1
Divisibility

We start with a number of fairly elementary results and techniques, mainly about greatest common divisors. You have probably met some of this material already, though it may not have been treated as formally as here. There are several good reasons for giving very precise definitions and proofs, even when there is general agreement about the validity of the mathematics involved. The first is that 'general agreement' is not the same as convincing proof: it is not unknown for majority opinion to be seriously mistaken about some point. A second reason is that, if we know exactly what assumptions are required in order to deduce certain conclusions, then we may be able to deduce similar conclusions in other areas where the same assumptions hold true. For example, this chapter is entirely devoted to the divisibility properties of *integers*, but it turns out that very similar definitions, methods and theorems are valid for certain other objects which can be added, subtracted and multiplied; some of these objects, such as polynomials, are very familiar, while others, such as Gaussian integers and quaternions, will be introduced in later chapters. These generalisations of the integers are also explored in algebra, under the heading of ring theory.

1.1 Divisors

Our starting-point is the *division algorithm*, which is as follows:

Theorem 1.1

If a and b are integers with $b > 0$, then there is a unique pair of integers q and r such that

$$a = qb + r \qquad \text{and} \qquad 0 \leq r < b\,.$$

Example 1.1

If $a = 9$ and $b = 4$ then we have $9 = 2 \times 4 + 1$ with $0 \leq 1 < 4$, so $q = 2$ and $r = 1$; if $a = -9$ and $b = 4$ then $q = -3$ and $r = 3$.

In Theorem 1.1, we call q the *quotient* and r the *remainder*. By dividing by b, so that

$$\frac{a}{b} = q + \frac{r}{b} \qquad \text{and} \qquad 0 \leq \frac{r}{b} < 1\,,$$

we see that q is the integer part $\lfloor a/b \rfloor$ of a/b, the greatest integer $i \leq a/b$. This makes it easy to calculate q, and then to find $r = a - qb$.

Proof

First we prove existence. Let

$$S = \{a - nb \mid n \in \mathbb{Z}\} = \{\, a, a \pm b, a \pm 2b, \ldots \}\,.$$

This set of integers contains non-negative elements (take $n = -|a|$), so $S \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$; by the well-ordering principle (see Appendix A), $S \cap \mathbb{N}$ has a least element, which has the form $r = a - qb \geq 0$ for some integer q. Thus $a = qb + r$ with $r \geq 0$. If $r \geq b$ then S contains a non-negative element $a - (q+1)b = r - b < r$; this contradicts the minimality of r, so we must have $r < b$.

To prove uniqueness, suppose that $a = qb + r = q'b + r'$ with $0 \leq r < b$ and $0 \leq r' < b$, so $r - r' = (q' - q)b$. If $q' \neq q$ then $|q' - q| \geq 1$, so $|r - r'| \geq |b| = b$, which is impossible since r and r' lie between 0 and $b-1$ inclusive. Hence $q' = q$ and so $r' = r$. □

We can now deal with the case $b < 0$: since $-b > 0$, Theorem 1.1 implies that there exist integers q^* and r such that $a = q^*(-b) + r$ and $0 \leq r < -b$, so

putting $q = -q^*$ we again have $a = qb + r$. Uniqueness is proved as before, so combining this with Theorem 1.1 we have:

Corollary 1.2

If a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that

$$a = qb + r \qquad \text{and} \qquad 0 \leq r < |b| .$$

(Note that when $b < 0$ we have

$$\frac{a}{b} = q + \frac{r}{b} \qquad \text{and} \qquad 0 \geq \frac{r}{b} > -1 ,$$

so that in this case q is $\lceil a/b \rceil$, the least integer $i \geq a/b$.)

