Programming Projects

1. Find all of the positive divisors of a positive integer from its prime factorization.
2. Find the greatest common divisor of two positive integers from their prime factorizations.
3. Find the least common multiple of two positive integers from their prime factorizations.
4. Find the number of zeros at the end of the decimal expansion of $n!$, where n is a positive integer.
5. Find the prime factorization of $n!$, where n is a positive integer.
6. Find the number of powerful numbers (defined in Exercise 9) less than a positive integer n.

3.6 Factorization Methods and the Fermat Numbers

By the fundamental theorem of arithmetic, we know that every positive integer can be written uniquely as the product of primes. In this section, we discuss the problem of determining this factorization, and we introduce several simple factoring methods. Factoring integers is an extremely active area of mathematical research, especially because it is important in cryptography, as we will see in Chapter 8. In that chapter, we will learn that the security of the RSA public-key cryptosystem is based on the observation that factoring integers is much, much harder than finding large primes.

Before we discuss the current status of factoring algorithms, we will consider the most direct way to factor integers, called *trial division.* We will explain why it is not very efficient. Recall from Theorem 3.2 that n either is prime or has a prime factor not exceeding $\sqrt{n}$. Consequently, when we divide n successively by the primes 2, 3, 5, . . . , not exceeding $\sqrt{n}$, either we find a prime factor p_1 of n or we conclude that n is prime. If we have located a prime factor p_1 of n, we next look for a prime factor of $n_1 = n/p_1$, beginning our search with the prime p_1, as n_1 has no prime factor less than p_1, and any factor of n_1 is also a factor of n. We continue, if necessary, determining whether any of the primes not exceeding $\sqrt{n_1}$ divide n_1. We continue in this manner, proceeding iteratively, to find the prime factorization of n.

Example 3.22. Let $n = 42{,}833$. We note that n is not divisible by 2, 3, or 5, but that $7 \mid n$. We have

$$42{,}833 = 7 \cdot 6119.$$

Trial divisions show that 6119 is not divisible by any of the primes 7, 11, 13, 17, 19, or 23. However, we see that

$$6119 = 29 \cdot 211.$$

Because $29 > \sqrt{211}$, we know that 211 is prime. We conclude that the prime factorization of 42,833 is $42{,}833 = 7 \cdot 29 \cdot 211$. ◀

Unfortunately, this method for finding the prime factorization of an integer is quite inefficient. To factor an integer N, it may be necessary to perform as many as $\pi(\sqrt{N})$ divisions (assuming that we already have a list of the primes not exceeding $\sqrt{N}$), altogether requiring on the order of $\sqrt{N}\log N$ bit operations because, from the prime number theorem, $\pi(\sqrt{N})$ is approximately $\sqrt{N}/\log\sqrt{N} = 2\sqrt{N}/\log N$, and from Theorem 2.7, these divisions take $O(\log^2 N)$ bit operations each.

Modern Factorization Methods

Mathematicians have long been fascinated with the problem of factoring integers. In the seventeenth century, *Pierre de Fermat* invented a factorization method based on the idea of representing a composite integer as the difference of two squares. This method is of theoretical and some practical importance, but is not very efficient in itself. We will discuss Fermat's factorization method later in this section.

Since 1970, many new factorization methods have been invented that make it possible, using powerful modern computers, to factor integers that had previously seemed impervious. We will describe several of the simplest of these newer methods. However, the most powerful factorization methods currently known are extremely complicated. Their description is beyond the scope of this book, but we will discuss the size of the integers that they can factor.

Among recent factorization methods (developed in the past 30 years) are several invented by J. M. Pollard, including the Pollard rho method (discussed in Section 4.6) and the Pollard $p-1$ method (discussed in Section 6.1). These two methods are generally too slow for difficult factoring problems, unless the numbers being factored have special properties. In Section 12.5, we will introduce another method for factoring that uses continued fractions. A variation of this method, introduced by Morrison and Brillhart, was the major method used to factor large integers during the 1970s. This algorithm was the first factoring algorithm to run in *subexponential time*, which means that the number of bit operations required to factor an integer n could be written in the form $n^{\alpha(n)}$ where $\alpha(n)$ decreases as n increases. A useful notation for describing the number

PIERRE DE FERMAT (1601–1665) was a lawyer by profession. He was a noted jurist at the provincial parliament in the French city of Toulouse. Fermat was probably the most famous amateur mathematician in history. He published almost none of his mathematical discoveries, but did correspond with contemporary mathematicians about them. From his correspondents, especially the French monk Mersenne (discussed in Chapter 6), the world learned about his many contributions to mathematics. Fermat was one of the inventors of analytic geometry. Furthermore, he laid the foundations of calculus. Fermat, along with Pascal, gave a mathematical basis to the concept of probability. Some of Fermat's discoveries come to us only because he made notes in the margins of his copy of the work of Diophantus. His son found his copy with these notes, and published them so that other mathematicians would be aware of Fermat's results and claims.

of bit operations required to factor a number by an algorithm running in subexponential time is $L(a, b)$, which implies that the number of bit operations used by the algorithm is $O(\exp(b(\log n)^a(\log\log n)^{1-a}))$. (The precise definition of $L(a, b)$ is somewhat more complicated.) The variation of the continued fraction algorithm invented by Morrison and Brillhart uses $L(1/2, \sqrt{3/2})$ bit operations. Its greatest success was the factorization of a 63-digit number in 1970.

