in this position is used for positive integers, and a 1 bit in this position is used for negative integers, just as in one's complement expansions. For a positive integer, the remaining bits are identical to the binary expansion of the integer. For a negative integer, the remaining bits are the bits of the binary expansion of $2^{n-1} - |x|$. Two's complement expansions of integers are often used by computers because addition and subtraction of integers can be performed easily using these expansions, where these integers can be either positive or negative.

36. Answer Exercise 30, but this time find the two's complement expansion using bit strings of length six.

37. Answer Exercise 31 if each expansion is a two's complement expansion of length five.

38. Answer Exercise 32 for two's complement expansions.

39. Answer Exercise 33 for two's complement expansions.

40. Answer Exercise 34 for two's complement expansions.

41. Show that the integer m with two's complement representation $(a_{n-1}a_{n-2}\cdots a_1a_0)$ can be found using the equation $m = -a_{n-1}\cdot 2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_1\cdot 2 + a_0$.

42. Give a simple algorithm for forming the two's complement representation of an integer from its one's complement representation.

43. Sometimes integers are encoded by using four-digit binary expansions to represent each decimal digit. This produces the **binary coded decimal** form of the integer. For instance, 791 is encoded in this way by 011110010001. How many bits are required to represent a number with n decimal digits using this type of encoding?

A **Cantor expansion** is a sum of the form

$$a_n n! + a_{n-1}(n-1)! + \cdots + a_2 2! + a_1 1!,$$

where a_i is an integer with $0 \leq a_i \leq i$ for $i = 1, 2, \ldots, n$.

44. Find the Cantor expansions of

a) 2. **b)** 7. **c)** 19.
d) 87. **e)** 1000. **f)** 1,000,000.

***45.** Describe an algorithm that finds the Cantor expansion of an integer.

***46.** Describe an algorithm to add two integers from their Cantor expansions.

47. Add $(10111)_2$ and $(11010)_2$ by working through each step of the algorithm for addition given in the text.

48. Multiply $(1110)_2$ and $(1010)_2$ by working through each step of the algorithm for multiplication given in the text.

49. Describe an algorithm for finding the difference of two binary expansions.

50. Estimate the number of bit operations used to subtract two binary expansions.

51. Devise an algorithm that, given the binary expansions of the integers a and b, determines whether $a > b$, $a = b$, or $a < b$.

52. How many bit operations does the comparison algorithm from Exercise 51 use when the larger of a and b has n bits in its binary expansion?

53. Estimate the complexity of Algorithm 1 for finding the base b expansion of an integer n in terms of the number of divisions used.

***54.** Show that Algorithm 5 uses $O((\log m)^2 \log n)$ bit operations to find b^n **mod** m.

55. Show that Algorithm 4 uses $O(q \log |a|)$ bit operations, assuming that $a > d$.

2.6 Applications of Number Theory

INTRODUCTION

Number theory has many applications, especially to computer science. In Section 2.4 we described several of these applications, including hashing functions, the generation of pseudorandom numbers, and shift ciphers. This section continues our introduction to number theory, developing some key results and presenting two important applications: a method for performing arithmetic with large integers and a recently invented type of cryptosystem, called a *public key system*. In such a cryptosystem, we do not have to keep encryption keys secret, since knowledge of an encryption key does not help someone decrypt messages in a realistic amount of time. Privately held decryption keys are used to decrypt messages.

Before developing these applications, we will introduce some key results that play a central role in number theory and its applications. For example, we will show how to solve systems of linear congruences modulo pairwise relatively prime integers using the Chinese Remainder Theorem, and then show how to use this result as a basis for

performing arithmetic with large integers. We will introduce Fermat's Little Theorem and the concept of a pseudoprime and will show how to use these concepts to develop a public key cryptosystem.

SOME USEFUL RESULTS

An important result we will use throughout this section is that the greatest common divisor of two integers a and b can be expressed in the form

$$sa + tb,$$

where s and t are integers. In other words, $\gcd(a, b)$ can be expressed as a **linear combination** with integer coefficients of a and b. For example, $\gcd(6, 14) = 2$, and $2 = (-2) \cdot 6 + 1 \cdot 14$. We state this fact as Theorem 1.