Example 1.2

As an application, we show that if n is a square then n leaves a remainder 0 or 1 when divided by 4. To prove this, let $n = a^2$. Theorem 1.1 (with $b = 4$) gives $a = 4q + r$ where $r = 0, 1, 2$ or 3, so that

$$n = (4q + r)^2 = 16q^2 + 8qr + r^2 .$$

If $r = 0$ then $n = 4(4q^2 + 2qr) + 0$, if $r = 1$ then $n = 4(4q^2 + 2qr) + 1$, if $r = 2$ then $n = 4(4q^2 + 2qr + 1) + 0$, and if $r = 3$ then $n = 4(4q^2 + 2qr + 2) + 1$. In each case, the remainder is 0 or 1.

Exercise 1.1

Find a shorter proof for Example 1.2, based on putting $b = 2$ in Theorem 1.1.

Exercise 1.2

What are the possible remainders when a perfect square is divided by 3, or by 5, or by 6 ?

Definition

If a and b are any integers, and $a = qb$ for some integer q, then we say that b *divides* a, or b is a *factor* of a, or a is a *multiple* of b. For instance, the factors of 6 are $\pm 1, \pm 2, \pm 3$ and ± 6. When b divides a we write $b|a$, and we use the notation $b \not| a$ when b does not divide a. To avoid common misconceptions, we

note that every integer divides 0 (since $0 = 0.b$ for all b), 1 divides every integer, and every integer divides itself. We now record some simple but useful facts about divisibility, proving two of them, and leaving the rest for the reader.

Exercise 1.3

Prove that

(a) if $a|b$ and $b|c$ then $a|c$;

(b) if $a|b$ and $c|d$ then $ac|bd$;

(c) if $m \neq 0$, then $a|b$ if and only if $ma|mb$;

(d) if $d|a$ and $a \neq 0$ then $|d| \leq |a|$.

Theorem 1.3

(a) If c divides $a_1, \ldots, a_k$, then c divides $a_1u_1 + \cdots + a_ku_k$ for all integers $u_1, \ldots, u_k$.

(b) $a|b$ and $b|a$ if and only if $a = \pm b$.

Proof

(a) If c divides a_i then $a_i = q_ic$ for some integers q_i $(i = 1, \ldots, k)$. Then $a_1u_1 + \cdots + a_ku_k = q_1cu_1 + \cdots + q_kcu_k = (q_1u_1 + \cdots + q_ku_k)c$, and as $q_1u_1 + \cdots + q_ku_k$ is an integer (since q_i and u_i are) we see that $c|(a_1u_1 + \cdots + a_ku_k)$.

(b) If $a = \pm b$ then $b = qa$ and $a = q'b$ where $q = q' = \pm 1$, so $a|b$ and $b|a$. Conversely, let $a|b$ and $b|a$, so $b = qa$ and $a = q'b$ for some integers q and q'. If $b = 0$ then the second equation gives $a = 0$, so $a = \pm b$ as required. We can therefore assume that $b \neq 0$. Eliminating a from the two equations, we have $b = qq'b$; cancelling b (possible since $b \neq 0$) we have $qq' = 1$, so $q, q' = \pm 1$ (using Exercise 1.3(d)) and hence $a = \pm b$. □

Exercise 1.4

If a divides b, and c divides d, must $a + c$ divide $b + d$?

The most useful form of Theorem 1.3(a) is the case $k = 2$, which we record in the following slightly simpler notation.

Corollary 1.4

If c divides a and b, then c divides $au + bv$ for all integers u and v.

Definition

If $d|a$ and $d|b$ we say that d is a *common divisor* (or *common factor*) of a and b; for instance, 1 is a common divisor of any pair of integers a and b. If a and b are not both 0, then Exercise 1.3(d) shows that no common divisor is greater than $\max(|a|, |b|)$, so that among all their common divisors there is a greatest one. This is the *greatest common divisor* (or *highest common factor*) of a and b; it is the unique integer d satisfying

(1) $d|a$ and $d|b$ (so that d is a common divisor),

(2) if $c|a$ and $c|b$ then $c \leq d$ (so that no common divisor exceeds d).

