

50. Show that if  $a$ ,  $b$ , and  $m$  are integers such that  $m \geq 2$  and  $a \equiv b \pmod{m}$ , then  $\gcd(a, m) = \gcd(b, m)$ .
- \*51. Prove or disprove that  $n^2 - 79n + 1601$  is prime whenever  $n$  is a positive integer.
52. Prove or disprove that  $p_1 p_2 \cdots p_n + 1$  is prime for every positive integer  $n$ , where  $p_1, p_2, \dots, p_n$  are the  $n$  smallest prime numbers.
53. Show that there is a composite integer in every arithmetic progression  $ak + b$ ,  $k = 1, 2, \dots$  where  $a$  and  $b$  are positive integers.
54. Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form  $3k + 2$ , where  $k$  is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes  $q_1, q_2, \dots, q_n$ , and consider the number  $3q_1 q_2 \cdots q_n - 1$ .]
55. Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form  $4k + 3$ , where  $k$  is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes  $q_1, q_2, \dots, q_n$ , and consider the number  $4q_1 q_2 \cdots q_n - 1$ .]
- \*56. Prove that the set of positive rational numbers is countable by setting up a function that assigns to a rational number  $p/q$  with  $\gcd(p, q) = 1$  the base 11 number formed by the decimal representation of  $p$  followed by the base 11 digit A, which corresponds to the decimal number 10, followed by the decimal representation of  $q$ .
- \*57. Prove that the set of positive rational numbers is countable by showing that the function  $K$  is a one-to-one correspondence between the set of positive rational numbers and the set of positive integers if  $K(m/n) = p_1^{2a_1} p_2^{2a_2} \cdots p_s^{2a_s} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_t^{2b_t-1}$ , where  $\gcd(m, n) = 1$  and the prime-power factorizations of  $m$  and  $n$  are  $m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$  and  $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$ .

## 4.4 Solving Congruences

### Introduction

Solving linear congruences, which have the form  $ax \equiv b \pmod{m}$ , is an essential task in the study of number theory and its applications, just as solving linear equations plays an important role in calculus and linear algebra. To solve linear congruences, we employ inverses modulo  $m$ . We explain how to work backwards through the steps of the Euclidean algorithm to find inverses modulo  $m$ . Once we have found an inverse of  $a$  modulo  $m$ , we solve the congruence  $ax \equiv b \pmod{m}$  by multiplying both sides of the congruence by this inverse.

Simultaneous systems of linear congruence have been studied since ancient times. For example, the Chinese mathematician Sun-Tsu studied them in the first century. We will show how to solve systems of linear congruences modulo pairwise relatively prime moduli. The result we will prove is called the Chinese remainder theorem, and our proof will give a method to find all solutions of such systems of congruences. We will also show how to use the Chinese remainder theorem as a basis for performing arithmetic with large integers.

We will introduce a useful result of Fermat, known as Fermat's little theorem, which states that if  $p$  is prime and  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ . We will examine the converse of this statement, which will lead us to the concept of a pseudoprime. A pseudoprime  $m$  to the base  $a$  is a composite integer  $m$  that masquerades as a prime by satisfying the congruence  $a^{m-1} \equiv 1 \pmod{m}$ . We will also give an example of a Carmichael number, which is a composite integer that is a pseudoprime to all bases  $a$  relatively prime to it.

We also introduce the notion of discrete logarithms, which are analogous to ordinary logarithms. To define discrete logarithms we must first define primitive roots. A primitive root of a prime  $p$  is an integer  $r$  such that every integer not divisible by  $p$  is congruent to a power of  $r$  modulo  $p$ . If  $r$  is a primitive root of  $p$  and  $r^e \equiv a \pmod{p}$ , then  $e$  is the discrete logarithm of  $a$  modulo  $p$  to the base  $r$ . Finding discrete logarithms turns out to be an extremely difficult problem in general. The difficulty of this problem is the basis for the security of many cryptographic systems.

## Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

where  $m$  is a positive integer,  $a$  and  $b$  are integers, and  $x$  is a variable, is called a **linear congruence**. Such congruences arise throughout number theory and its applications.

