42. Use the generating function $G(x) = \sum_{k=0}^{\infty} f_k x^k$ where f_k is the kth Fibonacci number to find an explicit formula for f_k, proving Theorem 1.7. (*Hint:* Use the fact that $f_k = f_{k-1} + f_{k-2}$ for $k = 2, 3, \ldots$ to show that $G(x) - xG(x) - x^2G(x) = x$. Solve this to show that $G(x) = x/(1 - x - x^2)$ and then write $G(x)$ in terms of partial fractions, as is done in calculus.) (See [Ro07] for information on using generating functions.)

43. Find an explicit formula for the Lucas numbers using the technique of Exercise 41.

44. Find an explicit formula for the Lucas numbers using the technique of Exercise 42.

45. Use mathematical induction to prove Theorem 1.7.

Computations and Explorations

1. Find the Fibonacci numbers f_{100}, f_{200}, and f_{500}.

2. Find the Lucas numbers L_{100}, L_{200}, and L_{500}.

3. Examine as many Fibonacci numbers as possible to determine which are perfect squares. Formulate a conjecture based on your evidence.

4. Examine as many Fibonacci numbers as possible to determine which are triangular numbers. Formulate a conjecture based on your evidence.

5. Examine as many Fibonacci numbers as possible to determine which are perfect cubes. Formulate a conjecture based on your evidence.

6. Find the largest Fibonacci number less than 10,000, less than 100,000, and less than 1,000,000.

7. A surprising theorem states that the Fibonacci numbers are the positive values of the polynomial $2xy^4 + x^2y^3 - 2x^3y^2 - y^5 - x^4y + 2y$ as x and y range over all nonnegative integers. Verify this conjecture for the values of x and y where x and y are nonnegative integers with $x + y \leq 100$.

Programming Projects

1. Given a positive integer n, find the first n terms of the Fibonacci sequence.

2. Given a positive integer n, find the first n terms of the Lucas sequence.

3. Give a positive integer n, find its Zeckendorf representation (defined in the preamble to Exercise 29).

1.5 Divisibility

The concept of the divisibility of one integer by another is central in number theory.

Definition. If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$. If a divides b, we also say that a is a *divisor* or *factor* of b and that b is a *multiple* of a.

If a divides b we write $a \mid b$, and if a does not divide b we write $a \nmid b$. (Be careful not to confuse the notations $a \mid b$, which denotes that a divides b, and a/b, which is the quotient obtained when a is divided by b.)

Example 1.29. The following statements illustrate the concept of the divisibility of integers: $13 \mid 182$, $-5 \mid 30$, $17 \mid 289$, $6 \nmid 44$, $7 \nmid 50$, $-3 \mid 33$, and $17 \mid 0$. ◀

Example 1.30. The divisors of 6 are ± 1, ± 2, ± 3, ± 6. The divisors of 17 are ± 1, ± 17. The divisors of 100 are ± 1, ± 2, ± 4, ± 5, ± 10, ± 20, ± 25, ± 50, ± 100. ◀

In subsequent chapters, we will need some simple properties of divisibility, which we now state and prove.

Theorem 1.8. If a, b, and c are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Because $a \mid b$ and $b \mid c$, there are integers e and f such that $ae = b$ and $bf = c$. Hence, $c = bf = (ae)f = a(ef)$, and we conclude that $a \mid c$. ■

Example 1.31. Because $11 \mid 66$ and $66 \mid 198$, Theorem 1.8 tells us that $11 \mid 198$. ◀

Theorem 1.9. If a, b, m, and n are integers, and if $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$.

Proof. Because $c \mid a$ and $c \mid b$, there are integers e and f such that $a = ce$ and $b = cf$. Hence, $ma + nb = mce + ncf = c(me + nf)$. Consequently, we see that $c \mid (ma + nb)$. ■

Example 1.32. As $3 \mid 21$ and $3 \mid 33$, Theorem 1.9 tells us that 3 divides

$$5 \cdot 21 - 3 \cdot 33 = 105 - 99 = 6.$$ ◀

The following theorem states an important fact about division.