However, the case $a = b = 0$ has to be excluded: every integer divides 0 and is therefore a common divisor of a and b, so there is no greatest common divisor in this case. When it exists, we denote the greatest common divisor of a and b by $\gcd(a, b)$, or simply (a, b). This definition extends in the obvious way to the greatest common divisor of any set of integers (not all 0).

One way of finding the greatest common divisor of a and b is simply to list all the divisors of a and all the divisors of b, and to choose the largest integer appearing in both lists. It is clearly sufficient to list positive divisors: if $a = 12$ and $b = -18$, for example, then by writing the positive divisors of 12 as $1, 2, 3, 4, 6, 12$, and those of -18 as $1, 2, 3, 6, 9, 18$, we immediately see that the greatest common divisor is 6. This method can be very tedious when a or b are large, but fortunately there is a more efficient method of calculating greatest common divisors, namely *Euclid's algorithm* (published in Book VII of Euclid's *Elements* around 300 BC). This is based on the following simple observation.

Lemma 1.5

If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.

Proof

By Corollary 1.4, any common divisor of b and r also divides $qb + r = a$; similarly, since $r = a - qb$, it follows that any common divisor of a and b also divides r. Thus the two pairs a, b and b, r have the same common divisors, so they have the same greatest common divisor. □

Euclid's algorithm uses this repeatedly to simplify the calculation of greatest common divisors by reducing the size of the given integers without changing their greatest common divisor. Suppose we are given two integers a and b (not both 0), and we wish to find $d = \gcd(a, b)$. If $a = 0$ then $d = |b|$, and if $b = 0$ then $d = |a|$, so ignoring these trivial cases we may assume that a and b are both non-zero. Since

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)\,,$$

we may assume that a and b are both positive. Since $\gcd(a, b) = \gcd(b, a)$ we may assume that $a \geq b$, and by ignoring the trivial case $\gcd(a, a) = a$ we may assume that $a > b$, so

$$a > b > 0\,.$$

We now use the division algorithm (Theorem 1.1) to divide b into a, and write

$$a = q_1 b + r_1 \qquad \text{with} \qquad 0 \leq r_1 < b\,.$$

If $r_1 = 0$ then $b|a$, so $d = b$ and we halt. If $r_1 \neq 0$ then we divide r_1 into b and write

$$b = q_2 r_1 + r_2 \qquad \text{with} \qquad 0 \leq r_2 < r_1\,.$$

Now Lemma 1.5 gives $\gcd(a, b) = \gcd(b, r_1)$, so if $r_2 = 0$ then $d = r_1$ and we halt. If $r_2 \neq 0$ we write

$$r_1 = q_3 r_2 + r_3 \qquad \text{with} \qquad 0 \leq r_3 < r_2\,,$$

and we continue in this way; since $b > r_1 > r_2 > \ldots \geq 0$, we must eventually get a remainder $r_n = 0$ (after at most b steps) at which point we stop. The last two steps will have the form

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad \text{with} \qquad 0 < r_{n-1} < r_{n-2}\,,$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad \text{with} \qquad r_n = 0.$$

Theorem 1.6

In the above calculation we have $d = r_{n-1}$ (the last non-zero remainder).

Proof

By applying Lemma 1.5 to the successive equations for $a, b, r_1, \ldots, r_{n-3}$ we see that

$$d = \gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})\,.$$

The last equation $r_{n-2} = q_n r_{n-1}$ shows that $r_{n-1} | r_{n-2}$, so $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$ and hence $d = r_{n-1}$. □

Example 1.3

To calculate $d = \gcd(1492, 1066)$ we write

$$\begin{aligned} 1492 &= 1.1066 + 426 \\ 1066 &= 2.426 + 214 \\ 426 &= 1.214 + 212 \\ 214 &= 1.212 + 2 \\ 212 &= 106.2 + 0\,. \end{aligned}$$

The last non-zero remainder is 2, so $d = 2$.