How can we solve the linear congruence  $ax \equiv b \pmod{m}$ , that is, how can we find all integers  $x$  that satisfy this congruence? One method that we will describe uses an integer  $\bar{a}$  such that  $\bar{a}a \equiv 1 \pmod{m}$ , if such an integer exists. Such an integer  $\bar{a}$  is said to be an **inverse** of  $a$  modulo  $m$ . Theorem 1 guarantees that an inverse of  $a$  modulo  $m$  exists whenever  $a$  and  $m$  are relatively prime.

### THEOREM 1

If  $a$  and  $m$  are relatively prime integers and  $m > 1$ , then an inverse of  $a$  modulo  $m$  exists. Furthermore, this inverse is unique modulo  $m$ . (That is, there is a unique positive integer  $\bar{a}$  less than  $m$  that is an inverse of  $a$  modulo  $m$  and every other inverse of  $a$  modulo  $m$  is congruent to  $\bar{a}$  modulo  $m$ .)

**Proof:** By Theorem 6 of Section 4.3, because  $\gcd(a, m) = 1$ , there are integers  $s$  and  $t$  such that


$$sa + tm = 1.$$

This implies that

$$sa + tm \equiv 1 \pmod{m}.$$

Because  $tm \equiv 0 \pmod{m}$ , it follows that

$$sa \equiv 1 \pmod{m}.$$

Consequently,  $s$  is an inverse of  $a$  modulo  $m$ . That this inverse is unique modulo  $m$  is left as Exercise 7. 

Using inspection to find an inverse of  $a$  modulo  $m$  is easy when  $m$  is small. To find this inverse, we look for a multiple of  $a$  that exceeds a multiple of  $m$  by 1. For example, to find an inverse of 3 modulo 7, we can find  $j \cdot 3$  for  $j = 1, 2, \dots, 6$ , stopping when we find a multiple of 3 that is one more than a multiple of 7. We can speed this approach up if we note that  $2 \cdot 3 \equiv -1 \pmod{7}$ . This means that  $(-2) \cdot 3 \equiv 1 \pmod{7}$ . Hence,  $5 \cdot 3 \equiv 1 \pmod{7}$ , so 5 is an inverse of 3 modulo 7.

We can design a more efficient algorithm than brute force to find an inverse of  $a$  modulo  $m$  when  $\gcd(a, m) = 1$  using the steps of the Euclidean algorithm. By reversing these steps as in Example 17 of Section 4.3, we can find a linear combination  $sa + tm = 1$  where  $s$  and  $t$  are integers. Reducing both sides of this equation modulo  $m$  tells us that  $s$  is an inverse of  $a$  modulo  $m$ . We illustrate this procedure in Example 1.


**EXAMPLE 1** Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7. (Note that we have already shown that 5 is an inverse of 3 modulo 7 by inspection.)

*Solution:* Because  $\gcd(3, 7) = 1$ , Theorem 1 tells us that an inverse of 3 modulo 7 exists. The Euclidean algorithm ends quickly when used to find the greatest common divisor of 3 and 7:

$$7 = 2 \cdot 3 + 1.$$

From this equation we see that

$$-2 \cdot 3 + 1 \cdot 7 = 1.$$

This shows that  $-2$  and  $1$  are Bézout coefficients of 3 and 7. We see that  $-2$  is an inverse of 3 modulo 7. Note that every integer congruent to  $-2$  modulo 7 is also an inverse of 3, such as 5,  $-9$ , 12, and so on. 

**EXAMPLE 2** Find an inverse of 101 modulo 4620.

*Solution:* For completeness, we present all steps used to compute an inverse of 101 modulo 4620. (Only the last step goes beyond methods developed in Section 4.3 and illustrated in Example 17 in that section.) First, we use the Euclidean algorithm to show that  $\gcd(101, 4620) = 1$ . Then we will reverse the steps to find Bézout coefficients  $a$  and  $b$  such that  $101a + 4620b = 1$ . It will then follow that  $a$  is an inverse of 101 modulo 4620. The steps used by the Euclidean algorithm to find  $\gcd(101, 4620)$  are

$$4620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1.$$

Because the last nonzero remainder is 1, we know that  $\gcd(101, 4620) = 1$ . We can now find the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing  $\gcd(101, 4620) = 1$  in terms of each successive pair of remainders. In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend. We obtain

$$1 = 3 - 1 \cdot 2$$


$$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$$

$$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101.$$

That  $-35 \cdot 4620 + 1601 \cdot 101 = 1$  tells us that  $-35$  and  $1601$  are Bézout coefficients of 4620 and 101, and 1601 is an inverse of 101 modulo 4620. 