Theorem 1.10. ***The Division Algorithm.*** If a and b are integers such that $b > 0$, then there are unique integers q and r such that $a = bq + r$ with $0 \leq r < b$. ■

In the equation given in the division algorithm, we call q the *quotient* and r the *remainder*. We also call a the *dividend* and b the *divisor*. (*Note:* We use the traditional name for this theorem even though the division algorithm is not actually an algorithm. We discuss algorithms in Section 2.2.)

We note that a is divisible by b if and only if the remainder in the division algorithm is 0. Before we prove the division algorithm, consider the following examples.

Example 1.33. If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, because $133 = 21 \cdot 6 + 7$ and $0 \leq 7 < 21$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$, because $-50 = 8(-7) + 6$ and $0 \leq 6 < 8$. ◀

We now prove the division algorithm using the well-ordering property.

Proof. Consider the set S of all integers of the form $a - bk$ where k is an integer, that is, $S = \{a - bk \mid k \in \mathbf{Z}\}$. Let T be the set of all nonnegative integers in S. T is nonempty, because $a - bk$ is positive whenever k is an integer with $k < a/b$.

By the well-ordering property, T has a least element $r = a - bq$. (These are the values for q and r specified in the theorem.) We know that $r \geq 0$ by construction, and it is easy to see that $r < b$. If $r \geq b$, then $r > r - b = a - bq - b = a - b(q + 1) \geq 0$, which contradicts the choice of $r = a - bq$ as the least nonnegative integer of the form $a - bk$. Hence, $0 \leq r < b$.

To show that these values for q and r are unique, assume that we have two equations $a = bq_1 + r_1$ and $a = bq_2 + r_2$, with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. By subtracting the second of these equations from the first, we find that

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Hence, we see that

$$r_2 - r_1 = b(q_1 - q_2).$$

This tells us that b divides $r_2 - r_1$. Because $0 \leq r_1 < b$ and $0 \leq r_2 < b$, we have $-b < r_2 - r_1 < b$. Hence, b can divide $r_2 - r_1$ only if $r_2 - r_1 = 0$ or, in other words, if $r_1 = r_2$. Because $bq_1 + r_1 = bq_2 + r_2$ and $r_1 = r_2$, we also see that $q_1 = q_2$. This shows that the quotient q and the remainder r are unique. ∎

We now use the greatest integer function (defined in Section 1.1) to give explicit formulas for the quotient and remainder in the division algorithm. Because the quotient q is the largest integer such that $bq \leq a$, and $r = a - bq$, it follows that

$$q = [a/b], \quad r = a - b[a/b]. \tag{1.4}$$

The following examples display the quotient and remainder of a division.

Example 1.34. Let $a = 1028$ and $b = 34$. Then $a = bq + r$ with $0 \leq r < b$, where $q = [1028/34] = 30$ and $r = 1028 - [1028/34] \cdot 34 = 1028 - 30 \cdot 34 = 8$. ◀

Example 1.35. Let $a = -380$ and $b = 75$. Then $a = bq + r$ with $0 \leq r < b$, where $q = [-380/75] = -6$ and $r = -380 - [-380/75] \cdot 75 = -380 - (-6)75 = 70$. ◀

We can use Equation (1.4) to prove a useful property of the greatest integer function.