In many cases, the value of d can be identified before a zero remainder is reached: since $d = \gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots$, one can stop as soon as one recognises the greatest common divisor of a pair of consecutive terms in the sequence $a, b, r_1, r_2, \ldots$. In Example 1.3, for instance, the remainders 214 and 212 clearly have greatest common divisor 2, so $d = 2$.

Exercise 1.5

Calculate $\gcd(1485, 1745)$.

Supplementary Exercises 1.17–1.24 consider the efficiency of Euclid's algorithm; see also Knuth (1968) for a detailed analysis. Stein's (1967) algorithm is similar, but more suitable for computer implementation: it avoids the time-consuming operation of division, and by concentrating on powers of 2 it exploits the binary arithmetic used in computers.

1.2 Bezout's identity

The following result uses Euclid's algorithm to give a simple expression for $d = \gcd(a, b)$ in terms of a and b:

Theorem 1.7

If a and b are integers (not both 0), then there exist integers u and v such that

$$\gcd(a, b) = au + bv\,.$$

(This equation is sometimes known as *Bezout's identity*. We will see later that the values of u and v are not uniquely determined by a and b.)

Proof

We use the equations which arise when we apply Euclid's algorithm to calculate $d = \gcd(a, b)$ as the last non-zero remainder r_{n-1}. The penultimate equation, in the form

$$r_{n-1} = r_{n-3} - q_{n-1}r_{n-2}\,,$$

expresses d as a multiple of r_{n-3} plus a multiple of r_{n-2}. We then use the previous equation, in the form

$$r_{n-2} = r_{n-4} - q_{n-2}r_{n-3}\,,$$

to eliminate r_{n-2} and express d as a multiple of r_{n-4} plus a multiple of r_{n-3}. We gradually work backwards through the equations in the algorithm, eliminating $r_{n-3}, r_{n-4}, \ldots$ in succession, until eventually we have expressed d as a multiple of a plus a multiple of b, that is, $d = au + bv$ for some integers u and v. □

Example 1.4

In Example 1.3 we used Euclid's algorithm to calculate d, where $a = 1492$ and $b = 1066$. Using those equations again, we have

$$\begin{aligned} d &= 2 \\ &= 214 - 1.212 \\ &= 214 - 1.(426 - 1.214) \\ &= -1.426 + 2.214 \\ &= -1.426 + 2.(1066 - 2.426) \\ &= 2.1066 - 5.426 \\ &= 2.1066 - 5(1492 - 1.1066) \\ &= -5.1492 + 7.1066\,, \end{aligned}$$

so we can take $u = -5$ and $v = 7$. The next exercise shows that the values we have found for u and v are not unique. (Later, in Theorem 1.13, we will see how to determine all possible values for u and v.)

Exercise 1.6

Find a pair of integers $u' \neq -5$ and $v' \neq 7$ such that $\gcd(1492, 1066) = 1492u' + 1066v'$.

Exercise 1.7

Express $\gcd(1485, 1745)$ in the form $1485u + 1745v$.

Exercise 1.8

Show that $c|a$ and $c|b$ if and only if $c|\gcd(a,b)$.

Having seen how to calculate the greatest common divisor of two integers, it is a straightforward matter to extend this to any finite set of integers (not all 0). The method, which involves repeated use of Euclid's algorithm, is based on the following exercise.

Exercise 1.9

Prove that $\gcd(a_1,\ldots,a_k) = \gcd(\gcd(a_1,a_2),a_3,\ldots,a_k)$.