Once we have an inverse  $\bar{a}$  of  $a$  modulo  $m$ , we can solve the congruence  $ax \equiv b \pmod{m}$  by multiplying both sides of the linear congruence by  $\bar{a}$ , as Example 3 illustrates.

**EXAMPLE 3** What are the solutions of the linear congruence  $3x \equiv 4 \pmod{7}$ ?


**Solution:** By Example 1 we know that  $-2$  is an inverse of  $3$  modulo  $7$ . Multiplying both sides of the congruence by  $-2$  shows that

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because  $-6 \equiv 1 \pmod{7}$  and  $-8 \equiv 6 \pmod{7}$ , it follows that if  $x$  is a solution, then  $x \equiv -8 \equiv 6 \pmod{7}$ .

We need to determine whether every  $x$  with  $x \equiv 6 \pmod{7}$  is a solution. Assume that  $x \equiv 6 \pmod{7}$ . Then, by Theorem 5 of Section 4.1, it follows that

$$3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7},$$

which shows that all such  $x$  satisfy the congruence. We conclude that the solutions to the congruence are the integers  $x$  such that  $x \equiv 6 \pmod{7}$ , namely,  $6, 13, 20, \dots$  and  $-1, -8, -15, \dots$  

## The Chinese Remainder Theorem

Systems of linear congruences arise in many contexts. For example, as we will see later, they are the basis for a method that can be used to perform arithmetic with large integers. Such systems can even be found as word puzzles in the writings of ancient Chinese and Hindu mathematicians, such as that given in Example 4.



**EXAMPLE 4** In the first century, the Chinese mathematician Sun-Tsu asked:

There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$$\begin{aligned}x &\equiv 2 \pmod{3}, \\x &\equiv 3 \pmod{5}, \\x &\equiv 2 \pmod{7}?\end{aligned}$$

We will solve this system, and with it Sun-Tsu's puzzle, later in this section. 

The *Chinese remainder theorem*, named after the Chinese heritage of problems involving systems of linear congruences, states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

**THEOREM 2 THE CHINESE REMAINDER THEOREM** Let  $m_1, m_2, \dots, m_n$  be pairwise relatively prime positive integers greater than one and  $a_1, a_2, \dots, a_n$  arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo  $m = m_1 m_2 \cdots m_n$ . (That is, there is a solution  $x$  with  $0 \leq x < m$ , and all other solutions are congruent modulo  $m$  to this solution.)

**Proof:** To establish this theorem, we need to show that a solution exists and that it is unique modulo  $m$ . We will show that a solution exists by describing a way to construct this solution; showing that the solution is unique modulo  $m$  is Exercise 30.

To construct a simultaneous solution, first let

$$M_k = m/m_k$$

for  $k = 1, 2, \dots, n$ . That is,  $M_k$  is the product of the moduli except for  $m_k$ . Because  $m_i$  and  $m_k$  have no common factors greater than 1 when  $i \neq k$ , it follows that  $\gcd(m_k, M_k) = 1$ . Consequently, by Theorem 1, we know that there is an integer  $y_k$ , an inverse of  $M_k$  modulo  $m_k$ , such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

We will now show that  $x$  is a simultaneous solution. First, note that because  $M_j \equiv 0 \pmod{m_k}$  whenever  $j \neq k$ , all terms except the  $k$ th term in this sum are congruent to 0 modulo  $m_k$ . Because  $M_k y_k \equiv 1 \pmod{m_k}$  we see that

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k},$$

for  $k = 1, 2, \dots, n$ . We have shown that  $x$  is a simultaneous solution to the  $n$  congruences.  $\triangleleft$

Example 5 illustrates how to use the construction given in our proof of the Chinese remainder theorem to solve a system of congruences. We will solve the system given in Example 4, arising in Sun-Tsu's puzzle.