THEOREM 1 If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

We will not give a formal proof of Theorem 1 here (see Exercise 66 in Section 3.3 and [Ro00] for proofs), but we will provide an example of a method for finding a linear combination of two integers equal to their greatest common divisor. (In this section, we will assume that a linear combination has integer coefficients.) The method proceeds by working backward through the divisions of the Euclidean algorithm. (We also describe an algorithm called the **extended Euclidean algorithm** that can be used to express $\gcd(a, b)$ as a linear combination of a and b in the preamble to Exercise 48.)

EXAMPLE 1 Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18.$$

Using the next-to-last division (the third division), we can express $\gcd(252, 198) = 18$ as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36.$$

The second division tells us that

$$36 = 198 - 3 \cdot 54.$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

The first division tells us that

$$54 = 252 - 1 \cdot 198.$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

completing the solution. ◀

We will use Theorem 1 to develop several useful results. One of our goals will be to prove the part of the Fundamental Theorem of Arithmetic asserting that a positive integer has at most one prime factorization. We will show that if a positive integer has a factorization into primes, where the primes are written in nondecreasing order, then this factorization is unique.

First, we need to develop some results about divisibility.

LEMMA 1 If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: Since $\gcd(a, b) = 1$, by Theorem 1 there are integers s and t such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by c, we obtain

$$sac + tbc = c.$$

Using Theorem 1 of Section 2.4, we can use this last equation to show that $a \mid c$. By part 2 of that theorem, $a \mid tbc$. Since $a \mid sac$ and $a \mid tbc$, by part 1 of that theorem, we conclude that a divides $sac + tbc$, and hence $a \mid c$. This finishes the proof. ◁

We will use the following generalization of Lemma 1 in the proof of uniqueness of prime factorizations. (The proof of Lemma 2 is left as an exercise in Section 3.3, since it can be most easily carried out using the method of mathematical induction, which will be covered in that section.)

LEMMA 2 If p is a prime and $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer, then $p \mid a_i$ for some i.

We can now show that a factorization of an integer into primes is unique. That is, we will show that every integer can be written as the product of primes in nondecreasing order in at most one way. This is part of the Fundamental Theorem of Arithmetic. We will prove the other part, that every integer has a factorization into primes, in Section 3.3.

Proof (of the uniqueness of the prime factorization of a positive integer): We will use a proof by contradiction. Suppose that the positive integer n can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, each p_i and q_j are primes such that $p_1 \le p_2 \le \cdots \le p_s$ and $q_1 \le q_2 \le \cdots \le q_t$.

When we remove all common primes from the two factorizations, we have

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

where no prime occurs on both sides of this equation and u and v are positive integers. By Lemma 1 it follows that p_{i_1} divides q_{j_k} for some k. Since no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of n into primes in nondecreasing order. ◁

Lemma 1 can also be used to prove a result about dividing both sides of a congruence by the same integer. We have shown (Theorem 10 in Section 2.4) that we can multiply both sides of a congruence by the same integer. However, dividing both sides of a congruence by an integer does not always produce a valid congruence, as Example 2 shows.

EXAMPLE 2 The congruence $14 \equiv 8 \pmod 6$ holds, but both sides of this congruence cannot be divided by 2 since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod 6$. ◀

However, using Lemma 1, we can show that we can divide both sides of a congruence by an integer relatively prime to the modulus. This is stated as Theorem 2.

THEOREM 2 Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod m$.

Proof: Since $ac \equiv bc \pmod m$, $m \mid ac - bc = c(a - b)$. By Lemma 1, since $\gcd(c, m) = 1$, it follows that $m \mid a - b$. We conclude that $a \equiv b \pmod m$. ◁

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, find all integers x that satisfy this congruence? One method that we will describe uses an integer $\overline{a}$ such that $\overline{a}a \equiv 1 \pmod m$, if such an integer exists. Such an integer $\overline{a}$ is said to be an **inverse** of a modulo m. Theorem 3 guarantees that an inverse of a modulo m exists whenever a and m are relatively prime.

