2 Show that $0 \leqslant x^2$ for any x in $\mathbb{Z}$, and deduce that $0 \leqslant 1$.

3 Deduce from the previous exercise that $n \leqslant n+1$ for all $n \in \mathbb{Z}$.

It is clear that we can define the other commonly used ordering symbols, $\geqslant$, $<$, and $>$, in terms of the symbol $\leqslant$. For example, $m > n$ must be defined as meaning that $n \leqslant m$ and $m \neq n$. We shall use these symbols as the need for them arises.

It might appear at first sight that we now have all the properties of $\mathbb{Z}$ that are required in mathematics, but, rather surprisingly, one vital axiom is missing. Suppose X is any subset of $\mathbb{Z}$; we say that the integer b is a **lower bound** for X if

$$b \leqslant x \quad \text{for all } x \in X.$$

Some subsets do not have lower bounds: for example, the set of negative integers $-1, -2, -3$, and so on, clearly has no lower bound. On the other hand, the set S denoted by the bold numbers in Fig. 1.1 has many lower bounds. A quick glance tells us that -40, for instance, is a lower bound, while a closer inspection reveals that -27 is the 'best' lower bound, since it actually belongs to S. In general, a lower bound for a set X which is itself a member of X is known as a **least member** for X.

90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9
−10	−9	−8	−7	−6	−5	−4	−3	−2	−1
−20	−19	−18	−17	−16	−15	−14	−13	−12	−11
−30	−29	−28	−27	−26	−25	−24	−23	−22	−21
−40	−39	−38	−37	−36	−35	−34	−33	−32	−31

Fig. 1.1
The least member of S is -27.

Our final axiom for $\mathbb{Z}$ asserts what is (apparently) an obvious property.

I13. If X is a subset of $\mathbb{Z}$ which is not empty and has a lower bound, then X has a least member.

Axiom **I13** is known as the **well-ordering axiom**. A good way to grasp its meaning is to consider a game in which two people alternately choose a member of X, subject to the rule that each number must be strictly less than the previous one. The axiom tells us that, when the numbers are required to be integers, the game will end; indeed the end occurs as soon as one of the players has the good sense to choose the least member. This apparently obvious property does *not* necessarily hold when we allow numbers which are not integers, because X might not have a least member even though it has a lower bound. For example, suppose X is the set of fractions $\frac{3}{2}, \frac{4}{3}, \frac{5}{4}$, and so on, having the general form $(n+1)/n$ $(n \geqslant 2)$. This set has a lower bound (1, for instance) but it has no least member, and so the players can go on playing for ever, choosing fractions closer and closer to 1.

The well-ordering axiom provides firm justification for our intuitive picture of the integers as a set of regularly spaced points on a straight line, extending indefinitely in either direction (Fig. 1.2). In particular, it says that we cannot get closer and closer to an integer without actually arriving, so that the picture in Fig. 1.3 is wrong.

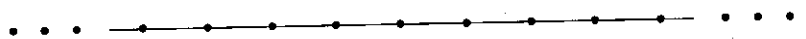


Fig. 1.2
The correct intuitive picture of $\mathbb{Z}$.

Fig. 1.3
An incorrect picture of $\mathbb{Z}$.

The fact that there are gaps between the integers leads us to say that the set $\mathbb{Z}$ is *discrete*, and it is this property which gives rise to the name 'discrete mathematics'. In calculus and analysis limiting processes are of fundamental importance, and it is essential to use number systems which are *continuous*, rather than discrete.

Exercises 1.2 (continued)

4 In each of the following cases say whether or not the set X has a lower bound, and if it has a lower bound, find its least member.

(i) $X=\{x\in\mathbb{Z}\mid x^2\leqslant 16\}$.
(ii) $X=\{x\in\mathbb{Z}\mid x=2y \text{ for some } y\in\mathbb{Z}\}$.
(iii) $X=\{x\in\mathbb{Z}\mid x^2\leqslant 100x\}$.

5 A subset Y of Z is said to have an **upper bound** c if $c\geqslant y$ for all $y\in Y$. An upper bound which is also a member of Y is said to be a **greatest member** of Y. Use Axiom **I13** to show that if Y is not empty and it has an upper bound, then it has a greatest member. [Hint: apply the axiom to the set whose members are $-y$ $(y\in Y)$.]