**EXAMPLE 5** To solve the system of congruences in Example 4, first let  $m = 3 \cdot 5 \cdot 7 = 105$ ,  $M_1 = m/3 = 35$ ,  $M_2 = m/5 = 21$ , and  $M_3 = m/7 = 15$ . We see that 2 is an inverse of  $M_1 = 35$  modulo 3, because  $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$ ; 1 is an inverse of  $M_2 = 21$  modulo 5, because  $21 \equiv 1 \pmod{5}$ ; and 1 is an inverse of  $M_3 = 15$  modulo 7, because  $15 \equiv 1 \pmod{7}$ . The solutions to this system are those  $x$  such that

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233 \equiv 23 \pmod{105}. \end{aligned}$$

It follows that 23 is the smallest positive integer that is a simultaneous solution. We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7. ◀

Although the construction in Theorem 2 provides a general method for solving systems of linear congruences with pairwise relatively prime moduli, it can be easier to solve a system using a different method. Example 6 illustrates the use of a method known as **back substitution**.

**EXAMPLE 6** Use the method of back substitution to find all integers  $x$  such that  $x \equiv 1 \pmod{5}$ ,  $x \equiv 2 \pmod{6}$ , and  $x \equiv 3 \pmod{7}$ .

**Solution:** By Theorem 4 in Section 4.1, the first congruence can be rewritten as an equality,  $x = 5t + 1$  where  $t$  is an integer. Substituting this expression for  $x$  into the second congruence tells us that

$$5t + 1 \equiv 2 \pmod{6},$$

which can be easily solved to show that  $t \equiv 5 \pmod{6}$  (as the reader should verify). Using Theorem 4 in Section 4.1 again, we see that  $t = 6u + 5$  where  $u$  is an integer. Substituting this expression for  $t$  back into the equation  $x = 5t + 1$  tells us that  $x = 5(6u + 5) + 1 = 30u + 26$ . We insert this into the third equation to obtain

$$30u + 26 \equiv 3 \pmod{7}.$$

Solving this congruence tells us that  $u \equiv 6 \pmod{7}$  (as the reader should verify). Hence, Theorem 4 in Section 4.1 tells us that  $u = 7v + 6$  where  $v$  is an integer. Substituting this expression for  $u$  into the equation  $x = 30u + 26$  tells us that  $x = 30(7v + 6) + 26 = 210v + 206$ . Translating this back into a congruence, we find the solution to the simultaneous congruences,

$$x \equiv 206 \pmod{210}. \quad \blacktriangleleft$$

## Computer Arithmetic with Large Integers

Suppose that  $m_1, m_2, \dots, m_n$  are pairwise relatively prime moduli and let  $m$  be their product. By the Chinese remainder theorem, we can show (see Exercise 28) that an integer  $a$  with  $0 \leq a < m$  can be uniquely represented by the  $n$ -tuple consisting of its remainders upon division by  $m_i$ ,  $i = 1, 2, \dots, n$ . That is, we can uniquely represent  $a$  by

$$(a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n).$$

**EXAMPLE 7** What are the pairs used to represent the nonnegative integers less than 12 when they are represented by the ordered pair where the first component is the remainder of the integer upon division by 3 and the second component is the remainder of the integer upon division by 4?

**Solution:** We have the following representations, obtained by finding the remainder of each integer when it is divided by 3 and by 4:

$$\begin{array}{lll} 0 = (0, 0) & 4 = (1, 0) & 8 = (2, 0) \\ 1 = (1, 1) & 5 = (2, 1) & 9 = (0, 1) \\ 2 = (2, 2) & 6 = (0, 2) & 10 = (1, 2) \\ 3 = (0, 3) & 7 = (1, 3) & 11 = (2, 3). \end{array} \quad \blacktriangleleft$$

To perform arithmetic with large integers, we select moduli  $m_1, m_2, \dots, m_n$ , where each  $m_i$  is an integer greater than 2,  $\gcd(m_i, m_j) = 1$  whenever  $i \neq j$ , and  $m = m_1 m_2 \cdots m_n$  is greater than the results of the arithmetic operations we want to carry out.

Once we have selected our moduli, we carry out arithmetic operations with large integers by performing componentwise operations on the  $n$ -tuples representing these integers using their remainders upon division by  $m_i, i = 1, 2, \dots, n$ . Once we have computed the value of each component in the result, we recover its value by solving a system of  $n$  congruences modulo  $m_i, i = 1, 2, \dots, n$ . This method of performing arithmetic with large integers has several valuable features. First, it can be used to perform arithmetic with integers larger than can ordinarily be carried out on a computer. Second, computations with respect to the different moduli can be done in parallel, speeding up the arithmetic.

