where q is the *quotient* and r the *remainder.* This is the usual "long division" familiar from elementary arithmetic.

(6) The *Euclidean Algorithm* is an important procedure which produces a greatest common divisor of two integers a and b by iterating the Division Algorithm: if $a, b \in \mathbb{Z} - \{0\}$, then we obtain a sequence of quotients and remainders

$$\begin{aligned} a &= q_0 b + r_0 && (0)\\ b &= q_1 r_0 + r_1 && (1)\\ r_0 &= q_2 r_1 + r_2 && (2)\\ r_1 &= q_3 r_2 + r_3 && (3)\\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && (n)\\ r_{n-1} &= q_{n+1} r_n && (n{+}1) \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a decreasing sequence of strictly positive integers if the remainders are nonzero and such a sequence cannot continue indefinitely. Then r_n is the g.c.d. (a, b) of a and b.

Example

Suppose $a = 57970$ and $b = 10353$. Then applying the Euclidean Algorithm we obtain:

$$\begin{aligned} 57970 &= (5)10353 + 6205\\ 10353 &= (1)6205 + 4148\\ 6205 &= (1)4148 + 2057\\ 4148 &= (2)2057 + 34\\ 2057 &= (60)34 + 17\\ 34 &= (2)17 \end{aligned}$$

which shows that $(57970, 10353) = 17$.

(7) One consequence of the Euclidean Algorithm which we shall use regularly is the following: if $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

that is, *the g.c.d. of a and b is a $\mathbb{Z}$-linear combination of a and b.* This follows by recursively writing the element r_n in the Euclidean Algorithm in terms of the previous remainders (namely, use equation (n) above to solve for $r_n = r_{n-2} - q_n r_{n-1}$ in terms of the remainders r_{n-1} and r_{n-2}, then use equation $(n - 1)$ to write r_n in terms of the remainders r_{n-2} and r_{n-3}, etc., eventually writing r_n in terms of a and b).

Example

Suppose $a = 57970$ and $b = 10353$, whose greatest common divisor we computed above to be 17. From the fifth equation (the next to last equation) in the Euclidean Algorithm applied to these two integers we solve for their greatest common divisor: $17 = 2057 - (60)34$. The fourth equation then shows that $34 = 4148 - (2)2057$, so substituting this expression for the previous remainder 34 gives the equation $17 = 2057 - (60)[4148 - (2)2057]$, i.e., $17 = (121)2057 - (60)4148$. Solving the third equation for 2057 and substituting gives $17 = (121)[6205 - (1)4148] - (60)4148 = (121)6205 - (181)4148$. Using the second equation to solve for 4148 and then the first equation to solve for 6205 we finally obtain

$$17 = (302)57970 - (1691)10353$$

as can easily be checked directly. Hence the equation $ax + by = (a, b)$ for the greatest common divisor of a and b in this example has the solution $x = 302$ and $y = -1691$. Note that it is relatively unlikely that this relation would have been found simply by guessing.

The integers x and y in (7) above are not unique. In the example with $a = 57970$ and $b = 10353$ we determined one solution to be $x = 302$ and $y = -1691$, for instance, and it is relatively simple to check that $x = -307$ and $y = 1719$ also satisfy $57970x + 10353y = 17$. The general solution for x and y is known (cf. the exercises below and in Chapter 8).

(8) An element p of $\mathbb{Z}^+$ is called a *prime* if $p > 1$ and the only positive divisors of p are 1 and p (initially, the word prime will refer only to positive integers). An integer $n > 1$ which is not prime is called *composite*. For example, 2,3,5,7,11,13,17,19,... are primes and 4,6,8,9,10,12,14,15,16,18,... are composite.
An important property of primes (which in fact can be used to *define* the primes (cf. Exercise 3)) is the following: if p is a prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$.