Example 1.36. Show that if n is a positive integer, then $[x/n] = [[x]/n]$ whenever x is a real number. To prove this identity, suppose that $[x] = m$. By the division algorithm, we have integers q and r such that $m = nq + r$, where $0 \leq r \leq n - 1$. By Equation (1.4), we have $q = [[x]/n]$. Because $[x] \leq x < [x] + 1$, it follows that $x = [x] + \epsilon$, where $0 \leq \epsilon < 1$. We see that $[x/n] = [([x] + \epsilon)/n] = [(m + \epsilon)/n] = [((nq + r) + \epsilon)/n] = [q + (r + \epsilon)/n]$. Because $0 \leq \epsilon < 1$, we have $0 \leq r + \epsilon < (n - 1) + 1 = n$. It follows that $[x/n] = [q]$. ◀

Given a positive integer d, we can classify integers according to their remainders when divided by d. For example, with $d = 2$, we see from the division algorithm that

every integer when divided by 2 leaves a remainder of either 0 or 1. This leads to the following definition of some common terminology.

Definition. If the remainder when n is divided by 2 is 0, then $n = 2k$ for some integer k, and we say that n is *even,* whereas if the remainder when n is divided by 2 is 1, then $n = 2k + 1$ for some integer k, and we say that n is *odd.*

Similarly, when $d = 4$, we see from the division algorithm that when an integer n is divided by 4, the remainder is either 0, 1, 2, or 3. Hence, every integer is of the form $4k$, $4k + 1$, $4k + 2$, or $4k + 3$, where k is a positive integer.

We will pursue these matters further in Chapter 4.

Greatest Common Divisors

If a and b are integers, not both 0, then the set of common divisors of a and b is a finite set of integers, always containing the integers $+1$ and -1. We are interested in the largest integer among the common divisors of the two integers.

Definition. The *greatest common divisor* of two integers a and b, which are not both 0, is the largest integer that divides both a and b.

The greatest common divisor of a and b is written as (a, b). (Note that the notation $\gcd(a, b)$ is also used, especially outside of number theory. We will use the traditional notation (a, b) here, even though it is the same notation used for ordered pairs.) Note that $(0, n) = (n, 0) = n$ whenever n is a positive integer. Even though every positive integer divides 0, we define $(0, 0) = 0$. This is done to ensure that the results we prove about greatest common divisors hold in all cases.

Example 1.37. The common divisors of 24 and 84 are ± 1, ± 2, ± 3, ± 4, ± 6, and ± 12. Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3$, $(100, 5) = 5$, $(17, 25) = 1$, $(0, 44) = 44$, $(-6, -15) = 3$, and $(-17, 289) = 17$. ◀

We are particularly interested in pairs of integers sharing no common divisors greater than 1. Such pairs of integers are called *relatively prime.*

Definition. The integers a and b, with $a \neq 0$ and $b \neq 0$, are *relatively prime* if a and b have greatest common divisor $(a, b) = 1$.

Example 1.38. Because $(25, 42) = 1$, 25 and 42 are relatively prime. ◀

We will study greatest common divisors at length in Chapter 4. In that chapter, we will give an algorithm for computing greatest common divisors. We will also prove many important results about them that lead to key theorems in number theory.