The *quadratic sieve,* described by Carl Pomerance in 1981, made it possible for the first time to factor numbers having more than one hundred digits not of a special form. This method, with many enhancements added after its original invention, uses $L(1/2, 1)$ bit operations. Its great success was in factoring a 129-digit integer known as RSA-129, whose factorization was posed as a challenge by the inventors of the RSA cryptosystem discussed in Chapter 8. Currently, the best general-purpose factoring algorithm for integers with more than 115 digits is the *number field sieve,* originally suggested by Pollard and improved by Buhler, Lenstra, and Pomerance, which uses $L(1/3, (64/9)^{1/3})$ bit operations. Its greatest success has been the factorization of a 200-digit integer known as RSA-200 in 2005. For factoring numbers with fewer than 115 digits, the quadratic sieve still seems to be quicker than the number field sieve.

An important feature of the number field and quadratic sieves (as well as other methods) is that these algorithms can be run in parallel on many computers (or processors) at the same time. This makes it possible for large teams of people to work on factoring the same integer. (See the historical note on factoring RSA-129 and other RSA challenge numbers, at the end of this subsection.)

How big will the numbers be that can be factored in the future? The answer depends on whether (or, more likely, how soon) more efficient algorithms are invented, as well as how quickly computing power advances. A useful and commonly used measure for estimating the amount of computing required to factor integers of a certain size is millions of instructions per second–years, or MIPS–years. (One MIPS–year represents the computing power of the classical DEC VAX 11/780 during one year. It is still used as a reference point even though this computer is obsolete. Pentium PCs operate at hundreds of MIPS.) Table 3.2 (adapted from information in [Od95]) displays the computing power (in terms of MIPS–years, rounded to the nearest power of ten) required to factor integers of a given size using the number field sieve. Teams of people can

Number of Decimal Digits	Approximate MIPS–Years Required
150	10^4
225	10^8
300	10^{11}
450	10^{16}
600	10^{20}

Table 3.2 *Computing power required to factor integers using the number field sieve.*

work together, dedicating thousands or even millions of MIPS–years to factor particular numbers. Consequently, even without the development of new algorithms, it might not be surprising to see the factorization, within the next few years, of integers (not of a special form) with 250, or perhaps 300, decimal digits.

For further information on factoring algorithms, we refer the reader to [Br89], [Br00], [CrPo05], [Di84], [Gu75], [Od95], [Po84], [Po90], [Ri94], [Ru83], [WaSm87], and [Wi84].

Fermat Factorization We now describe a factorization technique that is interesting, although it is not always efficient. This technique, discovered by Fermat, is known as *Fermat factorization,* and is based on the following lemma.

Lemma 3.9. If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers and differences of two squares that equal n.

Proof. Let n be an odd positive integer and let $n = ab$ be a factorization of n into two positive integers. Then n can be written as the difference of two squares, because

$$n = ab = s^2 - t^2,$$

where $s = (a + b)/2$ and $t = (a - b)/2$ are both integers because a and b are both odd.

Conversely, if n is the difference of two squares, say, $n = s^2 - t^2$, then we can factor n by noting that $n = (s - t)(s + t)$.

The RSA Factoring Challenge

The RSA Factoring Challenge, which ran from 1991 to 2007, was a contest that challenged mathematicians to factor certain large integers. Its purpose was to track progress in factorization methods, which has important implications for cryptography (see Chapter 8). The first RSA challenge made in 1991, first posed in 1977 in Martin Gardner's column in *Scientific American,* was to factor a 129-digit integer, known as RSA-129. A $100 prize was offered for the decryption of a message; the message could be decrypted easily when this 129-digit number was factored, but not otherwise. Seventeen years passed before this challenge was met in 1994. The factorization of RSA-129 using the quadratic sieve method took approximately 5000 MIPS–years, and was carried out in eight months by more than 600 people working together. RSA Labs, a part of RSA Data Security (the company that holds the patents for the RSA cryptosystem discussed in Chapter 8), sponsored the challenge, and offered cash prizes for the factorization of integers on challenge lists. They awarded awarded more than $80,000 for successful factorizations. Factorizations of numbers on their list led to world records. For example, in 1996, a team led by Arjen Lenstra used the number field sieve to factor RSA-130. This took approximately 750 MIPS–years. In 1999, the number field sieve was used to factor RSA-140 and RSA-155, using 2000 and 8000 MIPS–years, respectively. The largest number factored as part of this challenge was RSA-200, an integer with 200 decimal digits, which was factored in 2005 by a team led by Jens Franke at the University of Bonn.

