - f_0x + \sum_{k=2}^{\infty}(f_k - f_{k-1} - f_{k-2})x^k = 0 + x - 0 + \sum_{k=2}^{\infty} 0x^k = x$. Solving this for $G(x)$ yields $G(x) = x/(1 - x - x^2)$. Let α and β be defined as in Exercise 30. Then the denominator of $G(x)$ factors as $-(x + \beta)(x + \alpha)$. Expand $G(x)$ into partial fractions to get $G(x) = (1/\sqrt{5})\left(\beta/(x + \beta) - \alpha/(x + \alpha)\right)$. Because $1/\alpha = -\beta$ we can write the above as $G(x) = (1/\sqrt{5})\left(1/(1 - x\alpha) - 1/(1 - x\beta)\right)$. But these last two fractions represent the sums of geometric series, so we have $G(x) = (1/\sqrt{5})\left((1 + \alpha x + (\alpha x)^2 + \cdots) - (1 + \beta x + (\beta x)^2 + \cdots)\right) = (1/\sqrt{5})(0 + (\alpha - \beta)x + (\alpha^2 - \beta^2)x^2 + \cdots)$. Thus the coefficient on the nth power of x is given by $(1/\sqrt{5})(\alpha^n - \beta^n) = f_n$, for all $n \geq 0$.

1.4.43. We seek to solve the recurrence relation $L_n = L_{n-1} + L_{n-1}$ subject to the initial conditions $L_1 = 1$ and $L_2 = 3$. We solve the equation $r^2 - r - 1 = 0$ to discover the roots $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Then according to the theory in the paragraph above Exercise 41, $L_n = C_1\alpha^n + C_2\beta^n$. For $n = 1$ we have $L_1 = 1 = C_1\alpha + C_2\beta$. For $n = 2$ we have $3 = C_1\alpha^2 + C_2\beta^2$. Solving these two equations simultaneously yields $C_1 = 1$ and $C_2 = 1$. So the explicit formula is $L_n = \alpha^n + \beta^n$.

1.4.44. Let $H(x) = \sum_{k=0}^{\infty} L_k x^k$ be the generating function for the Lucas numbers. Note that we define $L_0 = 2$ so that $L_0 + L_1 = 3 = L_2$. Consider $H(x) - xH(x) - x^2H(x) = \sum_{k=0}^{\infty} L_k x^k - \sum_{k=0}^{\infty} L_k x^{k+1} - \sum_{k=0}^{\infty} L_k x^{k+2} = \sum_{k=0}^{\infty} L_k x^k - \sum_{k=1}^{\infty} L_{k-1}x^k - \sum_{k=2}^{\infty} L_{k-2}x^k = L_0x^0 + L_1x - L_0x + \sum_{k=2}^{\infty}(L_k - L_{k-1} - L_{k-2})x^k = 2 + x - 2x + \sum_{k=2}^{\infty} 0x^k = 2 - x$. We solve for $H(x)$ and find its partial fraction expansion $H(x) = (2 - x)/(1 - x - x^2) = (1/(2\sqrt{5}))\left((5 + \sqrt{5})/(x + \alpha) - (5 - \sqrt{5})/(x + \beta)\right)$, where α and β are defined as in Exercise 30. We multiply the top and bottom of the first fraction by β and use the fact that $\alpha\beta = 1$, and similarly treat the second fraction to get the above equal to $1/(1 - \alpha x) + 1/(1 - \beta x)$. But these are the representations for the sums of geometric series, so we have $H(x) = (1 + \alpha x + (\alpha x)^2 + \cdots) + (1 + \beta x + (\beta x)^2 + \cdots) = 2 + (\alpha + \beta)x + (\alpha^2 + \beta^2)x^2 + \cdots$. Therefore, $L_n = \alpha^n + \beta^n$ the coefficient on the nth power of x.

1.4.45. First check that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. We proceed by induction. The basis steps are $(1/\sqrt{5})(\alpha - \beta) = (1/\sqrt{5})(\sqrt{5}) = 1 = f_1$ and $(1/\sqrt{5})(\alpha^2 - \beta^2) = (1/\sqrt{5})((1 + \alpha) - (1 + \beta)) = (1/\sqrt{5})(\alpha - \beta) = 1 = f_2$. Assume the identity is true for all positive integers up to n. Then $f_{n+1} = f_n + f_{n-1} = (1/\sqrt{5})(\alpha^n - \beta^n) + (1/\sqrt{5})(\alpha^{n-1} - \beta^{n-1}) = (1/\sqrt{5})(\alpha^{n-1}(\alpha + 1) - \beta^{n-1}(\beta + 1)) = (1/\sqrt{5})(\alpha^{n-1}(\alpha^2) - \beta^{n-1}(\beta^2)) = (1/\sqrt{5})(\alpha^{n+1} - \beta^{n+1})$, which completes the induction.

1.5. Divisibility

1.5.1. We find that $3 \mid 99$ because $99 = 3 \cdot 33$, $5 \mid 145$ because $145 = 5 \cdot 29$, $7 \mid 343$ because $343 = 7 \cdot 49$, and $888 \mid 0$ because $0 = 888 \cdot 0$.

1.5.2. We see that 1001 is divisible by 7, 11, and 13.

1.5.3. a. Yes, $0 = 7 \cdot 0$.

b. Yes, $707 = 7 \cdot 101$.

c. By the division algorithm, we have $1717 = 245 \cdot 7 + 2$. Because the remainder is nonzero, we know that $7 \nmid 1717$.

d. By the division algorithm, we have $123321 = 17617 \cdot 7 + 2$. Because the remainder is nonzero, we know that $7 \nmid 123321$.

e. By the division algorithm, we have $-285714 = -40817 \cdot 7 + 5$. Because the remainder is nonzero, we know that $7 \nmid -285714$.

f. By the division algorithm, we have $-430597 = -61514 \cdot 7 + 1$. Because the remainder is nonzero, we know that $7 \nmid -430597$.

1.5.4. a. Yes, $0 = 22 \cdot 0$.

b. By the division algorithm, we have $444 = 20 \cdot 22 + 4$. Because the remainder is nonzero, we know that $22 \nmid 444$.

c. Yes, $1716 = 22 \cdot 78$.

d. Yes, $192544 = 22 \cdot 8752$.

e. Yes, $-32516 = 22 \cdot -1478$.

f. By the division algorithm, we have $-195518 = -8888 \cdot 22 + 18$. Because the remainder is nonzero, we know that $22 \nmid -195518$.

1.5.5. a. We have $100 = 5 \cdot 17 + 15$, so the quotient is 5 and the remainder is 15.

b. We have $289 = 17 \cdot 17$, so the quotient is 17 and the remainder is 0.

c. We have $-44 = -3 \cdot 17 + 7$, so the quotient is -3 and the remainder is 7.

d. We have $-100 = -6 \cdot 17 + 2$, so the quotient is -6 and the remainder is 2.

1.5.6. a. The positive integers which divide 12 are 1, 2, 3, 4, 6, and 12.

b. The positive integers which divide 22 are 1, 2, 11 and 22.

c. The positive integers which divide 37 are 1 and 37.

d. The positive integers which divide 41 are 1 and 41.

1.5.7. a. The positive integers which divide 13 are 1 and 13.

b. The positive integers which divide 21 are 1, 3, 7, and 21.

c. The positive integers which divide 36 are 1, 2, 3, 4, 6, 9, 12, 18, and 36

d. The positive integers which divide 44 are 1, 2, 4, 11, 22, and 44.

1.5.8. a. The positive integers which divide 8 are 1, 2, 4, and 8. The positive integers which divide 12 are 1, 2, 3, 4, 6, and 12. The largest integer in both sets is 4, so $(8, 12) = 4$.

b. The positive integers which divide 7 are 1 and 7. The positive integers which divide 9 are 1, 3 and 9. The largest integer in both sets is 1, so $(7, 9) = 1$.

c. The positive integers which divide 15 are 1, 3, 5, and 15. The positive integers which divide 25 are 1, 5 and 25. The largest integer in both sets is 5, so $(15, 25) = 5$.

d. The positive integers which divide 16 are 1, 2, 4, 8, and 16. The positive integers which divide 27 are 1, 3, 9, and 27. The largest integer in both sets is 1, so $(16, 27) = 1$.

1.5.9. a. The positive integers which divide 11 are 1 and 11. The positive integers which divide 22 are 1, 2 and 11. The largest integer in both sets is 11, so $(11, 22) = 11$.

b. The positive integers which divide 36 are 1, 2, 3, 4, 6, 9, 12, 18, and 36. The positive integers which divide 42 are 1, 2, 3, 6, 7, 14, 21, and 42. The largest integer in both sets is 6, so $(36, 42) = 6$.

c. The positive integers which divide 21 are 1, 3, 7, and 21. The positive integers which divide 22 are 1, 2, 11, and 22. The largest integer in both sets is 1, so $(21, 22) = 1$.

d. The positive integers which divide 16 are 1, 2, 4, 8, and 16. The positive integers which divide 64 are 1, 2, 4, 8, 16, 32, and 64. The largest integer in both sets is 16, so $(16, 64) = 16$.

1.5.10. Note that 10 is divisible by 2 and 5. Because 2, 4, 6, and 8 are divisible by 2 and because 5 is divisible by 5, none of these integers is relatively prime to 10. This leaves 1, 3, 7, and 9, which are all relatively prime to 10.

1.5.11. The only positive integers which divide 11 are 1 and 11. Therefore each of 1, 2, 3, ..., 10 is relatively prime to 11.

1.5.12. Because $(a, b) = (b, a)$ we can assume without loss of generality that $a \leq b$. We check to see that this leaves us with $(1, 1)$, $(1, 2)$, $(1, 3)$, ..., $(1, 10)$, $(2, 3)$, $(2, 5)$, $(2, 7)$, $(2, 9)$, $(3, 4)$, $(3, 5)$, $(3, 7)$, $(3, 8)$, $(3, 10)$, $(4, 5)$, $(4, 7)$, $(4, 9)$, $(5, 6)$, $(5, 7)$, $(5, 8)$, $(5, 9)$, $(6, 7)$, $(7, 8)$, $(7, 9)$, $(7, 10)$, $(8, 9)$ and $(9, 10)$.