(9) The *Fundamental Theorem of Arithmetic* says: if $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \dots, p_s$ and positive integers $\alpha_1, \alpha_2, \dots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}.$$

This factorization is unique in the sense that if $q_1, q_2, \dots, q_t$ are any distinct primes and $\beta_1, \beta_2, \dots, \beta_t$ positive integers such that

$$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t},$$

then $s = t$ and if we arrange the two sets of primes in increasing order, then $q_i = p_i$ and $\alpha_i = \beta_i$, $1 \le i \le s$. For example, $n = 1852423848 = 2^3 3^2 11^2 19^3 31$ and this decomposition into the product of primes is unique.

Suppose the positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$$

where $p_1, p_2, \dots, p_s$ are distinct and the exponents are ≥ 0 (we allow the exponents to be 0 here so that the products are taken over the same set of primes — the exponent will be 0 if that prime is not actually a divisor). Then the greatest common divisor of a and b is

$$(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_s^{\min(\alpha_s,\beta_s)}$$

(and the least common multiple is obtained by instead taking the maximum of the α_i and β_i instead of the minimum).

Example

In the example above, $a = 57970$ and $b = 10353$ can be factored as $a = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 31$ and $b = 3 \cdot 7 \cdot 17 \cdot 29$, from which we can immediately conclude that their greatest common divisor is 17. Note, however, that for large integers it is extremely difficult to determine their prime factorizations (several common codes in current use are based on this difficulty, in fact), so that this is not an effective method to determine greatest common divisors in general. The Euclidean Algorithm will produce greatest common divisors quite rapidly without the need for the prime factorization of a and b.

10) The *Euler φ-function* is defined as follows: for $n \in \mathbb{Z}^+$ let $\varphi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n, i.e., $(a, n) = 1$. For example, $\varphi(12) = 4$ since 1, 5, 7 and 11 are the only positive integers less than or equal to 12 which have no factors in common with 12. Similarly, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, etc. For primes p, $\varphi(p) = p - 1$, and, more generally, for all $a \geq 1$ we have the formula

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1).$$

The function φ is *multiplicative* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{if } (a, b) = 1$$

(note that it is important here that a and b be relatively prime). Together with the formula above this gives a general formula for the values of φ : if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, then

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_s^{\alpha_s - 1}(p_s - 1). \end{aligned}$$

For example, $\varphi(12) = \varphi(2^2)\varphi(3) = 2^1(2-1)3^0(3-1) = 4$. The reader should note that we shall use the letter φ for many different functions throughout the text so when we want this letter to denote Euler's function we shall be careful to indicate this explicitly.

EXERCISES

1. For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y.

(a) $a = 20, b = 13$.
(b) $a = 69, b = 372$.
(c) $a = 792, b = 275$.
(d) $a = 11391, b = 5673$.
(e) $a = 1761, b = 1567$.
(f) $a = 507885, b = 60808$.

2. Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t.

3. Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

4. Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers
$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$
are also solutions to $ax + by = N$ (this is in fact the general solution).

5. Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ-function.

6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

7. If p is a prime prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p}$ is not a rational number).

8. Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\dots 2 \cdot 1$ (it involves the greatest integer function).

9. Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y.

10. Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ-function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

11. Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ-function.

0.3 $\mathbb{Z}/n\mathbb{Z}$: THE INTEGERS MODULO n

Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by
$$a \sim b \text{ if and only if } n \mid (b - a).$$

Clearly $a \sim a$, and $a \sim b$ implies $b \sim a$ for any integers a and b, so this relation is trivially reflexive and symmetric. If $a \sim b$ and $b \sim c$ then n divides $a - b$ and n divides $b - c$ so n also divides the sum of these two integers, i.e., n divides $(a - b) + (b - c) = a - c$, so $a \sim c$ and the relation is transitive. Hence this is an equivalence relation. Write $a \equiv b \pmod{n}$ (read: a is *congruent* to b mod n) if $a \sim b$. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of a by $\bar{a}$ — this is called the *congruence class* or *residue class* of a mod n and consists of the integers which differ from a by an integral multiple of n, i.e.,
$$\begin{aligned}\bar{a} &= \{a + kn \mid k \in \mathbb{Z}\}\\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}.\end{aligned}$$

There are precisely n distinct equivalence classes mod n, namely
$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$$
determined by the possible remainders after division by n and these residue classes partition the integers $\mathbb{Z}$. The set of equivalence classes under this equivalence relation