We leave it to the reader to show that this is a one-to-one correspondence. ■

To carry out the method of Fermat factorization, we look for solutions of the equation $n = x^2 - y^2$ by searching for perfect squares of the form $x^2 - n$. Hence, to find factorizations of n, we search for a square among the sequence of integers

$$t^2 - n,\ (t+1)^2 - n,\ (t+2)^2 - n, \ldots$$

where t is the smallest integer greater than $\sqrt{n}$. This procedure is guaranteed to terminate, because the trivial factorization $n = n \cdot 1$ leads to the equation

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

Example 3.23. We factor 6077 using the method of Fermat factorization. Because $77 < \sqrt{6077} < 78$, we look for a perfect square in the sequence

$$\begin{aligned} 78^2 - 6077 &= 7 \\ 79^2 - 6077 &= 164 \\ 80^2 - 6077 &= 323 \\ 81^2 - 6077 &= 484 = 22^2. \end{aligned}$$

Because $6077 = 81^2 - 22^2$, we see that $6077 = (81 - 22)(81 + 22) = 59 \cdot 103$. ◀

Unfortunately, Fermat factorization can be very inefficient. To factor n using this technique, it may be necessary to check as many as $(n+1)/2 - [\sqrt{n}]$ integers to determine whether they are perfect squares. Fermat factorization works best when it is used to factor integers having two factors of similar size. Although Fermat factorization is rarely used to factor large integers, its basic idea is the basis for many more powerful factorization algorithms used extensively in computer calculations.

The Fermat Numbers

The integers $F_n = 2^{2^n} + 1$ are called the *Fermat numbers*. Fermat conjectured that these integers are all primes. Indeed, the first few are primes, namely, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65{,}537$. Unfortunately, $F_5 = 2^{2^5} + 1$ is composite, as we will now demonstrate.

Example 3.24. The Fermat number $F_5 = 2^{2^5} + 1$ is divisible by 641. We can show that $641 \mid F_5$ without actually performing the division, using several not-so-obvious observations. Note that

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4.$$

Hence,

$$\begin{aligned} 2^{2^5}+1 &= 2^{32}+1 = 2^4\cdot 2^{28}+1 = (641-5^4)2^{28}+1 \\ &= 641\cdot 2^{28} - (5\cdot 2^7)^4 + 1 = 641\cdot 2^{28} - (641-1)^4 + 1 \\ &= 641(2^{28} - 641^3 + 4\cdot 641^2 - 6\cdot 641 + 4). \end{aligned}$$

Therefore, we see that $641 \mid F_5$. ◀

The following result is a valuable aid in the factorization of Fermat numbers.

Theorem 3.20. Every prime divisor of the Fermat number $F_n = 2^{2^n}+1$ is of the form $2^{n+2}k+1$.

The proof of Theorem 3.20 is presented as an exercise in Chapter 11. Here, we indicate how Theorem 3.20 is useful in determining the factorization of Fermat numbers.

Example 3.25. From Theorem 3.20, we know that every prime divisor of $F_3 = 2^{2^3}+1 = 257$ must be of the form $2^5k+1 = 32\cdot k+1$. Because there are no primes of this form less than or equal to $\sqrt{257}$, we can conclude that $F_3 = 257$ is prime. ◀

Example 3.26. When factoring $F_6 = 2^{2^6}+1$, we use Theorem 3.20 to see that all of its prime factors are of the form $2^8k+1 = 256\cdot k+1$. Hence, we need only perform trial divisions of F_6 by primes of the form $256\cdot k+1$ that do not exceed $\sqrt{F_6}$. After considerable computation, we find that a prime divisor is obtained with $k = 1071$, that is, $274{,}177 = (256\cdot 1071+1) \mid F_6$. ◀

Known Factorizations of Fermat Numbers A tremendous amount of effort has been devoted to the factorization of Fermat numbers. As yet, no new Fermat primes (beyond F_4) have been found. Many mathematicians believe that no additional Fermat primes exist. We will develop a primality test for Fermat numbers in Chapter 11, which has been used to show that many Fermat numbers are composite. (When such a test is used, it is not necessary to use trial division to show that a number is not divisible by a prime not exceeding its square root.)

As of early 2010, a total of 243 Fermat numbers are known to be composite, but the complete factorizations are known for only seven composite Fermat numbers: F_5, F_6, F_7, F_8, F_9, F_{10}, and F_{11}. The Fermat number F_9, a number with 155 decimal digits, was factored in 1990 by Mark Manasse and Arjen Lenstra, using the number field sieve, which breaks the problem of factoring an integer into a large number of smaller factoring problems that can be done in parallel. Though Manasse and Lenstra farmed out computations for the factorization of F_9 to hundreds of mathematicians and computer scientists, it still took about two months to complete the computations. (For details of the factorization of F_9, see [Ci90].)

The prime factorization of F_{11} was discovered by Richard Brent in 1989, using a factorization algorithm known as the elliptic curve method (described in detail in [Br89]). There are 617 decimal digits in F_{11}, and $F_{11} = 319{,}489\cdot 974{,}849\cdot P_{21}\cdot P_{22}\cdot P_{564}$, where

P_{21}, P_{22}, and P_{564} are primes with 21, 22, and 564 digits, respectively. It took until 1995 for Brent to completely factor F_{10}. He discovered, using elliptic curve factorization, that $F_{10} = 45{,}592{,}577 \cdot 6{,}487{,}031{,}809 \cdot P_{40} \cdot P_{252}$, where P_{40} and P_{252} are primes with 40 and 252 digits, respectively.