1.5.13. Without loss of generality, we assume $a < b$. This leaves us with $(10, 11)$, $(10, 13)$, $(10, 17)$, $(10, 19)$, $(11, 12)$, $(11, 13)$, ..., $(11, 20)$, $(12, 13)$, $(12, 17)$, $(12, 19)$, $(13, 14)$, $(13, 15)$, ..., $(13, 20)$, $(14, 15)$, $(14, 17)$, $(14, 19)$, $(15, 16)$, $(15, 17)$, $(15, 19)$, $(16, 17)$, $(16, 19)$, $(17, 18)$, $(17, 19)$, $(17, 20)$, $(18, 19)$ and $(19, 20)$.

1.5.14. Suppose that $a \mid b$ and $b \mid a$. Then there are integers k and l such that $b = ka$ and $a = lb$. This implies that $b = klb$, so that $kl = 1$. Hence either $k = l = 1$ or $k = l = -1$. It follows that either $a = b$ or $a = -b$.

1.5.15. By hypothesis we know $b = ra$ and $d = sc$, for some r and s. Thus $bd = rs(ac)$ and $ac \mid bd$.

1.5.16. We have $6 \mid 2 \cdot 3$, but 6 divides neither 2 nor 3.

1.5.17. If $a \mid b$, then $b = na$ and $bc = n(ca)$, i.e. $ac \mid bc$. Now, suppose $ac \mid bc$. Thus $bc = nac$ and, as $c \neq 0$, $b = na$, i.e., $a \mid b$.

1.5.18. Suppose $a \mid b$. Then $b = na$, and $b - a = na - a = (n - 1)a$. Because a and b are positive $(n - 1)a$ is positive and $a \leq b$.

1.5.19. By definition, $a \mid b$ if and only if $b = na$ for some integer n. Then raising both sides of this equation to the kth power yields $b^k = n^k a^k$ whence $a^k \mid b^k$.

1.5.20. Suppose that x and y are even. Then $x = 2k$ and $y = 2l$ where k and l are integers. Hence $x + y = 2k + 2l = 2(k + l)$ so that $x + y$ is also even. Suppose that x and y are odd. Then $x = 2k + 1$ and $y = 2l + 1$ where k and l are integers. Hence $x + y = (2k + 1) + (2l + 1) = 2k + 2l + 2 = 2(k + l + 1)$, so that $x + y$ is even. Suppose that x is even and y is odd. Then $x = 2k$ and $y = 2l + 1$ where k and l are integers. Hence $x + y = 2k + (2l + 1) = 2(k + l) + 1$. It follows $x + y$ is odd.

1.5.21. Let a and b be odd, and c even. Then $ab = (2x + 1)(2y + 1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1$, so ab is odd. On the other hand, for any integer n, we have $cn = (2z)n = 2(zn)$ which is even.

1.5.22. By the division algorithm, there exist integers s, t such that $a = bs + t, 0 < t < b$ because $b \nmid a$. If t is odd, then we are done. If t is even, then $b - t$ is odd, $|t - b| < b$, and $a = b(s + 1) + (t - b)$.

1.5.23. By the division algorithm, $a = bq + r$, with $0 \leq r < b$. Thus $-a = -bq - r = -(q + 1)b + b - r$. If $0 \leq b - r < b$ then we are done. Otherwise $b - r = b$, or $r = 0$ and $-a = -qb + 0$.

1.5.24. We have $a = qb + r = (tc + s)b + r = tcb + bs + r$.

1.5.25. a. The division algorithm covers the case when b is positive. If b is negative, then we may apply the division algorithm to a and $|b|$ to get a quotient q and remainder r such that $a = q|b| + r$ and $0 \leq r < |b|$. But because b is negative, we have $a = q(-b) + r = (-q)b + r$, as desired.

b. We have $17 = -7(-2) + 3$. Here $r = 3$.

1.5.26. This is called the *l*east remainder algorithm. Suppose that a and b are positive integers. By the division algorithm there are integers s and t with $a = bs + t$ and $0 \leq t < b$. If $0 \leq t \leq \frac{b}{2}$ set $r = t, e = 1$, and $q = s$, so that $a = bq + er$ with $0 \leq r \leq \frac{b}{2}$. If $\frac{b}{2} < t < b$ set $r = b - t, e = -1$, and $q = s + 1$ so that $bq + er = b(s + 1) + (t - b) = bs + t = a$ and $0 < r = t - b < \frac{b}{2}$. Hence there are integers q, e and r such that $a = bq + er$ where $e = \pm 1$ and $0 \leq r \leq \frac{b}{2}$.

1.5.27. By the division algorithm, let $m = qn + r$, with $0 \leq r < n - 1$ and $q = [m/n]$. Then $[(m + 1)/n] = [(qn + r + 1)/n] = [q + (r + 1)/n] = q + [(r + 1)/n]$ as in Example 1.31. If $r = 0, 1, 2, \ldots, n - 2$, then $m \neq kn - 1$ for any integer k and $1/n \leq (r + 1)/n < 1$ and so $[(r + 1)/n] = 0$. In this case, we have $[(m + 1)/n] = q + 0 = [m/n]$. On the other hand, if $r = n - 1$, then $m = qn + n - 1 = n(q + 1) - 1 = nk - 1$, and $[(r + 1)/n] = 1$. In this case, we have $[(m + 1)/n] = q + 1 = [m/n] + 1$.

1.5.28. Suppose $n = 2k$. Then $n - 2[n/2] = 2k - 2[2k/2] = 0$. On the other hand, suppose $n - 2[n/2] = 0$. Then $n/2 = [n/2]$ and $n/2$ is an integer. In other words, n is even.

1.5.29. The positive integers divisible by the positive integer d are those integers of the form kd where k is a positive integer. The number of these that are less than x is the number of positive integers k with $kd \leq x$, or equivalently with $k \leq x/d$. There are $[x/d]$ such integers.

1.5.30. There are $[1000/5] = 200$ positive integers not exceeding 1000 that are divisible by 5, $[1000/25] = 40$ such integers that are divisible by 25, $[1000/125] = 8$ such integers that are divisible by 125, and $[1000/625] = 1$ such integer that is divisible by 625.

1.5.31. There are $[1000/7] - [100/7] = 142 - 14 = 128$ integers between 100 and 1000 that are divisible by 7. There are $[1000/49] - [100/49] = 20 - 2 = 18$ integers between 100 and 1000 that are divisible by 49.

1.5.32. The number of integers not exceeding 1000 that are not divisible by either 3 or 5 equals $1000 - ([1000/3] + [1000/5]) + [1000/15] = 533$.

1.5.33. Using the Principle of Inclusion-Exclusion, the answer is $1000 - ([1000/3] + [1000/5] + [1000/7]) + ([1000/15] + [1000/21] + [1000/35]) - ([1000/105) = 1000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 457$.

1.5.34. For an integer to be divisible by 3, but not by 4, an integer must be divisible by 3, but not by 12. There are $[1000/3] = 333$ positive integers not exceeding 1000 that are divisible by 3. Of these $[1000/12] = 82$ are divisible by 12 (because anything that is divisible by 12 is automatically divisible by 3). Hence there are $333 - 83 = 250$ possible integers not exceeding 1000 that are divisible by 3, but not by 4.

1.5.35. Let w be the weight of a letter in ounces. Note that the function $-[-x]$ rounds x up to the least integer less than or equal to x. (That is, it's the equivalent of the ceiling function.) The cost of mailing a letter weighing w ounces is, then, 44 cents plus 17 cents for each ounce or part thereof more than 1, so we need to round $w - 1$ up to the next integer. So the cost is $c(w) = 44 - [1 - w]17$ cents. Suppose that $44 - [1 - w]17 = 181$ then $-[1 - w]17 = 181 - 44 = 137$ which is not a multiple of 17, so no letter can cost \$1.81. Suppose that $44 - [1 - w]17 = 265$ then $-[1 - w]17 = 265 - 44 = 221 = 13 \cdot 17$. Then $[1 - w] = -13$, so $-13 \leq 1 - w < -12$, or $13 < w \leq 14$. So a letter weighing at least 13 ounces but less than 14 ounces would cost \$2.65.

1.5.36. Note that $a^3 - a = a(a^2 - 1) = (a - 1)a(a + 1)$. By the division algorithm $a = 3k, a = 3k + 1$, or $a = 3k + 2$, where k is an integer. If $a = 3k$, 3 divides a, if $a = 3k + 1$ then $a - 1 = 3k$, so that 3 divides $a - 1$,

and if $a = 3k+2$, then $a+1 = 3k+3 = 3(k+1)$, so that 3 divides $a+1$. Hence 3 divides $(a-1)a(a+1) = a^3 - a$ for every nonnegative integer a. (Note: This can also be proved using mathematical induction.)

1.5.37. Multiplying two integers of this form gives us $(4n+1)(4m+1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1$. Similarly, $(4n+3)(4m+3) = 16mn + 12m + 12n + 9 = 4(4mn + 3m + 3n + 2) + 1$.

1.5.38. Suppose that n is odd. Then $n = 2t+1$ where t is an integer. It follows that $n^2 = (2t+1)^2 = 4t^2 + 4t + 1 = 4t(t+1) + 1$. Now if t is even, then $t = 2u$ where u is an integer. Hence $n^2 = 8u(2u+1) + 1 = 8k + 1$, where $k = u(2u+1)$ is an integer. If t is odd, then $t = 2u+1$ where u is an integer. Hence $n^2 = (8u+4)(2u+2) + 1 = 8(2u+1)(u+1) + 1 = 8k + 1$, where $k = (2u+1)(u+1)$.

1.5.39. Every odd integer may be written in the form $4k+1$ or $4k+3$. Observe that $(4k+1)^4 = 16^2k^4 + 4(4k)^3 + 6(4k)^2 + 4(4k) + 1 = 16(16k^4 + 16k^3 + 6k^2 + k) + 1$. Proceeding further, $(4k+3)^4 = (4k)^4 + 12(4k)^3 + 54(4k)^2 + 108(4k) + 3^4 = 16(16k^4 + 48k^3 + 54k^2 + 27k + 5) + 1$.

1.5.40. The product of the integers $6k+5$ and $6l+5$ is $(6k+5)(6l+5) = 36kl + 30(k+l) + 25 = 6[6kl + 5(k+l) + 4] + 1 = 6N + 1$ where $N = 6kl + 5(k+l) + 4$. Hence this product is of the form $6N+1$.

1.5.41. Of any consecutive three integers, one is a multiple of three. Also, at least one is even. Therefore, the product is a multiple of $2 \cdot 3 = 6$.

1.5.42. The basis step is completed by noting that $1^5 - 1 = 0$ is divisible by 5. For the inductive hypothesis, assume that $n^5 - n$ is divisible by 5. This implies that there is an integer k such that $n^5 - n = 5k$. It follows that $(n+1)^5 - (n+1) = (n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) - (n+1) = (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n) = 5k + 5l = 5(k+l)$. Hence $(n+1)^5 - (n+1)$ is also divisible by 5.

1.5.43. For the basis step note that $0^3 + 1^3 + 2^3 = 9$ is a multiple of 9. Suppose that $n^3 + (n+1)^3 + (n+2)^3 = 9k$ for some integer k. Then $(n+1)^3 + (n+2)^3 + (n+3)^3 = n^3 + (n+1)^3 + (n+2)^3 + (n+3)^3 - n^3 = 9k + n^3 + 9n^2 + 27n + 27 - n^3 = 9k + 9n^2 + 27n + 27 = 9(k + n^2 + 3n + 3)$ which is a multiple of 9.

1.5.44. We prove this by mathematical induction. We will prove that f_{3n-2} is odd, f_{3n-1} is odd, and f_{3n} is even whenever n is a positive integer. For $n = 1$ we see that $f_{3\cdot 1-2} = f_1 = 1$ is odd, $f_{3\cdot 1-1} = f_2 = 1$ is odd, and $f_{3\cdot 1} = f_3 = 2$ is even. Now assume that f_{3n-2} is odd, f_{3n-1} is odd, and f_{3n} is even where n is a positive integer. Then $f_{3(n+1)-2} = f_{3n+1} = f_{3n} + f_{3n-1}$ is odd because f_{3n} is even and f_{3n-1} is odd, $f_{3(n+1)-1} = f_{3n+2} = f_{3n+1} + f_{3n}$ is odd because f_{3n+1} is odd and f_{3n} is even, and $f_{3(n+1)} = f_{3n+3} = f_{3n+2} + f_{3n+1}$ is even because f_{3n+2} and f_{3n+1} are odd. This completes the proof.

1.5.45. We proceed by mathematical induction. The basis step is clear. Assume that only f_{4n}'s are divisible by 3 for $f_i, i \leq 4k$. Then, as $f_{4k+1} = f_{4k} + f_{4k-1}$, $3 \mid f_{4k}$ and $3 \mid f_{4k+1}$ gives us the contradiction $3 \mid f_{4k-1}$. Thus $3 \nmid f_{4k+1}$. Continuing on, if $3 \mid f_{4k}$ and $3 \mid f_{4k+2}$, then $3 \mid f_{4k+1}$, which contradicts the statement just proved. If $3 \mid f_{4k}$ and $3 \mid f_{4k+3}$, then because $f_{4k+3} = 2f_{4k+1} + f_{4k}$, we again have a contradiction. But, as $f_{4k+4} = 3f_{4k+1} + 2f_{4k}$, and $3 \mid f_{4k}$ and $3 \mid 3 \cdot f_{4k+1}$, we see that $3 \mid f_{4k+4}$.

1.5.46. We proceed by induction. The basis step is clear. Suppose f_n is divisible by 4. By Exercise 34, $f_{n+1}, f_{n+2}, f_{n+4}, f_{n+5}$ are all odd. Suppose f_{n+3} is divisible by 4. Now, $f_{n+3} = 2f_{n+1} + f_n$. Because f_n and f_{n+3} are divisible by 4, so must by $2f_{n+1}$. This is a contradiction. On the other hand, $f_{n+6} = 8f_{n+1} + f_n$. Because both terms are multiples of 4, so is f_{n+6}.

1.5.47. First note that for $n > 5$, $5f_{n-4} + 3f_{n-5} = 2f_{n-4} + 3(f_{n-4} + f_{n-5}) = 2f_{n-4} + 3f_{n-3} = 2(f_{n-4} + f_{n-3}) + f_{n-3} = 2f_{n-2} + f_{n-3} = f_{n-2} + f_{n-2} + f_{n-3} = f_{n-2} + f_{n-1} = f_n$, which proves the first identity. Now note that $f_5 = 5$ is divisible by 5. Suppose that f_{5n} is divisible by 5. From the identity above $f_{5n+5} = 5f_{5n+5-4} + 3f_{5n+5-5} = 5f_{5n+1} + 3f_{5n}$, which is divisible by 5 because $5f_{5n+1}$ is a multiple of 5 and, by the induction hypothesis, so is f_{5n}. This completes the induction.

1.5.48. We use mathematical induction on the integer m. For $m = 1$ we have $f_{n+1} = f_{n-1}f_1 + f_nf_2 = f_{n-1} + f_n$ which is true from the definition of the Fibonacci numbers. For $m = 2$ we have $f_{n+2} = f_{n-1}f_2 + f_nf_3 =$

$f_{n-1}+2f_n = f_{n-1}+f_n+f_n = f_{n+1}+f_n$ which is true from the definition of the Fibonacci numbers. This finishes the basis step of the proof. Now assume that $f_{n+m} = f_m f_{n+1} + f_{m-1}f_n$ holds for all integers m with $m < k$. We will show that it must also hold for $m = k$. We have $f_{n+k-2} = f_{k-2}f_{n+1} + f_{k-3}f_n$ and $f_{n+k-1} = f_{k-1}f_{n+1}+f_{k-2}f_n$. Adding these two equations gives $f_{n+k-2}-f_{n+k-1} = f_{n+1}(f_{k-2}+f_{k-1})+f_n(f_{k-3}+f_{k-2})$. Hence $f_{n+k} = f_{n+1}f_k + f_n f_{k-1}$. Hence the identity is also true for $m = k$. We now show that $f_m \mid f_n$ if $m \mid n$. Because $m \mid n$ we have $n = km$. We prove this using mathematical induction on k. For $k = 1$ we have $n = m$ so $f_m \mid f_n$ because $f_m = f_n$. Now assume f_{mk} is divisible by f_m. Note that $f_{m(k+1)} = f_{mk+m} = f_{mk-1}f_m + f_{mk}f_{m+1}$. The first product is divisible by f_m because f_m is a factor in this term and the second product is divisible by f_m by the inductive hypothesis. Hence $f_m \mid f_{m(k+1)}$. This finishes the inductive proof.

1.5.49. Iterating the transformation T starting with 39 we find that $T(39) = 59$; $T(59) = 89$; $T(89) = 134$; $T(134) = 67$; $T(67) = 101$; $T(101) = 152$; $T(152) = 76$; $T(76) = 38$; $T(38) = 19$; $T(19) = 29$; $T(29) = 44$; $T(44) = 22$; $T(22) = 11$; $T(11) = 17$; $T(17) = 26$; $T(26) = 13$; $T(13) = 20$; $T(20) = 10$; $T(10) = 5$; $T(5) = 8$; $T(8) = 4$; $T(4) = 2$; $T(2) = 1$.

1.5.50. If $3n$ is odd, then so is n. So, $T(n) = (3n+1)/2 = 2^{2k}/2 = 2^{2k-1}$. Because $T(n)$ is a power of 2, the exponent will decrease down to one with repeated applications of T.

1.5.51. We prove this using the second principle of mathematical induction. Because $T(2) = 1$, the Collatz conjecture is true for $n = 2$. Now assume that the conjecture holds for all integers less that n. By assumption there is an integer k such that k iterations of the transformation T, starting at n, produces an integer m less than n. By the inductive hypothesis there is an integer l such that iterating T l times starting at m produces the integer 1. Hence iterating T $k + l$ times starting with n leads to 1. This finishes the proof.

1.5.52. Suppose $n = 2k$ for some k. Then $T(n) = k < 2k = n$. Suppose that $n = 4k + 1$ for some k. Then $T(T(n)) = T(6k + 2) = 3k + 1 < 4k + 1 = n$. Now suppose that $n = 8k + 3$, where k is an even number. $T(T(T(T(n)))) = 9k/2 + 1 < 8k + 3 = n$. This leaves 17 numbers to be considered, $7, 11, 15, 23, 27, 31, 39, 43, 47, 55, 59, 63, 71, 75, 79, 87, 91, 95$. These can be methodically tested. The worst of them is 27, which requires over 70 applications of T to reach 1.

1.5.53. We first show that $(2+\sqrt{3})^n + (2-\sqrt{3})^n$ is an even integer. By the binomial theorem it follows that $(2+\sqrt{3})^n + (2-\sqrt{3})^n = \sum_{j=0}^{n} \binom{n}{j} 2^j \sqrt{3}^{n-j} + \sum_{j=0}^{n} \binom{n}{j} 2^j (-1)^{n-j} \sqrt{3}^{n-j} = 2(2^n + \binom{n}{2} 3 \cdot 2^{n-2} + \binom{n}{4} 3^2 \cdot 2^{n-4} + \cdots) = 2l$ where l is an integer. Next, note that $(2-\sqrt{3})^n < 1$. Because $(2+\sqrt{3})^n$ is not an integer, we see that $[(2+\sqrt{3})^n] = (2+\sqrt{3})^n + (2-\sqrt{3})^n - 1$. It follows that $[(2+\sqrt{3})^n]$ is odd.