THEOREM 3 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 $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

Proof: By Theorem 1, since $\gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

This implies that

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

Since $tm \equiv 0 \pmod{m}$, 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 9 at the end of this section. ◁

The proof of Theorem 3 describes a method for finding the inverse of a modulo m when a and m are relatively prime: find a linear combination of a and m that equals 1 (which can be done by working backward through the steps of the Euclidean algorithm); the coefficient of a in this linear combination is an inverse of a modulo m. We illustrate this procedure in Example 3.

EXAMPLE 3 Find an inverse of 3 modulo 7.

Solution: Since $\gcd(3, 7) = 1$, Theorem 3 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 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.) ◀

When we have an inverse $\overline{a}$ of a modulo m, we can easily solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides of the linear congruence by $\overline{a}$, as Example 4 illustrates.

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

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

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

Since $-6 \equiv 1 \pmod{7}$ 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 10 of Section 2.4, 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, ... and -1, -8, -15, ... ◀

THE CHINESE REMAINDER THEOREM

Links

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 5.

EXAMPLE 5 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

$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 5,$$
$$x \equiv 2 \pmod 7?$$

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 4

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers. The system

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

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 24 at the end of this section.

To construct a simultaneous solution, first let

$$M_k = m/m_k$$

for $k = 1, 2, \ldots, n$. That is, M_k is the product of the moduli except for m_k. Since 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 3, 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 since $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k. Since $M_k y_k \equiv 1 \pmod{m_k}$ we see that

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

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

The following example illustrates how to use the construction given in the proof of Theorem 4 to solve a system of congruences. We will solve the system given in Example 5, arising in Sun-Tsu's puzzle.

EXAMPLE 6 To solve the system of congruences in Example 5, 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, since $35 \equiv 2 \pmod 3$; 1 is an inverse of $M_2 = 21$ modulo 5, since $21 \equiv 1 \pmod 5$; and 1 is an inverse of $M_3 = 15 \pmod 7$, since $15 \equiv 1 \pmod 7$. 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. ◀

COMPUTER ARITHMETIC WITH LARGE INTEGERS

Suppose that $m_1, m_2, \ldots, m_n$ are pairwise relatively prime integers greater than or equal to 2 and let m be their product. By the Chinese Remainder Theorem, we can show (see Exercise 22) 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, $i = 1, 2, \ldots, n$. That is, we can uniquely represent a by

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

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:

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

◀

To perform arithmetic with large integers, we select moduli $m_1, m_2, \ldots, m_n$, 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 result 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, $i = 1, 2, \ldots, n$. 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, $i = 1, 2, \ldots, n$. 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, since 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), since 123,684 **mod** 99 = 33,123,684 **mod** 98 = 8; 123,684 **mod** 97 = 9; and 123,684 **mod** 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

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

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 39) 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, since it is easy to do binary arithmetic modulo such integers, and since 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 41 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 42 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. Since 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 for each of these six moduli, none of which exceeds 2^{35}.

PSEUDOPRIMES

In Section 2.4 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 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 is prime? First, they observed that the congruence holds whenever n is prime. For example, 5 is prime and

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

Second, they never found a composite integer n for which the congruence holds. 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.

The great French mathematician Fermat showed that the congruence holds when n is prime. He proved the following, more general result.

THEOREM 5

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

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

The proof of Theorem 5 is outlined in Exercise 17 at the end of this section.

Links

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 it was incorrect. However, he may have been tempting others to look for a proof, not being able to find one himself.

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 9 The integer 341 is a pseudoprime to the base 2 since it is composite ($341 = 11 \cdot 31$) and as Exercise 27 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 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, less than 10^{10} there are 455,052,512 primes, but only 14,884 pseudoprimes to the base 2. Unfortunately, we cannot distinguish between primes and pseudoprimes just by choosing sufficiently many bases, because there are composite integers n that pass all tests with bases with $\gcd(b, n) = 1$. 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 10 The integer 561 is a Carmichael number. To see this, first note that 561 is composite since $561 = 3 \cdot 11 \cdot 17$. 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

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

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.

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 23 at the end of this section, 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 at the end of this section, 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 5 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.

PUBLIC KEY CRYPTOGRAPHY

Links

In Section 2.4 we introduced methods for encrypting messages based on congruences. When these encryption methods are used, messages, which are strings of characters, are translated into numbers. Then the number for each character is transformed into another number, either using a shift or an affine transformation modulo 26. These methods are examples of **private key cryptosystems.** Knowing the encryption key lets you quickly find the decryption key. For example, when a shift cipher is used with encryption key k, a number p representing a letter is sent to

$$c = (p + k) \bmod 26.$$

Decryption is carried out by shifting by $-k$; that is,

$$p = (c - k) \bmod 26.$$

When a private key cryptosystem is used, a pair of people who wish to communicate in secret must have a separate key. Since anyone knowing this key can both encrypt and decrypt messages easily, these two people need to securely exchange the key.

In the mid-1970s, cryptologists introduced the concept of **public key cryptosystems.** When such cryptosystems are used, knowing how to send someone a message does not help you decrypt messages sent to this person. In such a system, every person can have a publicly known encryption key. Only the decryption keys are kept secret, and only the intended recipient of a message can decrypt it, since the encryption key does not let someone find the decryption key without an extraordinary amount of work (such as more than 2 billion years of computer time).

In 1976, three researchers at M.I.T.—Ronald Rivest, Adi Shamir, and Leonard Adleman—introduced a public key cryptosystem, known as the **RSA system,** from the initials of its inventors. The RSA cryptosystem is based on modular exponentiation modulo, the product of two large primes, which can be done rapidly using Algorithm 5 in Section 2.5. Each individual has an encryption key consisting of a modulus $n = pq$, where p and q are large primes, say, with 200 digits each, and an exponent e that is relatively prime to $(p - 1)(q - 1)$. To produce a usable key, two large primes must be found. This can be

done quickly on a computer using probabilistic primality tests, referred to earlier in this section. However, the product of these primes $n = pq$, with approximately 400 digits, cannot be factored in a reasonable length of time. As we will see, this is an important reason why decryption cannot be done quickly without a separate decryption key.

RSA ENCRYPTION

In the RSA encryption method, messages are translated into sequences of integers. This can be done by translating each letter into an integer, as is done with the Caesar cipher. These integers are grouped together to form larger integers, each representing a block of letters. The encryption proceeds by transforming the integer M, representing the plaintext (the original message), to an integer C, representing the ciphertext (the encrypted message), using the function

$$C = M^e \bmod n.$$

(To perform the encryption, we use an algorithm for fast modular exponentiation, such as Algorithm 5 in Section 2.5.) We leave the encrypted message as blocks of numbers and send these to the intended recipient.

Example 11 illustrates how RSA encryption is performed. For practical reasons we use small primes p and q in this example, rather than primes with 100 or more digits. Although the cipher described in this example is not secure, it does illustrate the techniques used in the RSA cipher.

EXAMPLE 11 Encrypt the message STOP using the RSA cryptosystem with $p = 43$ and $q = 59$, so that $n = 43 \cdot 59 = 2537$, and with $e = 13$. Note that

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1.$$

Links

RONALD RIVEST (BORN 1948) Ronald Rivest received a B.A. from Yale in 1969 and his Ph.D. in computer science from Stanford in 1974. Rivest is a computer science professor at M.I.T. and was a cofounder of RSA Data Security, which held the patent on the RSA cryptosystem that he invented together with Adi Shamir and Leonard Adleman. Areas that Rivest has worked in besides cryptography include machine learning, VLSI design, and computer algorithms. He is a coauthor of a popular text on algorithms ([CoLeRiSt01]).