Many Fermat numbers are known to be composite because at least one prime factor of these numbers has been found, using results such as Theorem 3.20. It is also known that F_n is composite for $n = 14$, 20, 22, and 24, but no factors of these numbers have yet been found. The largest n for which it is known that F_n is composite is $n = 2{,}478{,}782$. ($F_{382,447}$ was the first Fermat number with more than 100,000 digits shown to be composite; it was shown to be composite in July 1999.) F_{33} is the smallest Fermat number that has not yet been shown to be composite, if it is indeed composite. Because of steady advances in computer software and hardware, we can expect new results on the nature of Fermat numbers and their factorizations to be found at a healthy rate.

The factorization of Fermat numbers is part of the *Cunningham project*, sponsored by the American Mathematical Society. Devoted to building tables of all the known factors of integers of the form $b^n \pm 1$, where $b = 2$, 3, 5, 6, 7, 10, 11, and 12, the project's name refers to A. J. Cunningham, a colonel in the British army, who compiled a table of factors of integers of this sort in the early years of the twentieth century. The factor tables as of 1988 are contained in [Br88]; the current state of affairs is available over the Internet. Numbers of the form $b^n \pm 1$ are of special interest because of their importance in generating pseudorandom numbers (see Chapter 10), their importance in abstract algebra, and their significance in number theory.

In conjunction with the Cunningham project, a list of the "ten most wanted" integers to be factored is kept by Samuel Wagstaff of Purdue University. For example, until it was factored in 1990, F_9 was on this list. With advances in factoring techniques and computer power, increasingly larger numbers are included on the list. In the early 1980s, the largest had between 50 and 70 decimal digits; in the early 1990s, they had between 90 and 130 decimal digits; in the early 2000s, they had between 150 and 200 decimal digits, as of early 2010, they had between 185 and 233 decimal digits.

Using the Fermat Numbers to Prove the Infinitude of Primes It is possible to prove that there are infinitely many primes using Fermat numbers. We begin by showing that any two distinct Fermat numbers are relatively prime. The following lemma will be used.

Lemma 3.10. Let $F_k = 2^{2^k} + 1$ denote the kth Fermat number, where k is a nonnegative integer. Then for all positive integers n, we have

$$F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2.$$

Proof. We will prove the lemma using mathematical induction. For $n = 1$, the identity reads

$$F_0 = F_1 - 2.$$

This is obviously true, because $F_0 = 3$ and $F_1 = 5$. Now, let us assume that the identity holds for the positive integer n, so that

$$F_0F_1F_2 \cdots F_{n-1} = F_n - 2.$$

With this assumption, we can easily show that the identity holds for the integer $n + 1$, because

$$\begin{aligned} F_0F_1F_2 \cdots F_{n-1}F_n &= (F_0F_1F_2 \cdots F_{n-1})F_n \\ &= (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) \\ &= (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \end{aligned}$$

■

This leads to the following theorem.

Theorem 3.21. Let m and n be distinct nonnegative integers. Then the Fermat numbers F_m and F_n are relatively prime.

Proof. Let us assume that $m < n$. By Lemma 3.10, we know that

$$F_0F_1F_2 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

Assume that d is a common divisor of F_m and F_n. Then, Theorem 1.8 tells us that

$$d \mid (F_n - F_0F_1F_2 \cdots F_m \cdots F_{n-1}) = 2.$$

Hence, either $d = 1$ or $d = 2$. However, because F_m and F_n are odd, d cannot be 2. Consequently, $d = 1$ and $(F_m, F_n) = 1$. ■

Using Fermat numbers, we now give another proof that there are infinitely many primes. First, we note that by Lemma 3.1 in Section 3.1, every Fermat number F_n has a prime divisor p_n. Because $(F_m, F_n) = 1$, we know that $p_m \neq p_n$ whenever $m \neq n$. Hence, we can conclude that there are infinitely many primes.

The Fermat Primes and Geometry The Fermat primes are important in geometry. The proof of the following famous theorem of Gauss may be found in [Or88].

Theorem 3.22. A regular polygon of n sides can be constructed using a straightedge (unmarked ruler) and compass if and only if n is the product of a nonnegative power of 2 and a nonnegative number of distinct Fermat primes.

3.6 Exercises

1. Find the prime factorization of each of the following positive integers.
   a) 33,776,925 b) 210,733,237 c) 1,359,170,111
2. Find the prime factorization of each of the following positive integers.
   a) 33,108,075 b) 7,300,977,607 c) 4,165,073,376,607
3. Using the Fermat factorization method, factor each of the following positive integers.
   a) 143 b) 2279 c) 43 d) 11,413

4. Using the Fermat factorization method, factor each of the following positive integers.

a) 8051 c) 46,009 e) 3,200,399

b) 73 d) 11,021 f) 24,681,023

5. Show that the last two decimal digits of a perfect square must be one of the following pairs: 00, $e1$, $e4$, 25, $o6$, $e9$, where e stands for any even digit and o stands for any odd digit. (*Hint:* Show that n^2, $(50 + n)^2$, and $(50 - n)^2$ all have the same final decimal digits, and then consider those integers n with $0 \leq n \leq 25$.)