1.5.54. Suppose $[a/2] + [a/3] + [a/5] = a$. By the division algorithm, there exist integers q and r such that $a = 30q + r$ with $0 \le r \le 29$. Because a is positive, we must have $q \ge 0$. Then $[a/2] + [a/3] + [a/5] = [(30q+r)/2] + [(30q+r)/3] + [(30q+r)/5] = 15q + [r/2] + 10q + [r/3] + 6q + [r/5] = 31q + [r/2] + [r/3] + [r/5] = 30q + r$. Simplifying gives us $q = r - [r/2] - [r/3] - [r/5]$. Note the following fact: If c and b are positive integers, the division algorithm gives us integers s and t with $c = sb + t$ and $0 \le t < b$. Then $[c/b] = [(sb+t)/b] = sb/b = (c-t)/b \ge (c-(b-1))/b$. Using this inequality in our last equation gives us $q \le r - (r-1)/2 - (r-2)/3 - (r-4)/5 = r(-1/30) + 59/30 \le 59/30$ because $r \ge 0$. Thus $q = 0$ or 1, which forces $1 \le a \le 30(1) + 29 = 59$. So we need only check these 59 numbers. We compute $a - ([a/2] + [a/3] + [a/5])$ for $a = 1, 2, 3, \ldots, 59$ and find the 29 solutions: 6, 10, 12, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 31, 32, 33, 34, 35, 37, 38, 39, 41, 43, 44, 47, 49, 53, and 59.

1.5.55. We prove existence of q and r by induction on a. First assume that $a \ge 0$. Assume existence in the division algorithm holds for all nonnegative integers less than a. If $a < b$, then let $q = 0$ and $r = a$, so that $a = qb + r$ and $0 \le r = a < b$. If $a \ge b$, then $a - b$ is nonnegative and by the induction hypothesis, there exist q' and r' such that $a - b = q'b + r'$, with $0 \le r' < b$. Then $a = (q'+1)b + r'$, so we let $q = q' + 1$ and $r = r'$. This establishes the induction step, so existence is proved for $a \ge 0$. Now suppose $a < 0$. Then $-a > 0$ so from our work above, there exist q' and r' such that $-a = q'b + r'$ and $0 \le r' < b$. Then $a = -q'b - r'$. If $r' = 0$, we're done. If not, then $0 \le b - r' < b$ and $a = (-q' - 1)b + b - r'$, so letting $q = -q' - 1$ and $r = b - r'$ satisfies the theorem. Uniqueness is proved just as in the text.

CHAPTER 2

Integer Representations and Operations

2.1. Representations of Integers

2.1.1. We have $1999 = 7 \cdot 285 + 4, 285 = 7 \cdot 40 + 5$, and $40 = 7 \cdot 5 + 5$, and $5 = 7 \cdot 0 + 5$. The sequence of remainders gives the base 7 digits. Hence $(1999)_{10} = (5554)_7$. We have $(6105)_7 = 6 \cdot 7^3 + 1 \cdot 7^2 + 0 \cdot 7 + 5 = (2112)_{10}$.

2.1.2. We have $89156 = 8 \cdot 11144 + 4$, $11144 = 8 \cdot 1393 + 0$, $1393 = 8 \cdot 174 + 1$, $174 = 8 \cdot 21 + 6$, $21 = 8 \cdot 2 + 5$, and $2 = 8 \cdot 0 + 2$. The sequence of remainders gives us $(89156)_{10} = (256104)_8$. We have $(706113)_8 = 7 \cdot 8^5 + 6 \cdot 8^3 + 8^2 + 8 + 3 = (232523)_{10}$.

2.1.3. We have $(10101111)_2 = (175)_{10}$, and $(999)_{10} = (1111100111)_2$.

2.1.4. We have $(101001000)_2 = 2^3 + 2^6 + 2^8 = (328)_{10}$.

2.1.5. We group together blocks of four binary digits starting from the right. We have $(0101)_2 = (5)_{16}$, $(1111)_2 = (F)_{16}, (1000)_2 = (8)_{16}$. Hence $(100011110101)_2 = (8F5)_{16}$. Likewise, $(1110)_2 = (E)_{16}$, $(0100)_2 = (4)_{16}$, and $(0111)_2 = (7)_{16}$. Therefore, $(11101001110)_2 = (74E)_{16}$.

2.1.6. Each hexadecimal digit corresponds to a block of four binary digits. Translating each hexadecimal digit into the corresponding block of four binary digits gives $(ABCDEF)_{16} = (101010111100110111101111)_2$, $(DEFACED)_{16} = (11011110111111010110011101101)_2$, and $(9A0B)_{16} = (1001101000001011)_2$.

2.1.7. This is because we are using the blocks of three digits as one "digit," which has 1000 possible values.

2.1.8. The proof of Theorem 1.10 goes through exactly, with the inequality $0 \leq a_i \leq b - 1$ replaced by $0 \leq a_i <\mid b \mid$ at each step.

2.1.9. We find that $(101001)_{-2} = 1(-2)^5 + 0(-2)^4 + 1 \cdot (-2)^3 + 0(-2)^2 + 0(-2)^1 + 1(-2)^0 = -39$ and $(12012)_{-3} = 1(-3)^4 + 2(-3)^3 + 0(-3)^2 + 1(-3)^1 + 2(-3)^0 = 26$.

2.1.10. $-7 = (-2) \cdot 4 + 1, 4 = (-2) \cdot (-2) + 0, -2 = (-2) \cdot 1 + 0, 1 = (-2) \cdot 0 + 1$, so $(-7)_{10} = (1001)_{-2}$. $-17 = (-2) \cdot 9 + 1, 9 = (-2) \cdot -4 + 1, -4 = (-2) \cdot 2 + 0, 2 = (-2) \cdot -1 + 0, -1 = (-2) \cdot 1 + 1, 1 = (-2) \cdot 0 + 1$, so $(-17)_{10} = (110011)_{-2}$. $61 = (-2) \cdot -30 + 1, -30 = (-2) \cdot 15 + 0, 15 = (-2) \cdot -7 + 1 - 7 = (-2) \cdot 4 + 1, 4 = (-2) \cdot 2 + 0, 2 = (-2) \cdot 1 + 1, 1 = (-2) \cdot 0 + 1$, so $(61)_{10} = (1001101)_{-2}$.

2.1.11. If m is any integer weight less than 2^k, then by Theorem 1.10, m has a base two expansion $m = a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_1 2^1 + a_0 2^0$, where each a_i is 0 or 1. The 2^i weight is used if and only if $a_i = 1$.

2.1.12. To show existence, mimic the proof of Theorem 2.1 using Exercise 18 of Section 1.5. To show uniqueness, assume that a given number has two representations and look at the difference of these representations. Observe that a number is equal to 0 if and only if e_j is 0 for all j. The result follows.

2.1.13. Let w be the weight to be measured. By Exercise 10, w has a unique balanced ternary expansion. Place the object in pan 1. If $e_i = 1$ then place a weight of 3^i into pan 2. If $e_i = -1$ then place a weight of 3^i in pan 1. If $e_i = 0$ then do not use the weight of 3^i. Now the pans will be balanced.

2.1.14. Each base 9 digit corresponds to two base 3 digits and vice versa. The correspondence is $(0)_9 = (00)_3, (1)_9 = (01)_3, (2)_9 = (02)_3, (3)_9 = (10)_3, (4)_9 = (11)_3, (5)_9 = (12)_3, (6)_9 = (20)_3, (7)_9 = (21)_3, (8)_9 = (22)_3$. To convert a base 9 expansion to a base 3 expansion we simply replace each base 9 digit with the corresponding two base 3 digits. To convert a base 3 expansion to a base 9 expansion, we start at the right of the expansion and replace blocks of two base 3 digits to the corresponding base 9 digit, putting an initial 0 in the last block from the left if it consists only of 1 digit.

2.1.15. To convert a number from base r to base r^n, take the number in blocks of size n. To go the other way, convert each digit of a base r^n number to base r, and concatenate the results.

2.1.16. If $n = (a_k a_{k-1} \dots a_1 a_0)_b$, then $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 + a_0$. Now it follows directly that $n = (a_k b^{k-j} + a_{k-1} b^{k-j-1} + \cdots + a_j) b^j + a_{j-1} b^{j-1} + \cdots + a_0$.

2.1.17. Multiplying n by b^m gives $b^m n = b^m(a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0) = (a_k b^{k+m} + a_{k-1} b^{k+m-1} + \cdots + a_1 b^{m+1} + a_0 b^m + 0 \cdot b^{m-1} + \cdots + 0) = (a_k a_{k-1} \dots a_1 a_0 00 \dots 00)_b$, where we have placed m zeroes at the end of the base b expansion of n.

2.1.18. a. $22 = (10110)_2$, and because $22 > 0$, the one's complement representation is 22 is 010110.

b. $31 = (11111)_2$, and because $31 > 0$, the one's complement representation of 31 is 011111.

c. $7 = (00111)_2$, and because $-7 < 0$, the one's complement of -7 is a 1 followed by the complement of the binary representation of 7, to wit, 111000.

d. $19 = (10011)_2$, and because $-19 < 0$, the one's complement of -19 is a 1 followed by the complement of the binary representation of 19, to wit, 101100.

2.1.19. a. The lead digit is a one, so the number is negative. Its absolute value has a binary representation of the complement of 1001, i.e. 0110. Thus 11001 is the one's complement representation of -6.

b. 01101 is the one's complement representation of 13.

c. 10001 is the one's complement representation of -14.

d. 11111 is a one's complement representation of 0. Note that 00000 also represents 0.

2.1.20. Take the complement of each and every digit.

2.1.21. If m is positive, then $a_{n-1} = 0$ and $a_{n-2} a_{n-3} \dots a_0$ is the binary expansion of m. Hence, $m = \sum_{i=0}^{n-2} a_i 2^i$ as desired. If m is negative, then the one's complement expansion for m has its leading bit equal to 1. If we view the bit string $a_{n-2} a_{n-3} \dots a_0$ as a a binary number, then it represents $(2^{n-1} - 1) - (-m)$, because finding the one's complement is equivalent to subtracting the binary number from $111 \cdots 1$. That is $(2^{n-1} - 1) - (-m) = \sum_{i=0}^{n-2} a_i 2^i$. Solving for m gives us the desired identity.

2.1.22. a. $22 = (10110)_2$. Because 22 is positive, we append a leading 0 to this expansion to obtain 010110 as the two's complement representation of 22.

b. $31 = (11111)_2$. Because 31 is positive, we append a leading 0 to this expansion to obtain 011111 as the two's complement representation of 31.

c. Because -7 is negative, we consider the binary expansion of $2^5 - 7 = 25 = (11001)_2$, and then append a leading 1 to obtain 111001 as the two's complement representation of -7.

d. Because -19 is negative, we consider the binary expansion of $2^5 - 19 = 13 = (01101)_2$, and then append a leading 1 to obtain 101101 as the two's complement representation of -19.