1.5 Exercises

1. Show that $3 \mid 99$, $5 \mid 145$, $7 \mid 343$, and $888 \mid 0$.
2. Show that 1001 is divisible by 7, by 11, and by 13.
3. Decide which of the following integers are divisible by 7.
   a) 0 c) 1717 e) −285,714
   b) 707 d) 123,321 f) −430,597
4. Decide which of the following integers are divisible by 22.
   a) 0 c) 1716 e) −32,516
   b) 444 d) 192,544 f) −195,518
5. Find the quotient and remainder in the division algorithm, with divisor 17 and dividend
   a) 100. b) 289. c) −44. d) −100.
6. Find all positive integers that divide each of these integers.
   a) 12 b) 22 c) 37 d) 41
7. Find all positive integers that divide each of these integers.
   a) 13 b) 21 c) 36 d) 44
8. Find these greatest common divisors by finding all positive integers that divide each integer in the pair and selecting the largest that divides both.
   a) (8, 12) b) (7, 9) c) (15, 25) d) (16, 27)
9. Find these greatest common divisors by finding all positive integers that divide each integer in the pair and selecting the largest that divides both.
   a) (11, 22) b) (36, 42) c) (21, 22) d) (16, 64)
10. Find all positive integers less than 10 that are relatively prime to it.
11. Find all positive integers less than 11 that are relatively prime to it.
12. Find all pairs of positive integers not exceeding 10 that are relatively prime.
13. Find all pairs of positive integers between 10 and 20, inclusive, that are relatively prime.
14. What can you conclude if a and b are nonzero integers such that $a \mid b$ and $b \mid a$?
15. Show that if a, b, c, and d are integers with a and c nonzero, such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.
16. Are there integers a , b, and c such that $a \mid bc$, but $a \nmid b$ and $a \nmid c$?
17. Show that if a, b, and $c \neq 0$ are integers, then $a \mid b$ if and only if $ac \mid bc$.
18. Show that if a and b are positive integers and $a \mid b$, then $a \leq b$.
19. Show that if a and b are integers such that $a \mid b$, then $a^k \mid b^k$ for every positive integer k.
20. Show that the sum of two even or of two odd integers is even, whereas the sum of an odd and an even integer is odd.
21. Show that the product of two odd integers is odd, whereas the product of two integers is even if either of the integers is even.
22. Show that if a and b are odd positive integers and $b \nmid a$, then there are integers s and t such that $a = bs + t$, where t is odd and $| t | < b$.

23. When the integer a is divided by the integer b, where $b > 0$, the division algorithm gives a quotient of q and a remainder of r. Show that if $b \nmid a$, when $-a$ is divided by b, the division algorithm gives a quotient of $-(q+1)$ and a remainder of $b - r$, whereas if $b \mid a$, the quotient is $-q$ and the remainder is 0.

24. Show that if a, b, and c are integers with $b > 0$ and $c > 0$, such that when a is divided by b the quotient is q and the remainder is r, and when q is divided by c the quotient is t and the remainder is s, then when a is divided by bc, the quotient is t and the remainder is $bs + r$.

25. a) Extend the division algorithm by allowing negative divisors. In particular, show that whenever a and $b \neq 0$ are integers, there are unique integers q and r such that $a = bq + r$, where $0 \leq r < |b|$.

b) Find the remainder when 17 is divided by -7.

➢ **26.** Show that if a and b are positive integers, then there are unique integers q and r such that $a = bq + r$, where $-b/2 < r \leq b/2$. This result is called the *modified division algorithm.*

27. Show that if m and $n > 0$ are integers, then

$$\left\lceil \frac{m+1}{n} \right\rceil = \begin{cases} \left\lceil \frac{m}{n} \right\rceil & \text{if } m \neq kn - 1 \text{ for some integer } k; \\ \left\lceil \frac{m}{n} \right\rceil + 1 & \text{if } m = kn - 1 \text{ for some integer } k. \end{cases}$$

28. Show that the integer n is even if and only if $n - 2[n/2] = 0$.

29. Show that the number of positive integers less than or equal to x, where x is a positive real number, that are divisible by the positive integer d equals $[x/d]$.

30. Find the number of positive integers not exceeding 1000 that are divisible by 5, by 25, by 125, and by 625.

31. How many integers between 100 and 1000 are divisible by 7? by 49?

32. Find the number of positive integers not exceeding 1000 that are not divisible by 3 or 5.

33. Find the number of positive integers not exceeding 1000 that are not divisible by 3, 5, or 7.

34. Find the number of positive integers not exceeding 1000 that are divisible by 3 but not by 4.

35. In early 2010, to mail a first-class letter in the United States of America it cost 44 cents for the first ounce and 17 cents for each additional ounce or fraction thereof. Find a formula involving the greatest integer function for the cost of mailing a letter in early 2010. Could it possibly have cost \$1.81 or \$2.65 to mail a first-class letter in the United States of America in early 2010?