6. Explain how the result of Exercise 5 can be used to speed up Fermat's factorization method.

7. Show that if the smallest prime factor of n is p, then $x^2 - n$ will not be a perfect square for $x > (n + p^2)/(2p)$, with the single exception $x = (n + 1)/2$.

Exercises 8–10 involve the method of *Draim factorization.* To use this technique to search for a factor of the positive integer $n = n_1$, we start by using the division algorithm, to obtain

$$n_1 = 3q_1 + r_1, \quad 0 \leq r_1 < 3.$$

Setting $m_1 = n_1$, we let

$$m_2 = m_1 - 2q_1, \quad n_2 = m_2 + r_1.$$

We use the division algorithm again, to obtain

$$n_2 = 5q_2 + r_2, \quad 0 \leq r_2 < 5,$$

and we let

$$m_3 = m_2 - 2q_2, \quad n_3 = m_3 + r_2.$$

We proceed recursively, using the division algorithm, to write

$$n_k = (2k + 1)q_k + r_k, \quad 0 \leq r_k < 2k + 1,$$

and we define

$$m_k = m_{k-1} - 2q_{k-1}, \quad n_k = m_k + r_{k-1}.$$

We stop when we obtain a remainder $r_k = 0$.

8. Show that $n_k = kn_1 - (2k + 1)(q_1 + q_2 + \cdots + q_{k-1})$ and that $m_k = n_1 - 2 \cdot (q_1 + q_2 + \cdots + q_{k-1})$.

9. Show that if $(2k + 1) \mid n$, then$(2k + 1) \mid n_k$ and $n = (2k + 1)m_{k+1}$.

10. Factor 5899 using Draim factorization.

In Exercises 11–13, we develop a factorization technique known as *Euler's method.* It is applicable when the integer being factored is odd and can be written as the sum of two squares in two different ways. Let n be odd and let $n = a^2 + b^2 = c^2 + d^2$, where a and c are odd positive integers and b and d are even positive integers.

11. Let $u = (a - c, b - d)$. Show that u is even, and that if $r = (a - c)/u$ and $s = (d - b)/u$, then $(r, s) = 1$, $r(a + c) = s(d + b)$, and $s \mid (a + c)$.

12. Let $sv = a + c$. Show that $rv = d + b$, $v = (a + c, d + b)$, and v is even.

13. Conclude that n may be factored as $n = [(u/2)^2 + (v/2)^2](r^2 + s^2)$.

14. Use Euler's method to factor each of the following integers.
   a) $221 = 10^2 + 11^2 = 5^2 + 14^2$
   b) $2501 = 50^2 + 1^2 = 49^2 + 10^2$
   c) $1{,}000{,}009 = 1000^2 + 3^2 = 972^2 + 235^2$

15. Show that any number of the form $2^{4n+2} + 1$ can be factored easily by the use of the identity $4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$. Factor $2^{18} + 1$ using this identity.

16. Show that if a is a positive integer and $a^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer n. (*Hint:* Recall the identity $a^m + 1 = (a^k + 1)(a^{k(l-1)} - a^{k(l-2)} + \cdots - a^k + 1)$, where $m = kl$ and l is odd.)

17. Show that the last digit in the decimal expansion of $F_n = 2^{2^n} + 1$ is 7 if $n \geq 2$. (*Hint:* Using mathematical induction, show that the last decimal digit of 2^{2^n} is 6.)

18. Use the fact that every prime divisor of $F_4 = 2^{2^4} + 1 = 65{,}537$ is of the form $2^6k + 1 = 64k + 1$ to verify that F_4 is prime. (You should need only one trial division.)

19. Use the fact that every prime divisor of $F_5 = 2^{2^5} + 1$ is of the form $2^7k + 1 = 128k + 1$ to demonstrate that the prime factorization of F_5 is $F_5 = 641 \cdot 6{,}700{,}417$.

20. Find all primes of the form $2^{2^n} + 5$, where n is a nonnegative integer.

21. Estimate the number of decimal digits in the Fermat number F_n.

* **22.** What is the greatest common divisor of n and F_n, where n is a positive integer? Prove that your answer is correct.

23. Show that the only integer of the form $2^m + 1$, where m is a positive integer, that is a power of a positive integer (i.e., is of the form n^k, where n and k are positive integers with $k \geq 2$) occurs when $m = 3$.

24. Factoring kn by the Fermat factorization method, where k is a small positive integer, is sometimes easier than factoring n by this method. Show that to factor 901 by the Fermat factorization method, it is easier to factor $3 \cdot 901 = 2703$ than to factor 901.