**EXAMPLE 8** Suppose that performing arithmetic with integers less than 100 on a certain processor is much quicker than doing arithmetic with larger integers. We can restrict almost all our computations to integers less than 100 if we represent integers using their remainders modulo pairwise relatively prime integers less than 100. For example, we can use the moduli of 99, 98, 97, and 95. (These integers are relatively prime pairwise, because no two have a common factor greater than 1.)


By the Chinese remainder theorem, every nonnegative integer less than  $99 \cdot 98 \cdot 97 \cdot 95 = 89,403,930$  can be represented uniquely by its remainders when divided by these four moduli. For example, we represent 123,684 as  $(33, 8, 9, 89)$ , because  $123,684 \bmod 99 = 33$ ;  $123,684 \bmod 98 = 8$ ;  $123,684 \bmod 97 = 9$ ; and  $123,684 \bmod 95 = 89$ . Similarly, we represent 413,456 as  $(32, 92, 42, 16)$ .

To find the sum of 123,684 and 413,456, we work with these 4-tuples instead of these two integers directly. We add the 4-tuples componentwise and reduce each component with respect to the appropriate modulus. This yields

$$\begin{aligned} (33, 8, 9, 89) + (32, 92, 42, 16) \\ &= (65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95) \\ &= (65, 2, 51, 10). \end{aligned}$$

To find the sum, that is, the integer represented by  $(65, 2, 51, 10)$ , we need to solve the system of congruences

$$\begin{aligned} x &\equiv 65 \pmod{99}, \\ x &\equiv 2 \pmod{98}, \\ x &\equiv 51 \pmod{97}, \\ x &\equiv 10 \pmod{95}. \end{aligned}$$

It can be shown (see Exercise 53) that 537,140 is the unique nonnegative solution of this system less than 89,403,930. Consequently, 537,140 is the sum. Note that it is only when we have to recover the integer represented by  $(65, 2, 51, 10)$  that we have to do arithmetic with integers larger than 100. 

Particularly good choices for moduli for arithmetic with large integers are sets of integers of the form  $2^k - 1$ , where  $k$  is a positive integer, because it is easy to do binary arithmetic modulo such integers, and because it is easy to find sets of such integers that are pairwise relatively prime. [The second reason is a consequence of the fact that  $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$ , as Exercise 37 in Section 4.3 shows.] Suppose, for instance, that we can do arithmetic with integers less than  $2^{35}$  easily on our computer, but that working with larger integers requires special procedures. We can use pairwise relatively prime moduli less than  $2^{35}$  to perform arithmetic with integers as large as their product. For example, as Exercise 38 in Section 4.3 shows, the integers  $2^{35} - 1$ ,  $2^{34} - 1$ ,  $2^{33} - 1$ ,  $2^{31} - 1$ ,  $2^{29} - 1$ , and  $2^{23} - 1$  are pairwise relatively prime. Because the product of these six moduli exceeds  $2^{184}$ , we can perform arithmetic with integers as large as  $2^{184}$  (as long as the results do not exceed this number) by doing arithmetic modulo each of these six moduli, none of which exceeds  $2^{35}$ .

## Fermat's Little Theorem

The great French mathematician Pierre de Fermat made many important discoveries in number theory. One of the most useful of these states that  $p$  divides  $a^{p-1} - 1$  whenever  $p$  is prime and  $a$  is an integer not divisible by  $p$ . Fermat announced this result in a letter to one of his correspondents. However, he did not include a proof in the letter, stating that he feared the proof would be too long. Although Fermat never published a proof of this fact, there is little doubt that he knew how to prove it, unlike the result known as Fermat's last theorem. The first published proof is credited to Leonhard Euler. We now state this theorem in terms of congruences.

**THEOREM 3 FERMAT'S LITTLE THEOREM** If  $p$  is prime and  $a$  is an integer not divisible by  $p$ , then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer  $a$  we have

$$a^p \equiv a \pmod{p}.$$

**Remark:** Fermat's little theorem tells us that if  $a \in \mathbb{Z}_p$ , then  $a^{p-1} = 1$  in  $\mathbb{Z}_p$ .

The proof of Theorem 3 is outlined in Exercise 19.

Fermat's little theorem is extremely useful in computing the remainders modulo  $p$  of large powers of integers, as Example 9 illustrates.

**EXAMPLE 9** Find  $7^{222} \bmod 11$ .

**Solution:** We can use Fermat's little theorem to evaluate  $7^{222} \bmod 11$  rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that  $7^{10} \equiv 1 \pmod{11}$ , so  $(7^{10})^k \equiv 1 \pmod{11}$  for every positive integer  $k$ . To take advantage of this last congruence, we divide the exponent 222 by 10, finding that  $222 = 22 \cdot 10 + 2$ . We now see that

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

It follows that  $7^{222} \bmod 11 = 5$ . ◀

Example 9 illustrated how we can use Fermat's little theorem to compute  $a^n \bmod p$ , where  $p$  is prime and  $p \nmid a$ . First, we use the division algorithm to find the quotient  $q$  and remainder  $r$  when  $n$  is divided by  $p - 1$ , so that  $n = q(p - 1) + r$  where  $0 \leq r < p - 1$ . It follows that  $a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$ . Hence, to find  $a^n \bmod p$ , we only need to compute  $a^r \bmod p$ . We will take advantage of this simplification many times in our study of number theory.

## Pseudoprimes

In Section 4.2 we showed that an integer  $n$  is prime when it is not divisible by any prime  $p$  with  $p \leq \sqrt{n}$ . Unfortunately, using this criterion to show that a given integer is prime is inefficient. It requires that we find all primes not exceeding  $\sqrt{n}$  and that we carry out trial division by each such prime to see whether it divides  $n$ .



Are there more efficient ways to determine whether an integer is prime? According to some sources, ancient Chinese mathematicians believed that  $n$  was an odd prime if and only if

$$2^{n-1} \equiv 1 \pmod{n}.$$

If this were true, it would provide an efficient primality test. Why did they believe this congruence could be used to determine whether an integer  $n > 2$  is prime? First, they observed that the congruence holds whenever  $n$  is an odd prime. For example, 5 is prime and

$$2^{5-1} = 2^4 = 16 \equiv 1 \pmod{5}.$$

By Fermat's little theorem, we know that this observation was correct, that is,  $2^{n-1} \equiv 1 \pmod{n}$  whenever  $n$  is an odd prime. Second, they never found a composite integer  $n$  for which the congruence holds. However, the ancient Chinese were only partially correct. They were correct in thinking that the congruence holds whenever  $n$  is prime, but they were incorrect in concluding that  $n$  is necessarily prime if the congruence holds.

Unfortunately, there are composite integers  $n$  such that  $2^{n-1} \equiv 1 \pmod{n}$ . Such integers are called **pseudoprimes** to the base 2.

**EXAMPLE 10** The integer 341 is a pseudoprime to the base 2 because it is composite ( $341 = 11 \cdot 31$ ) and as Exercise 37 shows

$$2^{340} \equiv 1 \pmod{341}.$$

We can use an integer other than 2 as the base when we study pseudoprimes.

### DEFINITION 1

Let  $b$  be a positive integer. If  $n$  is a composite positive integer, and  $b^{n-1} \equiv 1 \pmod{n}$ , then  $n$  is called a *pseudoprime to the base  $b$* .

Given a positive integer  $n$ , determining whether  $2^{n-1} \equiv 1 \pmod{n}$  is a useful test that provides some evidence concerning whether  $n$  is prime. In particular, if  $n$  satisfies this congruence, then it is either prime or a pseudoprime to the base 2; if  $n$  does not satisfy this congruence, it is composite. We can perform similar tests using bases  $b$  other than 2 and obtain more evidence as to whether  $n$  is prime. If  $n$  passes all such tests, it is either prime or a pseudoprime to all the bases  $b$  we have chosen. Furthermore, among the positive integers not exceeding  $x$ , where  $x$  is a positive real number, compared to primes there are relatively few pseudoprimes to the base  $b$ , where  $b$  is a positive integer. For example, among the positive integers less than  $10^{10}$  there are 455,052,512 primes, but only 14,884 pseudoprimes to the base 2. Unfortunately, we