2.1.23. a. Because the first digit is a 1, we know that the integer is negative and that $(1001)_2 = 9$ is the binary expansion of $2^4 - |x|$. So $|x| = 16 - 9 = 7$, and thus $x = -7$.

b. Because the first digit is a 0, we know that the integer is positive and hence $x = (1101)_2 = 13$.

c. Because the first digit is a 1, we know that the integer is negative and that $(0001)_2 = 1$ is the binary expansion of $2^4 - |x|$. So $|x| = 16 - 1 = 15$, and thus $x = -15$.

d. Because the first digit is a 1, we know that the integer is negative and that $(1111)_2 = 15$ is the binary expansion of $2^4 - |x|$. So $|x| = 16 - 15 = 1$, and thus $x = -1$.

2.1.24. If m is positive, then $a_{n-1} = 0$ and $\sum_{i=0}^{n-2} a_i 2^i$ is the binary expansion of m. Hence $m = -a_{n-1}2^{n-1} + \sum_{i=0}^{n-2} a_i 2^i$. If m is negative, then $a_{n-1} = 1$ and $\sum_{i=0}^{n-2} a_i 2^i$ is the binary expansion of $2^{n-1} + m$. Hence, $m = -a_{n-1}2^{n-1} + \sum_{i=0}^{n-2} a_i 2^i$.

2.1.25. If each of the digits in the two's complement representation for m is complemented and then 1 is added to the resulting binary number, the result is the two's complement representation for $-m$. To see this note that $m + (-m) + (-1) =$ (binary expansion of m) + (2^{n-1}+binary expansion for $2^{n-1} - m$) + $(-1) = 2^{n-1} + 2^{n-1} - 1 = 2^n - 1 = (111\ldots1)_2$. Therefore the two's complement representation of $-m-1$ is the complement of m.

2.1.26. If m is positive, the representations are identical. If m is negative, then we compare the solutions to Exercises 25 and 20 to see that we need only add 1 to the one's complement representation of m to obtain the two's complement.

2.1.27. Because 4 bits are required for every decimal digit, $4n$ bits are required to store the number in this manner.

2.1.28. We see that 3! is the largest factorial less than 14. We have $14 = 2 \cdot 3! + 2$. Next, we find that $2 = 1 \cdot 2! + 0$. It follows that $14 = 2 \cdot 3! + 1 \cdot 2! + 0 \cdot 1! = (210)_!$. We see that 4! is the largest factorial less than 56. We have $56 = 2 \cdot 4! + 8$. Next, we find that $8 = 1 \cdot 3! + 2$, and $2 = 1 \cdot 2! + 0$. It follows that $56 = 2 \cdot 4! + 1 \cdot 3! + 1 \cdot 2! + 0 \cdot 1! = (2110)_!$. We see that 5! is the largest factorial less than 384. We have $384 = 3 \cdot 5! + 24$. Next we see that $384 = 1 \cdot 4!$. Hence $384 = 3 \cdot 5! + 1 \cdot 4! + 0 \cdot 3! + 0 \cdot 2! + 0 \cdot 1! = (31000)_!$.

2.1.29. We first show that every positive integer has a Cantor expansion. To find a Cantor expansion of the positive integer n, let m be the unique positive integer such that $m! \leq n < (m+1)!$. By the division algorithm there is an integer a_m such that $n = m! \cdot a_m + r_m$ where $0 \leq a_m \leq m$ and $0 \leq r_m < m!$. We iterate, finding that $r_m = (m-1)! \cdot a_{m-1} + r_{m-1}$ where $0 \leq a_{m-1} \leq m-1$ and $0 \leq r_{m-1} < (m-1)!$. We iterate $m-2$ more times, where we have $r_i = (i-1)! \cdot a_{i-1} + r_{i-1}$ where $0 \leq a_{i-1} \leq i-1$ and $0 \leq r_{i-1} < (i-1)!$ for $i = m+1, m, m-1, \ldots, 2$ with $r_{m+1} = n$. At the last stage we have $r_2 = 1! \cdot a_1 + 0$ where $r_2 = 0$ or 1 and $r_2 = a_1$.

Now that we have shown that every integer has a Cantor expansion, we must show that this expansion is unique. So suppose that n has two different Cantor expansions $n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1! = b_m m! + b_{m-1}(m-1)! + \cdots + b_2 2! + b_1 1!$, where a_j and b_j are integers, and $0 \leq a_j \leq j$ and $0 \leq b_j \leq j$ for $j = 1, 2, \ldots, m$. Suppose that k is the largest integer such that $a_k \neq b_k$, and without loss of generality, assume $a_k > b_k$, which implies that $a_k \geq b_k + 1$. Then $a_k k! + a_{k-1}(k-1)! + \cdots + a_1 1! = b_k k! + b_{k-1}(k-1)! + \cdots + b_1 1!$. Using the identity $\sum_{j=1}^{k} j \cdot j! = (k+1)! - 1$, proved in Exercise 16 of Section 1.3, we see that $b_k k! + b_{k-1}(k-1)! + \cdots + b_1 1! \leq b_k k! + (k-1) \cdot (k-1)! + \cdots + 1 \cdot 1! \leq b_k k! + k! - 1 = (b_k + 1)k! - 1 < a_k k!$. This is a contradiction, so the expansion is unique.

2.1.30. If Player One takes 2 matches then they must be from the same stack. Player Two may then win by taking the other two. If Player One takes only one match, then Player Two can take one match from the other stack, which is a winning position as discussed in the description of Nim.

2.1.31. Call a position *good* if the number of ones in each column is even, and *bad* otherwise. Because a player can only affect one row, he or she must affect some column sums. Thus any move from a good position

produces a bad position. To find a move from a bad position to a good one, construct a binary number by putting a 1 in the place of each column with odd sum, and a 0 in the place of each column with even sum. Subtracting this number of matches from the largest pile will produce a good position.

2.1.32. Let (w, x, y, z) represent the number $wxyz$, where w, x, y, z are single digits. Let a, b, c, d be the digits of a fixed point n of T (a number such that $T(n) = n$). We first show that all four digits of n are different. Suppose, to the contrary, that $b = c$. Then $(a, b, b, d) - (d, b, b, a) = (a - 1 - d, 9, 9, 10 + d - a)$. Because n is a fixed point, we can now see that it must have two 9s, and as $b = c$, in fact it must have three 9s. So $a = b = c = 9$. From this, because $d \neq 10 + d - a = d + 1$, we know that $d = 8 - d$, and $d = 4$. But $(9, 9, 9, 4) - (4, 9, 9, 9) = (4, 9, 9, 5)$, so there is not a fixed point with $b = c$. Therefore, $b \neq c$. Suppose, now, that $a > b > c = d$. Then $(a, b, c, c) - (c, c, b, a) = (a - c, b - 1 - c, c + 9 - b, 10 + c - a)$. As, $b - c - 1 < a - c$, $a - c > b - c - 1 < b$, and $c + 9 - b \geq 10 + c - a$, we know that a and b are $a - c$ and $c + 9 - b$, perhaps not respectively. If $a = a - c$, then $c = 0$. But then $b = 9 - b$, which is impossible. If $a = c + 9 - b$, then $b = a - c$ and $a = c + 9 - a - c$, from which it follows that 9 is even. So we conclude that $c \neq d$. Suppose that $a = b > c > d$. Then $(a, a, c, d) - (d, c, a, a) = (a - d, a - c - 1, c - a + 9, 10 + d - a)$. From the inequalities $a \geq a - d \geq a - c > a - c - 1$ and $c - a + 9 \geq d + 1 - a + 9 = 10 + d - a$ we may conclude that c and d are $a - c - 1$ and $10 + d - a$, perhaps not respectively. If $c = a - c - 1$, then we see that a must be odd. But in this case $d = 10 + d - a$ also, which tells us that a must be even. If, on the other hand, $c = 10 + d - a$ and $d = a - c - 1$, then $c = 10 + a - c - 1 - a = 9 - c$, which is impossible. We conclude here that $a \neq b$. Suppose that $a = b > c = d$. Then $(a, a, c, c) - (c, c, a, a) = (a - c, a - c - 1, c - a + 9, 10 + c - a)$. Because $a - c > a - c - 1, a - c = a$ and $c = 0$. Now $a - c - 1 = c$, so $a = 1$. But $(1, 1, 0, 0) - (0, 0, 1, 1) = (1, 0, 8, 9)$, so clearly this does not give a fixed point. So we now know that $a > b > c > d$. Now, $(a, b, c, d) - (d, c, b, a) = (a - d, -1 + b - c, 9 - b + c, 10 - a + d)$. Note that $a - d > -1 + b - c$, and $9 + c - b > 10 + d - a > d$. So, d is either $-1 + b - c$ or $10 + d - a$. If $d = 10 + d - a$, then $a = 10$, which is not a single digit. Thus, $d = -1 + b - c$. Now, we see that c is either $a - d$ or $10 + d - a$. If $c = a - d$, then $d = -1 + b - c = -1 + b - a + d$. From this, we arrive at $a + 1 = b$, a contradiction. Thus $c = 10 + d - 1$. If $a = a - d$, then $d = 0$. Proceeding along with thought, $b = c + 1 = 9 + c - b$ now, which tells us that $b = 8, c = 7$ and $a = 4$. This is a contradiction. Thus $a = 9 + c - b$ and $b = a - d$. We now have four equations in four unknowns. Solving this system, we find that $a = 7, b = 6, c = 4$, and $d = 1$. This gives a fixed point, namely 6174.

2.1.33. a. First show that the result of the operation must yield a multiple of 9. Then, it suffices to check only multiples of 9 with decreasing digits. There are only 79 of these. If we perform the operation on each of these 79 numbers and reorder the digits, we will have one of the following 23 numbers: 7551, 9954, 5553, 9990, 9981, 8820, 9810, 9620, 8532, 8550, 9720, 9972, 7731, 6543, 8730, 8640, 8721, 7443, 9963, 7632, 6552, 6642, or 6174. It will suffice to check only 9810, 7551, 9990, 8550, 9720, 8640, and 7632, because the other numbers will appear in the sequences which these 8 numbers generate.

b. From the solution in part (a), construct a tree from the last seven numbers. The longest branch is six steps. Every number will reach the tree in two steps. The maximum is given by 8500 (for instance) which takes eight steps.