This reduces the problem of calculating the greatest common divisor d of k integers to two smaller problems: we calculate $d_2 = \gcd(a_1,a_2)$ and then $d = \gcd(d_2,a_3,\ldots,a_k)$, involving two and $k-1$ integers respectively. This second problem can be further reduced by calculating $d_3 = \gcd(d_2,a_3)$ and then $d = \gcd(d_3,a_4,\ldots,a_k)$, involving two and $k-2$ integers. Continuing, we eventually reduce the problem to a sequence of $k-1$ calculations involving pairs of integers, each of which can be performed by Euclid's algorithm: we find $d_2 = \gcd(a_1,a_2), d_i = \gcd(d_{i-1},a_i)$ for $i = 3,\ldots,k$, and put $d = d_k$.

Example 1.5

To calculate $d = \gcd(36,24,54,27)$ we find $d_2 = \gcd(36,24) = 12$, then $d_3 = \gcd(12,54) = 6$, and finally $d = d_4 = \gcd(6,27) = 3$.

Exercise 1.10

Calculate $\gcd(1092,1155,2002)$ and $\gcd(910,780,286,195)$.

Exercise 1.11

Show that if $a_1,\ldots,a_k$ are non-zero integers, then their greatest common divisor has the form $a_1u_1+\cdots+a_ku_k$ for some integers $u_1,\ldots,u_k$. Find such an expression where $k = 3$ and $a_1 = 1092, a_2 = 1155, a_3 = 2002$.

Theorem 1.7 states that $\gcd(a,b)$ can be written as a multiple of a plus a multiple of b; using this we shall describe the set of all integers which can be written in this form.

Theorem 1.8

Let a and b be integers (not both 0) with greatest common divisor d. Then an integer c has the form $ax + by$ for some $x, y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ $(x, y \in \mathbb{Z})$.

Proof

If $c = ax + by$ where $x, y \in \mathbb{Z}$, then since d divides a and b, Corollary 1.4 implies that d divides c. Conversely, if $c = de$ for some integer e, then by writing $d = au + bv$ (as in Theorem 1.7) we get $c = aue + bve = ax + by$, where $x = ue$ and $y = ve$ are both integers. Thus the integers of the form $ax + by$ $(x, y \in \mathbb{Z})$ are the multiples of d, and the least positive integer of this form is the least positive multiple of d, namely d itself. □

Example 1.6

We saw in Example 1.3 that if $a = 1492$ and $b = 1066$ then $d = 2$, so the integers of the form $c = 1492x + 1066y$ are the multiples of 2. Example 1.4 gives $2 = 1492.(-5) + 1066.7$, so multiplying through by e we can express any even integer $2e$ in the form $1492x + 1066y$: for instance, $-4 = 1492.10 + 1066.(-14)$.

Definition

Two integers a and b are *coprime* (or *relatively prime*) if $\gcd(a, b) = 1$. For example, 10 and 21 are coprime, but 10 and 12 are not. More generally, a set $a_1, a_2, \ldots$ of integers are *coprime* if $\gcd(a_1, a_2, \ldots) = 1$, and they are *mutually coprime* if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$. If they are mutually coprime then they are coprime (since $\gcd(a_1, a_2, \ldots) | \gcd(a_i, a_j)$), but the converse is false: the integers $6, 10$ and 15 are coprime but are not mutually coprime.

Corollary 1.9

Two integers a and b are coprime if and only if there exist integers x and y such that

$$ax + by = 1\,.$$

Proof

Let $\gcd(a, b) = d$. If we put $c = 1$ in Theorem 1.8, we see that $ax + by = 1$ for some $x, y \in \mathbb{Z}$ if and only if $d|1$, that is, $d = 1$. □

For example, $10.(-2) + 21.1 = 1$, confirming that 10 and 21 are coprime.

Corollary 1.10

If $\gcd(a, b) = d$ then

$$\gcd(ma, mb) = md$$

for every integer $m > 0$, and

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 .$$

Proof

By Theorem 1.8, $\gcd(ma, mb)$ is the smallest positive value of $max + mby = m(ax + by)$, where $x, y \in \mathbb{Z}$, while d is the smallest positive value of $ax + by$, so $\gcd(ma, mb) = md$. Writing $d = au + bv$ and then dividing by d, we have

$$\frac{a}{d}.u + \frac{b}{d}.v = 1 ,$$

so Corollary 1.9 implies that the intergers a/d and b/d are coprime. □

Corollary 1.11

Let a and b be coprime integers.