ADI SHAMIR (BORN 1952) Adi Shamir was born in Tel Aviv, Israel. His undergraduate degree is from Tel Aviv University (1972) and his Ph.D. is from the Weizmann Institute of Science (1977). Shamir was a research assistant at the University of Warwick and an assistant professor at M.I.T. He is currently a professor in the Applied Mathematics Department at the Weizmann Institute and leads a group studying computer security. Shamir's contributions to cryptography, besides the RSA cryptosystem, include cracking knapsack cryptosystems, cryptanalysis of the Data Encryption Standard (DES), and the design of many cryptographic protocols.

LEONARD ADLEMAN (BORN 1945) Leonard Adleman was born in San Francisco, California. He received a B.S. in mathematics (1968) and his Ph.D. in computer science (1976) from the University of California, Berkeley. Adleman was a member of the mathematics faculty at M.I.T. from 1976 until 1980, where he was a co-inventor of the RSA cryptosystem, and in 1980 he took a position in the computer science department at the University of Southern California (USC). He was appointed to a chaired position at USC in 1985. Adleman has worked on computer security, computational complexity, immunology, and molecular biology. He invented the term "computer virus." Adleman's recent work on DNA computing has sparked great interest. He was a technical adviser for the movie *Sneakers*, in which computer security played an important role.

Solution: We translate the letters in STOP into their numerical equivalents and then group the numbers into blocks of four. We obtain

1819 1415.

We encrypt each block using the mapping

$$C = M^{13} \bmod 2537.$$

Computations using fast modular multiplication show that $1819^{13} \bmod 2537 = 2081$ and $1415^{13} \bmod 2537 = 2182$. The encrypted message is 2081 2182. ◀

RSA DECRYPTION

The plaintext message can be quickly recovered when the decryption key d, an inverse of e modulo $(p-1)(q-1)$, is known. [Such an inverse exists since $\gcd(e, (p-1)(q-1)) = 1$.] To see this, note that if $de \equiv 1 \pmod{(p-1)(q-1)}$, there is an integer k such that $de = 1 + k(p-1)(q-1)$. It follows that

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$

By Fermat's Little Theorem [assuming that $\gcd(M, p) = \gcd(M, q) = 1$, which holds except in rare cases], it follows that $M^{p-1} \equiv 1 \pmod{p}$ and $M^{q-1} \equiv 1 \pmod{q}$. Consequently,

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod{p}$$

and

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod{q}.$$

Since $\gcd(p, q) = 1$, it follows by the Chinese Remainder Theorem that

$$C^d \equiv M \pmod{pq}.$$

Example 12 illustrates how to decrypt messages sent using the RSA cryptosystem.

EXAMPLE 12 We receive the encrypted message 0981 0461. What is the decrypted message if it was encrypted using the RSA cipher from Example 11?

Solution: The message was encrypted using the RSA cryptosystem with $n = 43 \cdot 59$ and exponent 13. As Exercise 4 shows, $d = 937$ is an inverse of 13 modulo $42 \cdot 58 = 2436$. We use 937 as our decryption exponent. Consequently, to decrypt a block C, we compute

$$P = C^{937} \bmod 2537.$$

To decrypt the message, we use the fast modular exponentiation algorithm to compute $0981^{937} \bmod 2537 = 0704$ and $0461^{937} \bmod 2537 = 1115$. Consequently, the numerical version of the original message is 0704 1115. Translating this back to English letters, we see that the message is HELP. ◀

RSA AS A PUBLIC KEY SYSTEM

Links

Why is the RSA cryptosystem suitable for public key cryptography? When we know the factorization of the modulus n, that is, when we know p and q, we can use the Euclidean

algorithm to quickly find an exponent d inverse to e modulo $(p-1)(q-1)$. This lets us decrypt messages sent using our key. However, no method is known to decrypt messages that is not based on finding a factorization of n, or that does not also lead to the factorization of n. Factorization is believed to be a difficult problem, as opposed to finding large primes p and q, which can be done quickly. The most efficient factorization methods known (as of 2002) require billions of years to factor 400-digit integers. Consequently, when p and q are 200-digit primes, messages encrypted using $n = pq$ as the modulus cannot be found in a reasonable time unless the primes p and q are known.