Computations and Explorations

1. Using trial division, find the prime factorization of several integers of your choice exceeding 10,000.

2. Factor several integers of your choice exceeding 10,000, using Fermat factorization.

3. Factor the Fermat numbers F_6 and F_7 using Theorem 3.20.

Programming Projects

1. Given a positive integer n, find the prime factorization of n.

2. Given a positive integer n, perform the Fermat factorization method on n.

3. Given a positive integer n, perform Draim factorization on n (see the preamble to Exercise 8).

4. Check the Fermat number F_n, where n is a positive integer, for prime factors, using Theorem 3.20.

3.7 Linear Diophantine Equations

Consider the following problem: A man wishes to purchase \$510 of travelers' checks. The checks are available only in denominations of \$20 and \$50. How many of each denomination should he buy? If we let x denote the number of \$20 checks and y the number of \$50 checks that he should buy, then the equation $20x + 50y = 510$ must be satisfied. To solve this problem, we need to find all solutions of this equation, where both x and y are nonnegative integers.

A related problem arises when a woman wishes to mail a package. The postal clerk determines the cost of postage to be 83 cents, but only 6-cent and 15-cent stamps are available. Can some combination of these stamps be used to mail the package? To answer this, we first let x denote the number of 6-cent stamps and y the number of 15-cent stamps to be used. Then we must have $6x + 15y = 83$, where both x and y are nonnegative integers.

When we require that solutions of a particular equation come from the set of integers, we have a *diophantine equation.* These equations get their name from the ancient Greek mathematician *Diophantus*, who wrote on equations where solutions are restricted to rational numbers. The equation $ax + by = c$, where a, b, and c are integers, is called a *linear diophantine equation in two variables.*

Note that the pair of integers (x, y) is a solution of the linear diophantine equation $ax + by = c$ if and only if the (x, y) is a lattice point in the plane that lies on the line $ax + by = c$. We illustrate this in Figure 3.2 for the linear diophantine equation $2x + 3y = 5$.

The first person to describe a general solution of linear diophantine equations was the Indian mathematician *Brahmagupta*, who included it in a book he wrote in the seventh century. We now develop the theory for solving such equations. The following theorem tells us when such an equation has solutions, and when there are solutions, explicitly describes them.

Theorem 3.23. Let a and b be integers with $d = (a, b)$. The equation $ax + by = c$ has no integral solutions if $d \nmid c$. If $d \mid c$, then there are infinitely many integral solutions.

DIOPHANTUS (c. 250) wrote the *Arithmetica,* which is the earliest known book on algebra; it contains the first systematic use of mathematical notation to represent unknowns in equations and powers of these unknowns. Almost nothing is known about Diophantus, other than that he lived in Alexandria around 250 C.E. The only source of details about his life comes from an epigram found in a collection called the *Greek Anthology:* "Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh as a bachelor. Five years after his marriage was born a son who died four years before his father, at half his father's age." From this the reader can infer that Diophantus lived to the age of 84.

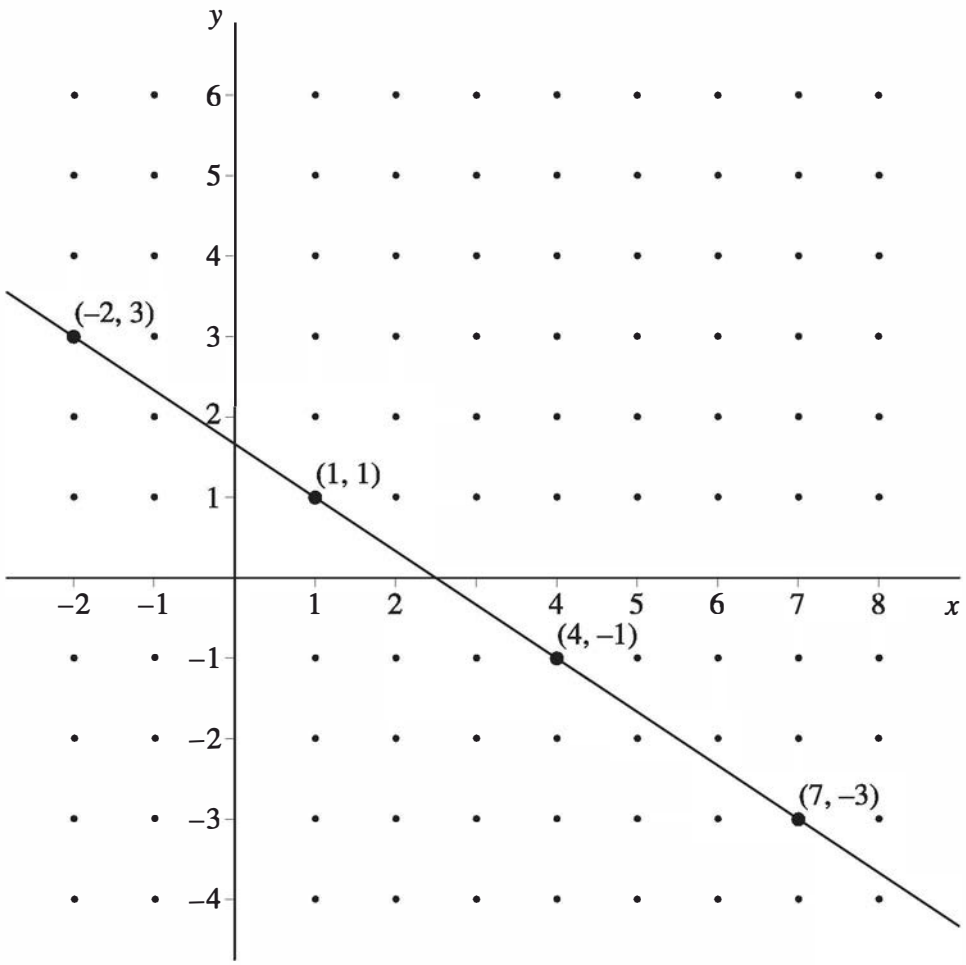

Figure 3.2 *Solutions of* $2x + 3y = 5$ *in integers* x *and* y *correspond to the lattice points on the line* $2x + 3y = 5$.