(a) If $a|c$ and $b|c$ then $ab|c$.

(b) If $a|bc$ then $a|c$.

Proof

(a) We have $ax + by = 1$, $c = ae$ and $c = bf$ for some integers x, y, e and f. Then $c = cax + cby = (bf)ax + (ae)by = ab(fx + ey)$, so $ab|c$.

(b) As in (a), $c = cax + cby$. Since $a|bc$ and $a|a$, Corollary 1.4 implies that $a|(cax + cby) = c$. □

Exercise 1.12

Show that both parts of Corollary 1.11 can fail if a and b are not coprime.

1.3 Least common multiples

Definition

If a and b are integers, then a *common multiple* of a and b is an integer c such that $a|c$ and $b|c$. If a and b are both non-zero, then they have positive common multiples (such as $|ab|$), so by the well-ordering principle they have a *least common multiple* or, more precisely, a least *positive* common multiple; this is the unique positive integer l satisfying

(1) $a|l$ and $b|l$ (so l is a common multiple), and

(2) if $a|c$ and $b|c$, with $c > 0$, then $l \leq c$ (so no positive common multiple is less than l).

We usually denote l by $\text{lcm}(a, b)$, or simply $[a, b]$. For example $\text{lcm}(15, 10) = 30$, since the positive multiples of 15 are $15, 30, 45, \ldots$ while those of 10 are $10, 20, 30, \ldots$. The properties of the least common multiple can be deduced from those of the greatest common divisor, by means of the following result.

Theorem 1.12

Let a and b be positive integers, with $d = \gcd(a, b)$ and $l = \text{lcm}(a, b)$. Then

$$dl = ab\,.$$

(Since $\gcd(a, b) = \gcd(|a|, |b|)$ and $\text{lcm}(a, b) = \text{lcm}(|a|, |b|)$, it is no great restriction to assume $a, b > 0$.)

Proof

Let $e = a/d$ and $f = b/d$, and consider

$$\frac{ab}{d} = \frac{de.df}{d} = def\,.$$

Clearly this is positive, so we can show that it is equal to l by showing that it satisfies conditions (1) and (2) of the definition of $\text{lcm}(a, b)$. First,

$$def = (de)f = af \quad \text{and} \quad def = (df)e = be\,;$$

thus $a|def$ and $b|def$, so (1) is satisfied. Second, suppose that $a|c$ and $b|c$, with $c > 0$; we need to show that $def \leq c$. By Theorem 1.7 there exist integers u and v such that $d = au + bv$. Now

$$\frac{c}{def} = \frac{cd}{(de)(df)} = \frac{cd}{ab} = \frac{c(au + bv)}{ab} = \left(\frac{c}{b}\right)u + \left(\frac{c}{a}\right)v$$

is an integer, since a and b are factors of c; thus $def|c$ and hence (by Exercise 1.3(d)) we have $def \leq c$, as required. □

Example 1.7

If $a = 15$ and $b = 10$, then $d = 5$ and $l = 30$; thus $dl = 150 = ab$, agreeing with Theorem 1.12.

We can use Theorem 1.12 to find $l = \text{lcm}(a, b)$ efficiently by first using Euclid's algorithm to find $d = \gcd(a, b)$, and then calculating $l = ab/d$.

Example 1.8

Since $\gcd(1492, 1066) = 2$ we have $\text{lcm}(1492, 1066) = (1492 \times 1066)/2 = 795236$.

Exercise 1.13

Calculate $\text{lcm}(1485, 1745)$.

Exercise 1.14

Show that c is a common multiple of a and b if and only if it is a multiple of $l = \text{lcm}(a, b)$.