Active research is under way to find new ways to efficiently factor integers. Integers that were thought, as recently as several years ago, to be far too large to be factored in a reasonable amount of time can now be factored routinely. Integers with more than 100 digits, as well as some with more than 150 digits, have been factored using team efforts. When new factorization techniques are found, it will be necessary to use larger primes to ensure secrecy of messages. Unfortunately, messages that were considered secure earlier can be saved and subsequently decrypted by unintended recipients when it becomes feasible to factor the $n = pq$ in the key used for RSA encryption.

The RSA method is now widely used. However, the most commonly used cryptosystems are private key cryptosystems. The use of public key cryptography, via the RSA system, is growing. However, there are applications that use both private key and public key systems. For example, a public key cryptosystem, such as RSA, can be used to distribute private keys to pairs of individuals when they wish to communicate. These people then use a private key system for encryption and decryption of messages.

Exercises

1. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 10, 11 **b)** 21, 44 **c)** 36, 48
d) 34, 55 **e)** 117, 213 **f)** 0, 223
g) 123, 2347 **h)** 3454, 4666 **i)** 9999, 11111

2. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 9, 11 **b)** 33, 44 **c)** 35, 78
d) 21, 55 **e)** 101, 203 **f)** 124, 323
g) 2002, 2339 **h)** 3457, 4669 **i)** 10001, 13422

3. Show that 15 is an inverse of 7 modulo 26.

4. Show that 937 is an inverse of 13 modulo 2436.

5. Find an inverse of 4 modulo 9.

6. Find an inverse of 2 modulo 17.

7. Find an inverse of 19 modulo 141.

8. Find an inverse of 144 modulo 233.

***9.** 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 2 to show that $b \equiv c \pmod{m}$.]

10. Show that an inverse of a modulo m does not exist if $\gcd(a, m) > 1$.

11. Solve the congruence $4x \equiv 5 \pmod{9}$.

12. Solve the congruence $2x \equiv 7 \pmod{17}$.

***13.** Show that if m is a positive integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \bmod m / \gcd(c, m)$.

14. a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

b) Use part (a) to show that $10! \equiv -1 \pmod{11}$.

15. Show that if p is prime, the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers x such that $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$.

***16. a)** Generalize the result in part (a) of Exercise 14; that is, show that if p is a prime, the positive integers less than p, except 1 and $p-1$, can be split into $(p-3)/2$ pairs of integers such that each pair consists of integers that are inverses of each other. (*Hint:* Use the result of Exercise 15.)

b) From part (a) conclude that $(p-1)! \equiv -1 \pmod{p}$ whenever p is prime. This result is known as **Wilson's Theorem.**

c) What can we conclude if n is a positive integer such that $(n-1)! \not\equiv -1 \pmod{n}$?

***17.** This exercise outlines a proof of Fermat's Little Theorem.

a) Suppose that a is not divisible by the prime p. Show that no two of the integers $1 \cdot a, 2 \cdot a, \ldots, (p-1)a$ are congruent modulo p.

b) Conclude from part (a) that the product of $1, 2, \ldots, p-1$ is congruent modulo p to the product of $a, 2a, \ldots, (p-1)a$. Use this to show that

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

c) Use Wilson's theorem (proved in Exercise 16) to show that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$.

d) Use part (c) to show that $a^p \equiv a \pmod{p}$ for all integers a.

18. Find all solutions to the system of congruences.
$x \equiv 2 \pmod 3$
$x \equiv 1 \pmod 4$
$x \equiv 3 \pmod 5$

19. Find all solutions to the system of congruences.
$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod{11}$

***20.** Find all solutions, if any, to the system of congruences.
$x \equiv 5 \pmod 6$
$x \equiv 3 \pmod{10}$
$x \equiv 8 \pmod{15}$

***21.** Find all solutions, if any, to the system of congruences.
$x \equiv 7 \pmod 9$
$x \equiv 4 \pmod{12}$
$x \equiv 16 \pmod{21}$

22. Use the Chinese Remainder Theorem to show that an integer a, with $0 \leq a < m = m_1 m_2 \cdots m_n$, where the integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, can be represented uniquely by the n-tuple (a **mod** m_1, a **mod** $m_2, \ldots, a$ **mod** m_n).