2.1.34. Let $a_0 = (a, b, c, d)$ be a base 5 fixed point of T_5. Then $T_5(a_0) = (a, b, c, d) - (d, c, b, a) = (a - d, b - 1 - c, c + 4 - b, d + 5 - a)$, for all a_0, with $b \neq c$. Note that the center two digits of $T(a_0)$ sum to $(3)_5$, and the outer two to $(10)_5$. Because the order of the digits is irrelevant, we need only examine four cases: $(1034)_5, (1124)_5, (2033)_5$, and $(2124)_5$. By checking these cases one at a time, we find that they all go to $(3032)_5$, which is a fixed point of T_5. Similarly, if $b \neq c$, then $T_5(a_0)$ is one of $(0444)_5, (1443)_5, (2442)_5, (3441)_5$, and $(4440)_5$. By symmetry, we need only check $(0444)_5, (1443)_5$, and $(2442)_5$. All of these do, in fact, go to $(3032)_5$, the Kaprekar's constant for the base 5.

2.1.35. Consider $a_0 = (3043)_6$. Then $T_6((3043)_6) = (3552)_6$, $T_6((3552)_6) = (3133)_6$, $T_6((3133)_6) = (1554)_6$, $T_6((1554)_6) = (4042)_6$, $T_6((4042)_6) = (4132)_6$, and $T_6((4132)_6) = (3043)_6 = a_0$. So T_6 repeats with period 6. Therefore, it never goes to a Kaprekar's constant for the base 6. Hence, there is no Kaprekar's constant for the base 6.

2.1.36. Let $(abc)_{10}$, be the digits of an integer with $a \leq b \leq c$, and a, b, and c not all the same. Then $(abc)_{10} - (cba)_{10} = ((a-c)(9)(10+c-a))_{10}$, so the form of the next integer is $9bc$. Then $(9bc)_{10} - (cb9)_{10} = ((9-c-1)(9)(1+c))_{10}$. After re-ordering, we see that after two iterations we must have one of the numbers $891, 792, 693$, or 594. Then $T(981) = 792$, $T(792) = 693$, $T(693) = 594$, and $T(594) = 495$, up to order of the digits. Therefore 495 is a Kaprekar's constant for three-digit base 10 integers.

2.1.37. Suppose $n = a_i + a_j = a_k + a_l$ with $i \leq j$ and $k \leq l$. First suppose $i \neq j$. Then $n = a_i + a_j = 2^i + 2^j$ is the binary expansion of n. By Theorem 2.1, this expansion is unique. If $k = l$ then $a_k + a_l = 2^{k+1}$ which would be a different binary expansion of n, so $k \neq l$. Then we must have $i = k$ and $j = l$ by Theorem 2.1, so the sum is unique. Next suppose $i = j$. Then $n = 2^{i+1}$ and so $a_k + a_l = 2^k + 2^l = 2^{i+1}$. This forces $k = l = i$, and again the sum is unique. Therefore $\{a_i\}$ is a Sidon sequence.

2.2. Computer Operations with Integers

2.2.1. To add $(101111011)_2$ and $(1100111011)_2$ we first add 1 and 1, obtaining the rightmost bit 0 and the carry 1. Then we add the bits 1 and 1 and the carry 1, obtaining the second bit from the right in the sum 1 and the carry 1. Then we add the bits 0 and 0, and the carry 1, obtaining the third bit from the right in the sum, 1. Then we add the bits 1 and 1, obtaining the fourth bit from the right in the sum, 0, and the carry 1. Then we add the bits 1 and 1 and the carry 1, obtaining the fifth bit from the right in the sum 1, and the carry 1. Then we add the bits 1 and 1 and the carry obtaining the sixth bit from the right in the sum 1, and the carry 1. Then we add the bits 1 and 0 and the carry 1 obtaining the seventh bit from the right in the sum, 0, and the carry, 1. Then we add the bits 0 and 0 and the carry 1, obtaining the eighth bit from the right in the sum 1. Then we add the bits 1 and 1, obtaining the ninth bit from the right, 0, and the carry 1. Then we add the (leading) bit 0 and the bit 1 and the carry 1, obtaining the tenth bit in the sum, 0, and the carry, 1, which is the leading bit from the left. Hence the sum is $(10010110110)_2$.

2.2.2. We have $(10001000111101)_2 + (11111101011111)_2 = (110000110011100)_2$

2.2.3. We have $(1111000011)_2 - (11010111)_2 = (1011101100)_2$

2.2.4. We have $(1101101100)_2 - (101110101)_2 = (111110111)_2$

2.2.5. To multiply $(11101)_2$ and $(110001)_2$ we need to add $2^0(110001)_2 = (110001)_2$, $2^2(110001)_2 = (11000100)_2$, $2^3(110001)_2 = (110001000)_2$, and $2^4(110001)_2 = (1100010000)_2$. The first bit and carry are computed from $1+0+0+0 = 1$. The second bit and carry are computed from $0+0+0+0 = 0$. The third bit and carry are computed from $0+1+0+0 = 1$. The fourth bit and carry are computed from $0+0+1+0 = 1$. The fifth bit and carry are computed from $1+0+0+1 = 10$. The sixth bit and carry are computed from (with the carry 1) $1+1+0+0+0 = 10$. The seventh bit and carry are computed from (with the carry 1) $1+0+1+0+0 = 10$. The eighth bit and carry are computed from (with the carry 1) 1+0+1+1+0=11. The ninth bit and carry are computed from (with the carry 1) 1+0+0+1+1= 11. The tenth bit and eleventh bit are computed from (with the carry 1) 1+0+0+0+1=10. Hence $(11101)_2 \cdot (110001)_2 = (10110001101)_2$.

2.2.6. We have $(1110111)_2 \cdot (10011011)_2 = (100100000001101)_2$

2.2.7. We have $(110011111)_2 = (11111)_2 \cdot (1101)_2 + (1100)_2$

2.2.8. We see that, because of the length of the words $(11101)_2$ and $(110100111)_2$, that our quotient has four digits. We begin with $(110100111)_2 = 2^3(11101)_2 + (10111111)_2$. We continue with $(10111111)_2 = 2^2(11101)_2 + (1001011)_2$ and $(1001011)_2 = 2(11101)_2 + (10001)_2$. Thus, when $(110100111)_2$ is divided by $(11101)_2$, we get a quotient of $(1110)_2$ and a remainder of $(10001)_2$.

2.2.9. We have $(1234321)_5 + (2030104)_5 = (3314430)_5$

2.2.10. We have $(4434201)_5 - (434421)_5 = (3444230)_5$

2.2.11. We have $(1234)_5 \cdot (3002)_5 = (3023)_5 + (4312000)_5 = (4320023)_5$

2.2.12. We have $(14321)_5 = (22)_5 \cdot (334)_5 + (313)_5$

2.2.13. To add $(ABAB)_{16}$ and $(BABA)_{16}$ we first add the rightmost hexadecimal digits B and A obtaining the rightmost digit of the sum, 5, and carry, 1. Then we add the hexadecimal digits in the second position from the right and the carry, namely A, B and 1, obtaining the second digit from the right in the sum, 6, and the carry, 1. Then we add the hexadecimal digits in the third position from the right, namely B, A, and 1, obtaining the digit in the third position from the right, 6, and the carry, 1. Finally, we add the hexadecimal digits in the leftmost position and the carry, namely A, B, and 1, obtaining the second hexadecimal digit from the left in the sum, 6, and the leftmost hexadecimal digit in the sum 1. Hence the sum is $(16665)_{16}$.

2.2.14. We have $(FEED)_{16} - (CAFE)_{16} = (33EF)_{16}$

2.2.15. We have $(FACE)_{16} \cdot (BAD)_{16} = (B705736)_{16}$

2.2.16. We have $(BEADED)_{16} = (11C)_{16} \cdot (ABBA)_{16} + (2B95)_{16}$

2.2.17. We represent the integer $(18235187)_{10}$ using three words: $((018)(235)(187))_{1000}$ and the integer $(22135674)_{10}$ using three words: $((022)(135)(674))_{1000}$, where each base 1000 digit is represented by three base 10 digits in parentheses. To find the sum, difference, and product of these integers from their base 1000 representations we carry out the algorithms for such computations for base 1000. The details are omitted.

2.2.18. The algorithms for addition, subtraction, multiplication, and integer division for numbers written in a negative base are identical to those written in a positive base.

2.2.19. To add numbers using the one's complement representation, first decide whether the answer will be negative or positive. To do this is easy if both numbers have the same lead (sign) bit; otherwise conduct a bit-by-bit comparison of a positive summand's digits and the complement of the negative's. Now, add the other digits (all but the initial (sign) bit) as an ordinary binary number. If the sum is greater than 2^n we have an overflow error. If not, consider the three quantities of the two summands and the sum. If exactly zero or two of these are negative, we're done. Otherwise, we need to add $(1)_2$ to this answer. Also, add an appropriate sign bit to the front of the number.

2.2.20. To subtract b from a, obtain $-b$ as in Exercise 20, Section 2.1. Then add a and $-b$ as in Exercise 19.

2.2.21. Let $a = (a_m a_{m-1} \dots a_2 a_1)_!$ and $b = (b_m b_{m-1} \dots b_2 b_1)_!$. Then $a+b$ is obtained by adding the digits from right to left with the following rule for producing carries. If $a_j + b_j + c_{j-1}$, where c_{j-1} is the carry from adding a_{j-1} and b_{j-1}, is greater than j, then $c_j = 1$, and the resulting jth digit is $a_j + b_j + c_{j-1} - j - 1$. Otherwise, $c_j = 0$. To subtract b from a, assuming $a > b$, we let $d_i = a_i - b_i + c_{i-1}$ and set $c_i = 0$ if $a_i - b_i + c_{i-1}$ is between 0 and j. Otherwise, $d_i = a_i - b_i + c_{i-1} + j + 1$ and set $c_i = -1$. In this manner, $a - b = (d_m d_{m-1} \dots d_2 d_1)_!$.