Moreover, if $x = x_0$, $y = y_0$ is a particular solution of the equation, then all solutions are given by

$$x = x_0 + (b/d)n, \qquad y = y_0 - (a/d)n,$$

where n is an integer.

Proof. Assume that x and y are integers such that $ax + by = c$. Then, because $d \mid a$ and $d \mid b$, by Theorem 1.9, $d \mid c$ as well. Hence, if $d \nmid c$, there are no integral solutions of the equation.

Now assume that $d \mid c$. By Theorem 3.8, there are integers s and t with

$$d = as + bt. \tag{3.3}$$

Because $d \mid c$, there is an integer e with $de = c$. Multiplying both sides of (3.3) by e, we have

$$c = de = (as + bt)e = a(se) + b(te).$$

Hence, one solution of the equation is given by $x = x_0$ and $y = y_0$, where $x_0 = se$ and $y_0 = te$.

To show that there are infinitely many solutions, let $x = x_0 + (b/d)n$ and $y = y_0 - (a/d)n$, where n is an integer. We will first show that any pair (x, y), with $x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$, where n is an integer, is a solution; then we will show that every solution must have this form. We see that this pair (x, y) is a solution, because

$$ax + by = ax_0 + a(b/d)n + by_0 - b(a/d)n = ax_0 + by_0 = c.$$

We now show that every solution of the equation $ax + by = c$ must be of the form described in the theorem. Suppose that x and y are integers with $ax + by = c$. Because

$$ax_0 + by_0 = c,$$

by subtraction we find that

$$(ax + by) - (ax_0 + by_0) = 0,$$

which implies that

$$a(x - x_0) + b(y - y_0) = 0.$$

Hence,

$$a(x - x_0) = b(y_0 - y).$$

Dividing both sides of this last equation by d, we see that

$$(a/d)(x - x_0) = (b/d)(y_0 - y).$$

By Theorem 3.6, we know that $(a/d, b/d) = 1$. Using Lemma 3.4, it follows that $(a/d) \mid (y_0 - y)$. Hence, there is an integer n with $(a/d)n = y_0 - y$; this means that $y = y_0 - (a/d)n$. Now, putting this value of y into the equation $a(x - x_0) = b(y_0 - y)$, we find that $a(x - x_0) = b(a/d)n$, which implies that $x = x_0 + (b/d)n$. ■

The following examples illustrate the use of Theorem 3.23.

Example 3.27. By Theorem 3.23, there are no integral solutions of the diophantine equation $15x + 6y = 7$, because $(15, 6) = 3$ but $3 \nmid 7$. ◀

BRAHMAGUPTA (598–670), thought to have been born in Ujjain, India, became the head of the astronomical observatory there; this observatory was the center of Indian mathematical studies at that time. Brahmagupta wrote two important books on mathematics and astronomy, *Brahma-sphuta-siddhanta* ("The Opening of the Universe") and *Khandakhadyaka,* written in 628 and 665, respectively. He developed many interesting formulas and theorems in planar geometry, and studied arithmetic progressions and quadratic equations. Brahmagupta developed new algebraic notation, and his understanding of the number system was advanced for his time. He is considered to be the first person to describe a general solution of linear diophantine equations. In astronomy, he studied eclipses, positions of the planets, and the length of the year.

Example 3.28. By Theorem 3.23, there are infinitely many solutions of the diophantine equation $21x + 14y = 70$, because $(21, 14) = 7$ and $7 \mid 70$. To find these solutions, note that by the Euclidean algorithm, $1 \cdot 21 + (-1) \cdot 14 = 7$, so that $10 \cdot 21 + (-10) \cdot 14 = 70$. Hence, $x_0 = 10$, $y_0 = -10$ is a particular solution. All solutions are given by $x = 10 + 2n$, $y = -10 - 3n$, where n is an integer. ◀

We will now use Theorem 3.23 to solve the two problems described at the beginning of the section.

Example 3.29. Consider the problem of forming 83 cents in postage using only 6- and 15-cent stamps. If x denotes the number of 6-cent stamps and y denotes the number of 15-cent stamps, we have $6x + 15y = 83$. Because $(6, 15) = 3$ does not divide 83, by Theorem 3.23 we know that there are no integral solutions. Hence, no combination of 6- and 15-cent stamps gives the correct postage. ◀

Example 3.30. Consider the problem of purchasing \$510 of travelers' checks, using only \$20 and \$50 checks. How many of each type of check should be used?