***23.** Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod m$, where $m = m_1 m_2 \cdots m_n$.

***24.** Complete the proof of the Chinese Remainder Theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime integers is unique modulo the product of these moduli. (*Hint:* Assume that x and y are two simultaneous solutions. Show that $m_i \mid x - y$ for all i. Using Exercise 23, conclude that $m = m_1 m_2 \cdots m_n \mid x - y$.)

25. Which integers leave a remainder of 1 when divided by 2 and also leave a remainder of 1 when divided by 3?

26. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

27. a) Show that $2^{340} \equiv 1 \pmod{11}$ by Fermat's Little Theorem and noting that $2^{340} = (2^{10})^{34}$.

b) Show that $2^{340} \equiv 1 \pmod{31}$ using the fact that $2^{340} = (2^5)^{68} = 32^{68}$.

c) Conclude from parts (a) and (b) that $2^{340} \equiv 1 \pmod{341}$.

28. a) Use Fermat's Little Theorem to compute 3^{302} **mod** 5, 3^{302} **mod** 7, and 3^{302} **mod** 11.

b) Use your results from part (a) and the Chinese Remainder Theorem to find 3^{302} **mod** 385. (Note that $385 = 5 \cdot 7 \cdot 11$.)

29. a) Use Fermat's Little Theorem to compute 5^{2003} **mod** 7, 5^{2003} **mod** 11, and 5^{2003} **mod** 13.

b) Use your results from part (a) and the Chinese Remainder Theorem to find 5^{2003} **mod** 1001. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Let n be a positive integer and let $n - 1 = 2^s t$, where s is a nonnegative integer and t is an odd positive integer. We say that n passes **Miller's test for the base** b if either $b^t \equiv 1 \pmod n$ or $b^{2^j t} \equiv -1 \pmod n$ for some j with $0 \leq j \leq s - 1$. It can be shown (see [Ro00]) that a composite integer n passes Miller's test for fewer than $n/4$ bases b with $1 < b < n$.

30. Show that if n is prime and b is a positive integer with $n \nmid b$, then n passes Miller's test to the base b.

31. Show that 2047 passes Miller's test to the base 2, but that it is composite. A composite positive integer n that passes Miller's test to the base b is called a **strong pseudoprime to the base** b. It follows that 2047 is a strong pseudoprime to the base 2.

32. Show that 1729 is a Carmichael number.

33. Show that 2821 is a Carmichael number.

***34.** Show that if $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes that satisfy $p_j - 1 \mid n - 1$ for $j = 1, 2, \ldots, k$, then n is a Carmichael number.

35. a) Use Exercise 34 to show that every integer of the form $(6m+1)(12m+1)(18m+1)$, where m is a positive integer and $6m+1, 12m+1$, and $18m+1$ are all primes, is a Carmichael number.

b) Use part (a) to show that 172,947,529 is a Carmichael number.

36. Find the nonnegative integer a less than 28 represented by each of these pairs, where each pair represents (a **mod** 4, a **mod** 7).

a) $(0,0)$ **b)** $(1,0)$ **c)** $(1,1)$
d) $(2,1)$ **e)** $(2,2)$ **f)** $(0,3)$
g) $(2,0)$ **h)** $(3,5)$ **i)** $(3,6)$

37. Express each nonnegative integer a less than 15 using the pair (a **mod** 3, a **mod** 5).

38. Explain how to use the pairs found in Exercise 37 to add 4 and 7.

39. Solve the system of congruences that arises in Example 8.

***40.** Show that if a and b are positive integers, then $(2^a - 1)$ **mod** $(2^b - 1) = 2^{a \bmod b} - 1$.

****41.** Use Exercise 40 to show that if a and b are positive integers, then $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. [*Hint:* Show that the remainders obtained when the Euclidean algorithm is used to compute $\gcd(2^a - 1,$

$2^b - 1$) are of the form $2^r - 1$, where r is a remainder arising when the Euclidean algorithm is used to find $\gcd(a, b)$.]