2.2.22. a. We have $(374)_{12}$ eggs removed from $(B03)_{12}$ eggs (where B is the base 12 digit that represents the decimal integer 11). Because $(B30)_{12} - (374)_{12} = (778)_{12}$ there are 7 gross, 7 dozen, and 8 eggs left.

b. We have $(5)_{12}$ times $(237)_{12}$ eggs in the delivery. Because $(5)_{12} \cdot (237)_{12} = (B5B)_{12}$ there were 11 gross, 5 dozen, and 11 eggs in the delivery.

c. We have three groups of eggs each containing $(BA6)_{12}/(3)_{12}$ eggs. Because $(BA6)_{12}/(3)_{12} = (3B6)_{12}$, each group contains 3 gross, 11 dozen, and 6 eggs.

2.2.23. We have $(a_n \dots a_1 5)_{10}^2 = (10(a_n \dots a_1)_{10} + 5)^2 = 100(a_n \dots a_1)_{10}^2 + 100(a_n \dots a_1)_{10} + 25 = 100(a_n \dots a_1)_{10}((a_n \dots a_1)_{10} + 1) + 25$. The decimal digits of this number consist of the decimal digits of $(a_n \dots a_1)_{10}((a_n \dots a_1)_{10} + 1)$ followed by 25 because this first product is multiplied by 100 which

shifts its decimal expansion two digits.

2.2.24. We have $(a_n \dots a_1 B)_{2B}^2 = (2B(a_n \dots a_1)_{10} + B)^2 = (2B)^2 (a_n \dots a_1)_{10}^2 + 4B^2 (a_n \dots a_1)_{2B} + B^2 = (2B)^2 (a_n \dots a_1)_{2B} ((a_n \dots a_1)_{2B} + 1) + 25$. The base $2B$ digits of this number consist of the base $2B$ digits of $(a_n \dots a_1)_{2B}(a_n \dots a_1)_{2B}+1$ followed by B^2 because this first product is multiplied by $(2B)^2$ which shifts its base $2B$ expansion two digits. To finish the proof, note that $B^2 = (B/20)_{2B} = (2B)(B/2) + 0$ is valid when B is even. Furthermore, when B is odd, $B^2 = ((B-1)/2B)_{2B} = (2B)((B-1)/2) + B$.

2.3. Complexity and Integer Operations

2.3.1. a. We have $2n + 7$ is $O(n)$ because $2n + 7 \leq 9n$ for every positive integer n.

b. Note that $n^2/3$ is not $O(n)$ for if C is a real number it follows $n^2/3 > Cn$ whenever $n > 3C$.

c. We have 10 is $O(n)$ because $10 \leq 10n$ whenever n is a positive integer.

d. We have $n^2 + 1 \leq 2n^2$ whenever n is a positive integer. Hence $\log(n^2 + 1) \leq \log(2n^2) = 2 \log n + \log 2 \leq 3n$ whenever n is a positive integer. It follows that $\log(n^2 + 1)$ is $O(n)$.

e. Note that $\sqrt{n^2 + 1} \leq \sqrt{2n^2} \leq \sqrt{2} \cdot n$ whenever n is a positive integer. Hence $\sqrt{n^2 + 1}$ is $O(n)$.

f. We have $(n^2 + 1)/(n + 1) < (2n^2/n = 2n$ whenever n is a positive integer. Hence $(n^2 + 1)/(n + 1)$ is $O(n)$.

2.3.2. Note that for $n \geq 1$, $2n^4 + 3n^3 + 17 \leq 2n^4 + 3n^4 + 17n^4 = 22n^4$. So we take $K = 22$, in the definition.

2.3.3. First note that $(n^3 + 4n^2 \log n + 101n^2)$ is $O(n^3)$ and that $(14n \log n + 8n)$ is $O(n \log n)$ as in Example 2.12. Now applying Theorem 2.3 yields the result.

2.3.4. Note that $n! = \prod_{j=1}^{n} j \leq \prod_{j=1}^{n} n = n^n$ whenever n is a positive integer. Hence $n! = O(n^n)$.

2.3.5. Use Exercise 4 and follow Example 2.12 noting that $(\log n)^3 \leq n^3$ whenever n is a positive integer.

2.3.6. Note that $n! = \sum_{j=1}^{n} j^m \leq \sum_{j=1}^{n} n^m = n^{m+1}$. Hence $\sum_{j=1}^{n} j^m = O(n^{m+1})$.

2.3.7. Let k be an integer with $1 \leq k \leq n$. Consider the function $f(k) = (n + 1 - k)k$, whose graph is a concave-down parabola with k-intercepts at $k = 0$ and $k = n + 1$. Because $f(1) = f(n) = n$, it is clear that $f(k) \geq n$ for $k = 1, 2, 3, \dots, n$. Now consider the product $(n!)^2 = \prod_{k=1}^{n} k(n + 1 - k) \geq \prod_{k=1}^{n} n$, by the inequality above. This last is equal to n^n. Thus we have $n^n \leq (n!)^2$. Taking logarithms of both sides yields $n \log(n) \leq 2 \log(n!)$, which shows that $n \log(n)$ is $O(\log(n!))$.

2.3.8. There exist by hypothesis k_1 and k_2 such that $f_1 \leq k_1 O(g_1)$ and $f_2 \leq k_2 O(g_2)$. Let $k = \max\{c_1 k_1, c_2 k_2\}$. Then $c_1 f_1 + c_2 f_2 \leq c_1 k_1 O(g_1) + c_2 k_2 O(g_2) \leq k(O(g_1) + O(g_2)) = kO(g_1 + g_2)$.

2.3.9. Suppose that f is $O(g)$ where $f(n)$ and $g(n)$ are positive integers for every integer n. Then there is an integer C such that $f(n) < Cg(n)$ for all $x \in S$. Then $f^k(n) < C^k g^k(n)$ for all $x \in S$. Hence f^k is $O(g^k)$.

2.3.10. Suppose $f(n) = O(\log_2 n)$. Then $f(n) \leq k \log_2 n = k \log_2 r \log_r n = k' \log_r n$. Conversely, if $f(n) \leq k \log_r n = k(\log_2 n)/(\log_2 r) = k' \log_2 n$, and so $f(n) = O(\log_2 n)$.

2.3.11. The number of digits in the base b expansion of n is $1 + k$ where k is the largest integer such that $b^k \leq n < b^{k+1}$ because there is a digit for each of the powers of $b^0, b^1, \dots, b^k$. Note that this inequality is equivalent to $k \leq \log_b n < k + 1$, so that $k = [\log_b n]$. Hence there are $[\log_b n] + 1$ digits in the base b expansion of n.

2.3.12. For addition, three numbers (two operations) must be added for each digit. Thus it takes less than or equal to $2n$ operations to add two numbers. Subtraction follows in a similar manner.

2.3.13. To multiply an n-digit integer by an m-digit integer in the conventional manner, one must multiply every digit of the first number by every digit of the second number. There are nm such pairs.

2.3.14. a. There are $n-1$ addition signs in $1+2+\cdots n$, so there are $n-1$ additions total. Each addition takes at most $2[\log_2 n]+2$ bit operations (see solution to Exercise 12 and Exercise 11). So, the total number of bit operations is at most $2(n-1)([\log_2 n]+1)$.

b. Here we have one multiplication, which will require at most $([\log_2 n+1]+1)^2$ operations. Shifting is one bit operation, so the total number of bit operations is at most $([\log_2 n+1]+1)^2-1$.

2.3.15. a. We use the result of Theorem 2.6. Let $m=[\log_2 n+1]$. If we first multiply consecutive pairs of integers in the the product, we have $O(n/2)$ multiplications of integers with at most m bits. By Theorem 2.6, there is an algorithm for doing this using $O(m\log_2 m\log_2\log_2 m)$ operations. Now we have $[n/2]$ integers of at most $2m$ bits. If we multiply pairs of these integers together, then by Theorem 2.6 again, this results in $O((n/4)(2m)\log_2 m\log_2\log_2 m)$, where we use the fact that $\log_2 km\log_2\log_2 km = O(\log_2 m\log_2\log_2 m)$ for any constant k. Continuing in this manner we find that computing $n!$ takes $O(\sum_{j=1}^{m} n/(2^j)2^{j-1}\log_2 m\log_2\log_2 m) = O((n/2)m^2\log_2 m\log_2\log_2 m) = O(n\log_2^2 n\log_2\log_2 n\log_2\log_2\log_2 n)$ operations.

b. We need to find three factorials, which will have the same big-O value as in part (a). We will also need to perform one subtraction (which will not affect the big-O value), one multiplication and one division. The factorials have at most $n\log n$ bits, so by Theorem 2.5, the multiplication will take at most $O((n\log n)^{1+\epsilon})$ bit operations. By Theorem 2.7, the division will take $O((n\log n)^{1+\epsilon})$, so in total the number of bit operations is $O((n\log n)^{1+\epsilon})$.

2.3.16. Let m be an integer. Then m has $n=[\log_2(m)+1]$ bits, from Exercise 11. Using the method of Example 2.1, we need to perform the division algorithm n times. Each division takes $O(n^2)=O([\log_2(m)+1]^2)=O(\log^2 m)$. Therefore, the binary expansion can be found in $O(\log^3 m)$ bit operations.

2.3.17. $(1001)_2\cdot(1011)_2=(2^4+2^2)(10)_2(10)_2+2^2(10-01)_2(11-10))_2+(2^2+1)(01)_2(11)_2=(10100)_2(100)_2+(100)_2(01)_2(01)_2+(101)_2(01)_2(11)_2=(1010000)_2+(100)_2+(1111)_2=(1100011)_2$

2.3.18. $(10010011)_2\cdot(11001001)_2 = (2^8+2^4)(1001)_2(1100)_2+2^4(1001-0011)_2(1001-1100))_2+(2^4+1)(0011)_2(1001)_2 = (100010000)_2(1101100)_2-(10000)_2(0110)_2(0011)_2+(10001)_2(11011)_2 = (110110000000000)_2+(11011000000)_2-(100100000)_2+(111001011)_2=(111001101101011)_2$, where we have used identity (1.9) with $n=2$ to do the smaller multiplications.

