15

The Fundamental Theorem of Arithmetic

One can use Euclid's algorithm to find the gcd of two positive integers a and b. One can also exploit the algorithm to express the gcd d in the form $d = ax + by$ where x and y are integers. Actually, d is the smallest positive integer with this property, and this fact can also be used to describe the gcd of a and b.

Theorem 15.1. *Given positive integers a and b, their gcd is the smallest positive integer d such that $d = ax + by$ with $x, y \in \mathbf{Z}$.*

Proof: Note that the set $\{ax + by | x, y \in \mathbf{Z}\}$ does contain positive integers, e.g., $2ab$. Let d be the smallest positive integer in the set. Clearly any common divisor of a and b divides d. So, to prove that $d = \gcd(a, b)$, we only have to show that d divides a and b. To prove that d divides a, divide a by d to get quotient q and remainder r, so that

$$a = qd + r, \quad 0 \leq r < d.$$

Then $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$ is also of the form $ax' + by'$ with $x', y' \in \mathbf{Z}$. Since d was the smallest positive integer of this form and since $0 \leq r < d$, it follows that $r = 0$, hence d divides a. Similarly, d divides b, so d is a common divisor of a and b.

The following consequence of the theorem is known as the *Fundamental Lemma of Arithmetic.*

Lemma 15.2. *Given positive integers a, b and c, if a divides bc and*

$\gcd(a,b) = 1$, *then a divides c. In particular, if a prime number p divides bc, then p divides b or p divides c.*

Proof: If $\gcd(a,b) = 1$, it follows from the theorem that there are integers x and y such that $ax + by = 1$. Moreover, if a divides bc, there is an integer z such that $bc = az$. Therefore,

$$c = axc + byc = a(xc + yz),$$

and so a divides c.

The Fundamental Theorem of Arithmetic asserts that every positive integer has a factorization into primes; moreover, if we disregard the order of the primes, this factorization is unique. This theorem follows quite easily from the above lemma and we leave it as an exercise. For another proof and a discussion of its history, see Part I, Chapter 3.

Given positive integers a and b, say with $a > b$, we obtain a continued fraction expansion $a/b = (a_0, a_1, \ldots, a_n)$. Even though this continued fraction is *finite*, we can still use the analysis of the previous section to calculate its convergents p_0/q_0 up to p_n/q_n. In particular, $a/b = p_n/q_n$, hence $aq_n = bp_n$. Since $\gcd(p_n, q_n) = 1$, it follows from the Fundamental Lemma of Arithmetic that p_n divides a, say $a = p_n d$, whence also $b = q_n d$. Evidently, d is the gcd of a and b. But it also follows from Theorem 14.2, upon multiplying by d, that $aq_{n-1} - bp_{n-1} = d(-1)^{n-1}$. This allows us to find particular integers x and y such that $d = ax + by$, namely,

$$x = (-1)^{n-1} q_{n-1}, \qquad y = (-1)^n p_{n-1}.$$

Exercises

1. Prove that the smallest divisor > 1 of a positive integer > 1 is a prime number.

2. Deduce that every positive integer > 1 is a product of prime numbers and use the Fundamental Lemma of Arithmetic to show that this factorization into primes is unique.

3. If a, b and c are positive integers and $c > 1$, show that

$$\gcd(c^a - 1, c^b - 1) = c^d - 1,$$

where $d = \gcd(a,b)$. (Hint: use the above theorem.)

16

Linear Diophantine Equations

A *linear Diophantine equation* in two variables is an equation of the form $ax + by = c$ where a, b and c are given integers, and x and y are unknown integers. Sometimes x and y are restricted to the set of *positive* integers.

For example, $4x+6y = 8$ is a linear Diophantine equation. It has solution $x = 2$ and $y = 0$ (among others). Here we are not interested in noninteger solutions such as $x = \frac{1}{2}$, $y = 1$.

In order to simplify the presentation, we shall allow negative numbers as solutions, but we shall take a, b and c to be positive. By dividing the material into different cases, we could elaborate the whole theory in terms of positive integers. Thus, there is nothing in this chapter which would be inaccessible to the ancient Greeks. On the contrary, it is probable that they used essentially the following method to attack these equations.

The adjective 'Diophantine' comes from the name 'Diophantus'. Diophantus of Alexandria lived about 250 AD. However, in his equations he did not restrict x and y to be integers, but allowed them to be rationals. It was Brahmagupta of India (628 AD) who gave the first complete solution to the linear Diophantine equation (Boyer [1989], pp. 244-47).

Let $d = \gcd(a, b)$. Then there are integers a' and b' such that $a = da'$ and $b = db'$. If $ax + by = c$ then $d(a'x + b'y) = c$ and hence d is a factor of c. Thus, if d is not a factor of c, the Diophantine equation has no solutions. On the other hand, if d is a factor of c, then $c = dc'$ for some integer c', and we can cancel d to get $a'x + b'y = c'$, with $\gcd(a', b') = 1$. In giving a solution of $ax + by = c$, we can thus, without loss of generality, begin by assuming that $\gcd(a, b) = 1$.

To solve the Diophantine equation $ax + by = c$ when $\gcd(a, b) = 1$: