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

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