1.4 Linear Diophantine equations

In this book we will consider a number of *Diophantine equations* (named after the 3rd-century mathematician Diophantos of Alexandria): these are equations in one or more variables, for which we seek integer-valued solutions. One of the simplest of these is the *linear Diophantine equation* $ax + by = c$; we can use some of the preceding ideas to find all integer solutions x, y of this equation. The following result was known to the Indian mathematician Brahmagupta, around AD 628:

Theorem 1.13

Let a, b and c be integers, with a and b not both 0, and let $d = \gcd(a, b)$. Then the equation

$$ax + by = c$$

has an integer solution x, y if and only if c is a multiple of d, in which case there are infinitely many solutions. These are the pairs

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d} \qquad (n \in \mathbb{Z}),$$

where x_0, y_0 is any particular solution.

Proof

The fact that there is a solution if and only if $d|c$ is merely a restatement of Theorem 1.8. For the second part of the theorem, let x_0, y_0 be a particular solution, so

$$ax_0 + by_0 = c.$$

If we put

$$x = x_0 + \frac{bn}{d}, \quad y = y_0 - \frac{an}{d}$$

where n is any integer, then

$$ax + by = a\Big(x_0 + \frac{bn}{d}\Big) + b\Big(y_0 - \frac{an}{d}\Big) = ax_0 + by_0 = c,$$

so x, y is also a solution. (Note that x and y are integers since d divides b and a respectively.) This gives us infinitely many solutions, for different integers n. To show that these are the only solutions, let x, y be any integer solution, so $ax + by = c$. Since $ax + by = c = ax_0 + by_0$ we have

$$a(x - x_0) + b(y - y_0) = 0,$$

so dividing by d we get

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{1.1}$$

Now a and b are not both 0, and we can suppose that $b \neq 0$ (if not, interchange the roles of a and b in what follows). Since b/d divides each side of (1.1), and is coprime to a/d by Corollary 1.10, it divides $x - x_0$ by Corollary 1.11(b). Thus $x - x_0 = bn/d$ for some integer n, so

$$x = x_0 + \frac{bn}{d}.$$

Substituting back for $x - x_0$ in (1.1) we get

$$-\frac{b}{d}(y - y_0) = \frac{a}{d}(x - x_0) = \frac{a}{d}.\frac{bn}{d},$$

so dividing by b/d (which is non-zero) we have

$$y = y_0 - \frac{an}{d}.$$

□

Thus we can find the solutions of any linear Diophantine equation $ax+by = c$ by the following method:

(1) Calculate $d = \gcd(a, b)$, either directly or by Euclid's algorithm.

(2) Check whether d divides c: if it does not, there are no solutions, so stop here; if it does, write $c = de$.

(3) If $d|c$, use the method of proof of Theorem 1.7 to find integers u and v such that $au + bv = d$; then $x_0 = ue, y_0 = ve$ is a particular solution of $ax + by = c$.

(4) Now use Theorem 1.13 to find the general solution x, y of the equation.

Example 1.9

Let the equation be

$$1492x + 1066y = -4\,,$$

so $a = 1492$, $b = 1066$ and $c = -4$. In step (1), we use Example 1.3 to see that $d = 2$. In step (2) we check that d divides c: in fact, $c = -2d$, so $e = -2$. In step (3) we use Example 1.4 to write $d = -5.1492 + 7.1066$; thus $u = -5$ and $v = 7$, so $x_0 = (-5).(-2) = 10$ and $y_0 = 7.(-2) = -14$ give a particular solution of the equation. By Theorem 1.13, the general solution has the form

$$x = 10 + \frac{1066n}{2} = 10 + 533n\,, \quad y = -14 - \frac{1492n}{2} = -14 - 746n \qquad (n \in \mathbb{Z}).$$

Exercise 1.15

Find the general solution of the Diophantine equation $1485x + 1745y = 15$.