**PIERRE DE FERMAT (1601–1665)** Pierre de Fermat, one of the most important mathematicians of the seventeenth century, was a lawyer by profession. He is the most famous amateur mathematician in history. Fermat published little of his mathematical discoveries. It is through his correspondence with other mathematicians that we know of his work. Fermat was one of the inventors of analytic geometry and developed some of the fundamental ideas of calculus. Fermat, along with Pascal, gave probability theory a mathematical basis. Fermat formulated what was the most famous unsolved problem in mathematics. He asserted that the equation  $x^n + y^n = z^n$  has no nontrivial positive integer solutions when  $n$  is an integer greater than 2. For more than 300 years, no proof (or counterexample) was found. In his copy of the works of the ancient Greek mathematician Diophantus, Fermat wrote that he had a proof but that it would not fit in the margin. Because the first proof,

found by Andrew Wiles in 1994, relies on sophisticated, modern mathematics, most people think that Fermat thought he had a proof, but that the proof was incorrect. However, he may have been tempting others to look for a proof, not being able to find one himself.

cannot distinguish between primes and pseudoprimes just by choosing sufficiently many bases, because there are composite integers  $n$  that pass all tests with bases  $b$  such that  $\gcd(b, n) = 1$ . This leads to Definition 2.

**DEFINITION 2**

A composite integer  $n$  that satisfies the congruence  $b^{n-1} \equiv 1 \pmod{n}$  for all positive integers  $b$  with  $\gcd(b, n) = 1$  is called a *Carmichael number*. (These numbers are named after Robert Carmichael, who studied them in the early twentieth century.)

**EXAMPLE 11**

The integer 561 is a Carmichael number. To see this, first note that 561 is composite because  $561 = 3 \cdot 11 \cdot 17$ . Next, note that if  $\gcd(b, 561) = 1$ , then  $\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$ .

Using Fermat's little theorem we find that

$$b^2 \equiv 1 \pmod{3}, b^{10} \equiv 1 \pmod{11}, \text{ and } b^{16} \equiv 1 \pmod{17}.$$

It follows that

$$b^{560} = (b^2)^{280} \equiv 1 \pmod{3},$$

$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$

$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

By Exercise 29, it follows that  $b^{560} \equiv 1 \pmod{561}$  for all positive integers  $b$  with  $\gcd(b, 561) = 1$ . Hence 561 is a Carmichael number. 

Although there are infinitely many Carmichael numbers, more delicate tests, described in the exercise set, can be devised that can be used as the basis for efficient probabilistic primality tests. Such tests can be used to quickly show that it is almost certainly the case that a given integer is prime. More precisely, if an integer is not prime, then the probability that it passes a series of tests is close to 0. We will describe such a test in Chapter 7 and discuss the notions from probability theory that this test relies on. These probabilistic primality tests can be used, and are used, to find large primes extremely rapidly on computers.

## Primitive Roots and Discrete Logarithms

In the set of positive real numbers, if  $b > 1$ , and  $x = b^y$ , we say that  $y$  is the logarithm of  $x$  to the base  $b$ . Here, we will show that we can also define the concept of logarithms modulo  $p$  of positive integers where  $p$  is a prime. Before we do so, we need a definition.

**DEFINITION 3**


A *primitive root* modulo a prime  $p$  is an integer  $r$  in  $\mathbf{Z}_p$  such that every nonzero element of  $\mathbf{Z}_p$  is a power of  $r$ .



**ROBERT DANIEL CARMICHAEL (1879–1967)** Robert Daniel Carmichael was born in Alabama. He received his undergraduate degree from Lineville College in 1898 and his Ph.D. in 1911 from Princeton. Carmichael held positions at Indiana University from 1911 until 1915 and at the University of Illinois from 1915 until 1947. Carmichael was an active researcher in a wide variety of areas, including number theory, real analysis, differential equations, mathematical physics, and group theory. His Ph.D. thesis, written under the direction of G. D. Birkhoff, is considered the first significant American contribution to the subject of differential equations.

**EXAMPLE 12** Determine whether 2 and 3 are primitive roots modulo 11.


*Solution:* When we compute the powers of 2 in  $\mathbf{Z}_{11}$ , we obtain  $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$ . Because every element of  $\mathbf{Z}_{11}$  is a power of 2, 2 is a primitive root of 11.