2.3.19. a. $ab=(10^{2n}+10^n)A_1B_1+10^n(A_1-A_0)(B_0-B_1)+(10^n+1)A_0B_0$ where A_i and B_i are defined as in identity (1.9).

b. $73\cdot 87=(10^2+10)7\cdot 8+10(7-3)(7-8)+(11)3\cdot 7=5600+560-40+210+21=6351$.

c. $4216\cdot 2733=(10100)42\cdot 27+(100)(42-16)(33-27)+(101)16\cdot 33$. Then, $42\cdot 27=(10^2+10)4\cdot 2+10(4-2)(7-2)+(11)2\cdot 7=1134$, and, $26\cdot 06=(10^2+10)2\cdot 0+10(2-6)(6-0)+(11)6\cdot 6=156$, and $16\cdot 33=(10^2+10)1\cdot 3+10(1-6)(3-3)+(11)6\cdot 3=528$. Then $4216\cdot 2733=(10100)1134+(100)156+(101)528=11522328$.

2.3.20. Note that an element of the kth column of A will be multiplied with each element of the kth row of B. Thus, each of the n^2 entries of A will be multiplied n entries of B. In other words, n^3 multiplications will be performed.

2.3.21. That the given equation is an identity may be seen by direct calculation. The seven multiplications necessary to use this identity are: $a_{11}b_{11}$, $a_{12}b_{21}$, $(a_{11}-a_{21}-a_{22})(b_{11}-b_{12}-b_{22})$, $(a_{21}+a_{22})(b_{12}-b_{11})$,

$(a_{11} + a_{12} - a_{21} - a_{22})b_{22}$, $(a_{11} - a_{21})(b_{22} - b_{12})$, $a_{22}(b_{11} - b_{21} - b_{12} + b_{22})$.

2.3.22. We proceed by mathematical induction. Exercise 21 serves to complete the basis step. For the inductive hypothesis, assume that it requires 7^k multiplications to multiply two $2^k \times 2^k$ matrices, and fewer than 7^{k+1} additions. Note that the identity from Exercise 21 holds when the entries of the 2×2 matrices are themselves square matrices, all the same size. Thus we may view a $2^{k+1} \times 2^{k+1}$ matrix as a 2×2 matrix whose entries are $2^k \times 2^k$ matrices. Thus we will need to multiply $2^k \times 2^k$ matrices seven times, requiring $7 \cdot 7^k = 7^{k+1}$ multiplications. Similarly, we will need to add $2^k \times 2^k$ matrices 18 times, requiring exactly $18 \cdot 2^k$ additions. But $18 \cdot 2^k < 7 \cdot 3 \cdot 2 \cdot 2^{k-1} < 7^2 \cdot 2^{k-1} < 7^{k+1}$, as desired.

2.3.23. Let $k = [\log_2 n] + 1$. Then the number of multiplications for $2^k \times 2^k$ matrices is $O(7^k)$. But, $7^k = 2^{(\log_2 7)([\log_2 n]+1)} = O(2^{\log_2 n \log_2 7} 2^{\log_2 7}) = O(n^{\log_2 7})$. The other bit operations are absorbed into this term.

CHAPTER 3

Primes and Greatest Common Divisors

3.1. Prime Numbers

3.1.1. a. We see that 101 is prime because it is not divisible by any positive integers other than 1 or 101. To verify this it is sufficient to check that 101 is not divisible by any prime not exceeding $\sqrt{101}$. The only such primes are 2, 3, 5, and 7 and none of these divide 101.

b. We see that 103 is prime because it is not divisible by any positive integers other than 1 or 103. To verify this it is sufficient to check that 103 is not divisible by any prime not exceeding $\sqrt{103}$. The only such primes are 2, 3, 5, and 7 and none of these divide 103.

c. We see that 107 is prime because it is not divisible by any positive integers other than 1 or 107. To verify this it is sufficient to check that 107 is not divisible by any prime not exceeding $\sqrt{107}$. The only such primes are 2, 3, 5, and 7 and none of these divide 107.

d. We see that 111 is not prime because it is divisible by 3.

e. We see that 113 is prime because it is not divisible by any positive integers other than 1 or 113. To verify this it is sufficient to check that 113 is not divisible by any prime not exceeding $\sqrt{113}$. The only such primes are 2, 3, 5, and 7 and none of these divide 113.

f. We see that 121 is not prime because it is divisible by 11.

3.1.2. a. We have $201 = 3 \cdot 67$, so 201 is not prime.

b. We have $203 = 7 \cdot 29$, so 203 is not prime.

c. We have $207 = 9 \cdot 23$, so 207 is not prime.

d. 211 is prime.

e. We have $213 = 3 \cdot 71$, so 213 is not prime.

f. We have $221 = 13 \cdot 17$, so 221 is not prime.

3.1.3. The primes less than 150 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

3.1.4. In addition to the primes in Exercise 3, we have 151, 157, 163, 167, 173, 179, 181, 191, 193, 197 and 199.

3.1.5. Suppose that $n = x^4 - y^4 = (x - y)(x + y)(x^2 + y^2)$, where $x > y$. The integer n can not be prime because it divisible by $x + y$ which can not be 1 or n.

3.1.6. We note that n must be positive. Otherwise $n^3 + 1$ is less than or equal to 1 and no such integers are prime. Because $n^3 + 1 = (n + 1)(n^2 - n + 1), n^3 + 1$ is not prime unless one of the two factors on the right hand side of this equation is 1 and the other is $n^3 + 1$. But $n + 1$ is greater than 1 for every positive integer n, and the only way for $n + 1 = n^3 + 1$ is when $n = 1$ as is easily verified. It is this case we have

$1^3 + 1 = (1 + 1)(1^2 - 1 + 1) = 2$. Hence 2 is the only prime of this form.

3.1.7. Using the identity given in the hint with k such that $1 < k < n$ and $k \mid n$, then $a^k - 1 \mid a^n - 1$. Because $a^n - 1$ is prime by hypothesis, $a^k - 1 = 1$. From this, we see that $a = 2$ and $k = 1$, contradicting the fact that $k > 1$. Thus we must have $a = 2$ and n is prime.

3.1.8. Because Q_n is a positive integer greater than 1, by Lemma 3.1 it has a prime divisor p. If $p \leq n$, then $p|n!$, so then $p|Q_n - n! = 1$, a contradiction. Therefore, we must have $p > n$. So we can construct an infinite sequence of primes as follows. Choose p_1 to be a prime divisor of Q_1. Then choose p_2 to be a prime divisor of Q_{p_1}, and in general choose p_{k+1} to be a prime divisor of Q_{p_k}. Then $p_1 < p_2 < \cdots < p_k < \cdots$, which proves that there are infinitely many primes.

3.1.9. We need to assume $n \geq 3$ to assure that $S_n > 1$. Then by Lemma 3.1, S_n has a prime divisor p. If $p \leq n$ then $p|n!$, and so $p|n! - S_n = 1$, a contradiction. Therefore we must have $p > n$. Because we can find arbitrarily large primes, there must be infinitely many.

3.1.10. a. We proceed by induction. When $n = 1$ we have $p_1 = 2 \leq 2^{2^0} = 2$. Now assume that $p_k \leq 2^{2^k}$ for $k = 1, 2, \ldots, n - 1$. Then by Euclid's proof, a prime q other than $p_1, p_2, \ldots, p_n$ divides Q_n. Then $p_n < q \leq Q_n = p_1 p_2 \cdots p_n + 1 \leq 2^{2^0} 2^{2^1} \cdots 2^{2^{n-1}} = 2^{2^0 + 2^1 + \cdots + 2^{n-1}} = 2^{2^{n-1} - 1} + 1$. Because the inequality is strict and we are dealing with integers we have $p_n \leq 2^{2^{n-1} - 1} \leq 2^{2^{n-1}}$, which completes the induction step.

b. By part a., the $(n+1)$st prime is less than or equal to 2^{2^n}, and because a power of 2 can not be prime itself when $n > 0$, we must have at least $n + 1$ primes strictly less than 2^{2^n}.

3.1.11. $Q_1 = 3, Q_2 = 7, Q_3 = 31, Q_4 = 211, Q_5 = 2311, Q_6 = 30031$. The smallest prime factors are 3, 7, 31, 211, 2311, and 59, respectively.

3.1.12. Let $Q = p_1 p_2 \cdots p_{n-1} + 1$, where p_i is the ith prime. Then by Euclid's proof, some prime q different from $p_1, p_2, \ldots, p_{n-1}$ divides Q. Then $p_n \leq q \leq Q$.

3.1.13. If n is prime, we are done. Otherwise $n/p < (\sqrt[3]{n})^2$. If n/p is prime, then we are done. Otherwise, by Theorem 3.2, n/p has a prime factor less than $\sqrt{n/p} < \sqrt[3]{n}$, a contradiction.

3.1.14. Suppose $p = 3k + 1$ for some positive integer k. If k is odd, then $k = 2n + 1$ for some integer n and so $p = 3(2n + 1) + 1 = 6n + 4 = 2(3n + 2)$ which is clearly not prime, a contradiction. Therefore, k must be even, say $k = 2n$ for some integer n. Then $p = 3(2n) + 1 = 6n + 1$ as desired.

3.1.15. a. The arithmetic progression is $3n + 1$ and the first values are $4, 7, 10, \ldots$. The first prime is 7.

b. We list the first few numbers of the shape $5n + 4$ until we find a prime: $9, 14, 19$, which is prime.

c. We list the first few numbers of the shape $11n + 16$ until we find a prime: $27, 38, 49, 60, 71$, which is prime.

3.1.16. a. We list the first few numbers of the shape $5n + 1$ until we find a prime: $6, 11$, which is prime.

b. We list the first few numbers of the shape $7n + 2$ until we find a prime: $9, 16, 23$, which is prime. (But if we begin with $n = 0$, the first term is 2, which is prime.)

c. We list the first few numbers of the shape $23n + 13$ until we find a prime: $36, 59$, which is prime. (But if we begin with $n = 0$, the first term is 13 which is prime.)