It is sometimes useful to interpret the linear Diophantine equation $ax+by = c$ geometrically. If we allow x and y to take any real values, then the graph of this equation is a straight line L in the xy-plane. The points (x, y) in the plane with integer coordinates x and y are the *integer lattice-points*, the vertices of a tessellation (tiling) of the plane by unit squares. Pairs of integers x and y satisfying the equation correspond to integer lattice-points (x, y) on L; thus Theorem 1.13 asserts that L passes through such a lattice-point if and only if $d|c$, in which case it passes through infinitely many of them, with the given values of x and y.

Exercise 1.16

If $a_1, \ldots, a_k$ and c are integers, when does the Diophantine equation $a_1x_1 + \cdots + a_kx_k = c$ have integer solutions $x_1, \ldots, x_k$?

1.5 Supplementary exercises

Exercise 1.17

Let us define the *height* $h(a)$ of an integer $a \geq 2$ to be the greatest n such that Euclid's algorithm requires n steps to compute $\gcd(a, b)$ for some positive $b < a$ (that is, $\gcd(a, b) = r_{n-1}$). Show that $h(a) = 1$ if and only if $a = 2$, and find $h(a)$ for all $a \leq 8$.

Exercise 1.18

The *Fibonacci numbers* $f_n = 1, 1, 2, 3, 5, \ldots$ are defined by $f_1 = f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for all $n \geq 1$. Show that $0 \leq f_n < f_{n+1}$ for all $n \geq 2$. What happens if Euclid's algorithm is applied when a and b are a pair of consecutive Fibonacci numbers f_{n+2} and f_{n+1}? Show that $h(f_{n+2}) \geq n$.

Exercise 1.19

Suppose that $a > b > 0$, that Euclid's algorithm computes $\gcd(a, b)$ in n steps, and that a is the smallest integer with this property (that is, if $a' > b' > 0$ and $\gcd(a', b')$ requires n steps, then $a' \geq a$); show that a and b are consecutive Fibonacci numbers $a = f_{n+2}$ and $b = f_{n+1}$ (Lamé's Theorem, 1845).

Exercise 1.20

Show that $h(f_{n+2}) = n$, and f_{n+2} is the smallest integer of this height.

Exercise 1.21

Show that $f_n = (\phi^n - \psi^n)/\sqrt{5}$, where ϕ, ψ are the positive and negative roots of $\lambda^2 = \lambda + 1$. Deduce that $f_n = \{\phi^n/\sqrt{5}\}$, where $\{x\}$ denotes the integer closest to x. Hence obtain the approximate upper bound

$$\log_\phi(a\sqrt{5}) - 2 = \log_\phi(a) + \frac{1}{2}\log_\phi(5) - 2 \approx 4.785 \log_{10}(a) - 0.328$$

for the number of steps required to compute $\gcd(a, b)$ by Euclid's algorithm, where $a \geq b > 0$.

Exercise 1.22

Show that if a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that $a = qb + r$ and $-|b|/2 < r \leq |b|/2$. Use this result instead of Corollary 1.2 to devise an alternative algorithm to Euclid's for calculating greatest common divisors (the *least remainders algorithm*).

Exercise 1.23

Use the least remainders algorithm to compute $\gcd(1066, 1492)$ and $\gcd(1485, 1745)$, and compare the numbers of steps required by this algorithm with those required by Euclid's.

Exercise 1.24

What happens if the least remainders algorithm is applied to a pair of consecutive Fibonacci numbers?

Exercise 1.25

Show that if a and b are coprime positive integers, then every integer $c \geq ab$ has the form $ax + by$ where x and y are non-negative integers. Show that the integer $ab - a - b$ does not have this form.

http://www.springer.com/978-3-540-76197-6

Elementary Number Theory

Jones, G.A.; Jones, J.M.

1998, XIV, 302 p., Softcover
ISBN: 978-3-540-76197-6