42. Use Exercise 41 to show that 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.

43. Show that if p is an odd prime, then every divisor of the Mersenne number $2^p - 1$ is of the form $2kp + 1$, where k is a nonnegative integer. (*Hint:* Use Fermat's Little Theorem and Exercise 41.)

44. Use Exercise 43 to determine whether $M_{13} = 2^{13} - 1 = 8191$ and $M_{23} = 2^{23} - 1 = 8{,}388{,}607$ are prime.

***45.** Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p - 1)(q - 1)$.

46. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 11.

47. What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? (*Note:* Some computational aid is needed to do this in a realistic amount of time.)

The **extended Euclidean algorithm** can be used to express $\gcd(a, b)$ as a linear combination with integer coefficients of the integers a and b. We set $s_0 = 1, s_1 = 0, t_0 = 0$, and $t_1 = 1$ and let $s_j = s_{j-2} - q_{j-1}s_{j-1}$ and $t_j = t_{j-2} - q_{j-1}t_{j-1}$ for $j = 2, 3, \ldots, n$, where the q_j are the quotients in the divisions used when the Euclidean algorithm finds $\gcd(a, b)$ (see page 178). It can be shown (see [Ro00]) that $\gcd(a, b) = s_n a + t_n b$.

48. Use the extended Euclidean algorithm to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

49. Use the extended Euclidean algorithm to express $\gcd(144, 89)$ as a linear combination of 144 and 89.

50. Use the extended Euclidean algorithm to express $\gcd(1001, 100001)$ as a linear combination of 1001 and 100001.

51. Describe the extended Euclidean algorithm using pseudocode.

If m is a positive integer, the integer a is a **quadratic residue** of m if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. In other words, a quadratic residue of m is an integer relatively prime to m that is a perfect square modulo m. For example, 2 is a quadratic residue of 7 since $\gcd(2, 7) = 1$ and $3^2 \equiv 2 \pmod 7$ and 3 is a quadratic nonresidue of 7 since $\gcd(3, 7) = 1$ and $x^2 \equiv 3 \pmod 7$ has no solution.

52. Which integers are quadratic residues of 11?

53. Show that if p is an odd prime and a is an integer not divisible by p, then the congruence $x^2 \equiv a \pmod p$ has either no solutions or exactly two incongruent solutions modulo p.

54. Show that if p is an odd prime, then there are exactly $(p - 1)/2$ quadratic residues of p among the integers $1, 2, \ldots, p - 1$.

If p is an odd prime and a is an integer not divisible by p, the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue of p and -1 otherwise.

55. Show that if p is an odd prime and a and b are integers with $a \equiv b \pmod p$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

56. Prove that if p is an odd prime and a is a positive integer not divisible by p, then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

57. Use Exercise 56 to show that if p is an odd prime and a and b are integers not divisible by p, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

58. Show that if p is an odd prime, then -1 is a quadratic residue of p if $p \equiv 1 \pmod 4$ and 1 is not a quadratic residue of p if $p \equiv 3 \pmod 4$. (*Hint:* Use Exercise 56.)

59. Find all solutions of the congruence $x^2 \equiv 29 \pmod{35}$. (*Hint:* Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese Remainder Theorem.)

60. Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$. (*Hint:* Find the solutions of this congruence modulo 3, modulo 5, and modulo 7, and then use the Chinese Remainder Theorem.)

2.7 Matrices

INTRODUCTION

Matrices are used throughout discrete mathematics to express relationships between elements in sets. In subsequent chapters we will use matrices in a wide variety of models. For instance, matrices will be used in models of communications networks and transportation