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:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

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

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