36. Show that if a is an integer, then 3 divides $a^3 - a$.

37. Show that the product of two integers of the form $4k + 1$ is again of this form, whereas the product of two integers of the form $4k + 3$ is of the form $4k + 1$.

38. Show that the square of every odd integer is of the form $8k + 1$.

39. Show that the fourth power of every odd integer is of the form $16k + 1$.

40. Show that the product of two integers of the form $6k + 5$ is of the form $6k + 1$.

41. Show that the product of any three consecutive integers is divisible by 6.

42. Use mathematical induction to show that $n^5 - n$ is divisible by 5 for every positive integer n.

43. Use mathematical induction to show that the sum of the cubes of three consecutive integers is divisible by 9.

In Exercises 44–48, let f_n denote the nth Fibonacci number.

44. Show that f_n is even if and only if n is divisible by 3.

45. Show that f_n is divisible by 3 if and only if n is divisible by 4.

46. Show that f_n is divisible by 4 if and only if n is divisible by 6.

47. Show that $f_n = 5f_{n-4} + 3f_{n-5}$ whenever n is a positive integer with $n > 5$. Use this result to show that f_n is divisible by 5 whenever n is divisible by 5.

* **48.** Show that $f_{n+m} = f_m f_{n+1} + f_{m-1} f_n$ whenever m and n are positive integers with $m > 1$. Use this result to show that $f_n \mid f_m$ when m and n are positive integers with $n \mid m$.

Let n be a positive integer. We define

$$T(n) = \begin{cases} n/2 & \text{if } n \text{ is even;} \\ (3n+1)/2 & \text{if } n \text{ is odd.} \end{cases}$$

We then form the sequence obtained by iterating T: n, $T(n)$, $T(T(n))$, $T(T(T(n)))$, ... For instance, starting with $n = 7$, we have 7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, 2, 1, ... A well-known conjecture, sometimes called the *Collatz conjecture,* asserts that the sequence obtained by iterating T always reaches the integer 1 no matter which positive integer n begins the sequence.

49. Find the sequence obtained by iterating T starting with $n = 39$.

50. Show that the sequence obtained by iterating T starting with $n = (2^{2k} - 1)/3$, where k is a positive integer greater than 1, always reaches the integer 1.

51. Show that the Collatz conjecture is true if it can be shown that for every positive integer n with $n \geq 2$ there is a term in the sequence obtained by iterating T that is less than n.

52. Verify that there is a term in the sequence obtained by iterating T, starting with the positive integer n, that is less than n for all positive integers n with $2 \leq n \leq 100$. (*Hint:* Begin by considering sets of positive integers for which it is easy to show that this is true.)

* **53.** Show that $[(2 + \sqrt{3})^n]$ is odd whenever n is a nonnegative integer.

* **54.** Determine the number of positive integers n such that $[a/2] + [a/3] + [a/5] = a$, where, as usual, $[x]$ is the greatest integer function.

55. Prove the divison algorithm using the second principle of mathematical induction.

Computations and Explorations

1. Find the quotient and remainder when 111,111,111,111 is divided by 987,654,321.

2. Verify the Collatz conjecture described in the preamble to Exercise 49 for all integers n not exceeding 10,000.

3. Using numerical evidence, what sort of conjectures can you make concerning the number of iterations needed before the sequence of iterations $T(n)$ reaches 1, where n is a given positive integer?

4. Using numerical evidence, make conjectures about the divisibility of Fibonacci numbers by 7, by 8, by 9, by 11, and by 13.

Programming Projects

1. Decide whether an integer is divisible by a given integer.
2. Find the quotient and remainder in the division algorithm.
3. Find the quotient, remainder, and sign in the modified division algorithm given in Exercise 26.
4. Compute the terms of the sequence $n, T(n), T(T(n)), T(T(T(n))), \ldots$ for a given positive integer n, as defined in the preamble to Exercise 49.