When we compute the powers of 3 modulo 11, we obtain  $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$ . We note that this pattern repeats when we compute higher powers of 3. Because not all elements of  $\mathbf{Z}_{11}$  are powers of 3, we conclude that 3 is not a primitive root of 11. 

An important fact in number theory is that there is a primitive root modulo  $p$  for every prime  $p$ . We refer the reader to [Ro10] for a proof of this fact. Suppose that  $p$  is prime and  $r$  is a primitive root modulo  $p$ . If  $a$  is an integer between 1 and  $p - 1$ , that is, an element of  $\mathbf{Z}_p$ , we know that there is a unique exponent  $e$  such that  $r^e = a$  in  $\mathbf{Z}_p$ , that is,  $r^e \bmod p = a$ .

**DEFINITION 4** Suppose that  $p$  is a prime,  $r$  is a primitive root modulo  $p$ , and  $a$  is an integer between 1 and  $p - 1$  inclusive. If  $r^e \bmod p = a$  and  $0 \leq e \leq p - 1$ , we say that  $e$  is the *discrete logarithm* of  $a$  modulo  $p$  to the base  $r$  and we write  $\log_r a = e$  (where the prime  $p$  is understood).


**EXAMPLE 13** Find the discrete logarithms of 3 and 5 modulo 11 to the base 2.

*Solution:* When we computed the powers of 2 modulo 11 in Example 12, we found that  $2^8 = 3$  and  $2^4 = 5$  in  $\mathbf{Z}_{11}$ . Hence, the discrete logarithms of 3 and 5 modulo 11 to the base 2 are 8 and 4, respectively. (These are the powers of 2 that equal 3 and 5, respectively, in  $\mathbf{Z}_{11}$ .) We write  $\log_2 3 = 8$  and  $\log_2 5 = 4$  (where the modulus 11 is understood and not explicitly noted in the notation). 

The discrete logarithm problem is hard!

The **discrete logarithm problem** takes as input a prime  $p$ , a primitive root  $r$  modulo  $p$ , and a positive integer  $a \in \mathbf{Z}_p$ ; its output is the discrete logarithm of  $a$  modulo  $p$  to the base  $r$ . Although this problem might seem not to be that difficult, it turns out that no polynomial time algorithm is known for solving it. The difficulty of this problem plays an important role in cryptography, as we will see in Section 4.6

## Exercises

1. Show that 15 is an inverse of 7 modulo 26.
-  2. Show that 937 is an inverse of 13 modulo 2436.
3. By inspection (as discussed prior to Example 1), find an inverse of 4 modulo 9.
4. By inspection (as discussed prior to Example 1), find an inverse of 2 modulo 17.
5. Find an inverse of  $a$  modulo  $m$  for each of these pairs of relatively prime integers using the method followed in Example 2.
  - a)  $a = 4, m = 9$
  - b)  $a = 19, m = 141$
  - c)  $a = 55, m = 89$
  - d)  $a = 89, m = 232$
6. Find an inverse of  $a$  modulo  $m$  for each of these pairs of relatively prime integers using the method followed in Example 2.
  - a)  $a = 2, m = 17$
  - b)  $a = 34, m = 89$
  - c)  $a = 144, m = 233$
  - d)  $a = 200, m = 1001$
- \*7. Show that if  $a$  and  $m$  are relatively prime positive integers, then the inverse of  $a$  modulo  $m$  is unique modulo  $m$ . [Hint: Assume that there are two solutions  $b$  and  $c$  of the congruence  $ax \equiv 1 \pmod{m}$ . Use Theorem 7 of Section 4.3 to show that  $b \equiv c \pmod{m}$ .]
8. Show that an inverse of  $a$  modulo  $m$ , where  $a$  is an integer and  $m > 2$  is a positive integer, does not exist if  $\gcd(a, m) > 1$ .
9. Solve the congruence  $4x \equiv 5 \pmod{9}$  using the inverse of 4 modulo 9 found in part (a) of Exercise 5.
10. Solve the congruence  $2x \equiv 7 \pmod{17}$  using the inverse of 2 modulo 7 found in part (a) of Exercise 6.
11. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 5.
  - a)  $19x \equiv 4 \pmod{141}$
  - b)  $55x \equiv 34 \pmod{89}$
  - c)  $89x \equiv 2 \pmod{232}$