Let x be the number of \$20 checks and let y be the number of \$50 checks. We have the equation $20x + 50y = 510$. Note that the greatest common divisor of 20 and 50 is $(20, 50) = 10$. Because $10 \mid 510$, there are infinitely many integral solutions of this linear diophantine equation. Using the Euclidean algorithm, we find that $20(-2) + 50 = 10$. Multiplying both sides by 51, we obtain $20(-102) + 50(51) = 510$. Hence, a particular solution is given by $x_0 = -102$ and $y_0 = 51$. Theorem 3.23 tells us that all integral solutions are of the form $x = -102 + 5n$ and $y = 51 - 2n$. Because we want both x and y to be nonnegative, we must have $-102 + 5n \geq 0$ and $51 - 2n \geq 0$; thus, $n \geq 20\ 2/5$ and $n \leq 25\ 1/2$. Because n is an integer, it follows that $n = 21,\ 22,\ 23,\ 24$, or 25. Hence, we have the following five solutions: $(x, y) = (3, 9)$, $(8, 7)$, $(13, 5)$, $(18, 3)$, and $(23, 1)$. So the teller can give the customer 3 \$20 checks and 9 \$50 checks, 8 \$20 checks and 7 \$50 checks, 13 \$20 checks and 5 \$50 checks, 18 \$20 checks and 3 \$50 checks, or 23 \$20 checks and 1 \$50 check. ◀

We can extend Theorem 3.23 to cover linear diophantine equations with more than two variables, as the following theorem demonstrates.

Theorem 3.24. If $a_1, a_2, \ldots, a_n$ are nonzero integers, then the equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ has an integral solution if and only if $d = (a_1, a_2, \ldots, a_n)$ divides c. Furthermore, when there is a solution, there are infinitely many solutions.

Proof. If there are integers $x_1, x_2, \ldots, x_n$ such that $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, then because d divides a_i for $i = 1, 2, \ldots, n$, by Theorem 1.9, d also divides c. Hence, if $d \nmid c$ there are no integral solutions of the equation.

We will use mathematical induction to prove that there are infinitely many integral solutions when $d \mid c$. Note that by Theorem 3.23 this is true when $n = 2$.

Now, suppose that there are infinitely many solutions for all equations in n variables satisfying the hypotheses. By Theorem 3.9, the set of linear combinations $a_nx_n +$

$a_{n+1}x_{n+1}$ is the same as the set of multiples of (a_n, a_{n+1}). Hence, for every integer y there are infinitely many solutions of the linear diophantine equation $a_n x_n + a_{n+1}x_{n+1} = (a_n, a_{n+1})y$. It follows that the original equation in $n + 1$ variables can be reduced to a linear diophantine equation in n variables:

$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + (a_n, a_{n+1})y = c.$$

Note that c is divisible by $(a_1, a_2, \ldots, a_{n-1}, (a_n, a_{n+1}))$ because, by Lemma 3.2, this greatest common divisor equals $(a_1, a_2, \ldots, a_n, a_{n+1})$. By the inductive hypothesis, this equation has infinitely many integer solutions, as it is a linear diophantine equation in n variables where the greatest common divisor of the coefficients divides the constant c. It follows that there are infinitely many solutions to the original equation. ■

A method for solving linear diophantine equations in more than two variables can be found using the reduction in the proof of Theorem 3.24. We leave an application of Theorem 3.24 to the exercises.

3.7 Exercises

1. For each of the following linear diophantine equations, either find all solutions or show that there are no integral solutions.
   a) $2x + 5y = 11$ c) $21x + 14y = 147$ e) $1402x + 1969y = 1$
   b) $17x + 13y = 100$ d) $60x + 18y = 97$
2. For each of the following linear diophantine equations, either find all solutions or show that there are no integral solutions.
   a) $3x + 4y = 7$ c) $30x + 47y = -11$ e) $102x + 1001y = 1$
   b) $12x + 18y = 50$ d) $25x + 95y = 970$
3. Japanese businessman returning home from a trip to North America exchanges his U.S. and Canadian dollars for yen. If he received 9,763 yen, and received 99 yen for each U.S. and 86 yen for each Canadian dollar, how many of each type of currency did he exchange?
4. A student returning from Europe changes her euros and Swiss francs into U.S. money. If she received \$46.58 and received \$1.39 for each euro and 91¢ for each Swiss franc, how much of each type of currency did she exchange?
5. A professor returning home from conferences in Paris and London changes his euros and pounds into U.S. money. If he received \$125.78 and received \$1.31 for each euro and \$1.61 for each pound, how much of each type of currency did he exchange?
6. The Indian astronomer and mathematician Mahavira, who lived in the ninth century, posed this puzzle: A band of 23 weary travelers entered a lush forest where they found 63 piles each containing the same number of plantains and a remaining pile containing seven plantains. They divided the plantains equally. How many plantains were in each of the 63 piles? Solve this puzzle.
7. A grocer orders apples and oranges at a total cost of \$8.39. If apples cost him 25¢ each and oranges cost him 18¢ each, how many of each type of fruit did he order?
8. A shopper spends a total of \$5.49 for oranges, which cost 18¢ each, and grapefruit, which cost 33¢ each. What is the minimum number of pieces of fruit the shopper could have bought?