6 The integers n satisfying $1\leqslant n\leqslant 25$ are arranged in a square array of five rows and five columns in an arbitrary way. The greatest member of each row is selected, and s denotes the least of these. Similarly, the least member in each column is selected, and t denotes the greatest of these. Show that $s\geqslant t$, and give an example in which $s\neq t$.

1.3 Recursive definitions

Let $\mathbb{N}$ denote the set of positive integers, that is

$$\mathbb{N}=\{n\in\mathbb{Z}\mid n\geqslant 1\},$$

and let $\mathbb{N}_0$ denote the set $\mathbb{N}\cup\{0\}$, that is

$$\mathbb{N}_0=\{n\in\mathbb{Z}\mid n\geqslant 0\}.$$

If X is a subset of $\mathbb{N}$ (or $\mathbb{N}_0$) then it automatically has a lower bound, since each member x of X satisfies $x\geqslant 1$ (or $x\geqslant 0$). Thus in this case the well-ordering axiom takes the form

if X is a non-empty subset of $\mathbb{N}$ or $\mathbb{N}_0$
then X has a least member.

This is the form which is most often used in practice.

Our first use of the well-ordering axiom will be to justify a very common procedure. Frequently we encounter an expression of the form u_n, where n indicates any positive integer: for example, we might have $u_n=3n+2$, or $u_n=(n+1)(n+2)(n+3)$. In these examples u_n is given by an explicit formula and there is no difficulty in

explaining how u_n is to be calculated when n is given a specific value. However, in many cases we do not know a formula for u_n; indeed our problem may be to find one. In such cases we may be given some values of u_n for small positive integers n, and a relationship between the general u_n and some of the u_r for $r<n$.

For example, suppose we are given that

$$u_1=1,\qquad u_2=2,\qquad u_n=u_{n-1}+u_{n-2}\qquad (n\geqslant 3).$$

To calculate the values of u_n for all n in $\mathbb{N}$ we could proceed as follows:

$$u_3=u_2+u_1=2+1=3,$$
$$u_4=u_3+u_2=3+2=5,$$
$$u_5=u_4+u_3=5+3=8,$$

and so on. This is an example of a *recursive definition*. It is plainly 'obvious' that the method will give a unique value of u_n for every positive integer n. But strictly speaking we need the well-ordering axiom to justify this conclusion, along the following lines.

Suppose there is a positive integer n for which u_n is not uniquely defined. Then, by the well-ordering axiom there is a least positive integer m with this property. Since u_1 and u_2 are specified explicitly, m is not 1 or 2, and the equation $u_m=u_{m-1}+u_{m-2}$ is applicable. By the definition of m, u_{m-1} and u_{m-2} are uniquely defined, and the equation gives a unique value of u_m, contrary to hypothesis. The contradiction arises from the assumption that u_n is not well-defined for some n, and hence this assumption must be false.

The reader should not be dismayed by the use of such contorted arguments to establish something which is 'obviously' true. In the first place, we shall not labour these points unduly, and in the second place, the fact that the result is 'obvious' simply means that we are working with the correct mental picture of the sets $\mathbb{N}$ and $\mathbb{Z}$. Once we have established that picture on a firm foundation we can set out to extend it and obtain results which may not be quite so 'obvious'.

The method of recursive definition will occur very often in the rest of the book. There are other forms of the procedure which are usually concealed by the notation. What do we mean by the following expressions?

$$\sum_{r=1}^{n}2r-1,\qquad 1+3+5+\cdots+(2n-1).$$

It is clearly not enough to say that each one means the same as the

other, since each one contains a mysterious symbol, Σ and $\cdots$, respectively. What we should say is that each of them is equal to the expression s_n given by the following recursive definition:

$$s_1 = 1, \qquad s_n = s_{n-1} + (2n-1) \quad (n \geqslant 2).$$

This makes it clear that both mysterious symbols are really a form of shorthand for a recursive definition, and that consequently the expressions are properly defined for each n in $\mathbb{N}$.

Similar remarks apply to the definition of products such as $n!$ (spoken as *n factorial*). If we say that

$$n! = \prod_{i=1}^{n} i, \quad \text{or} \quad n! = 1 \times 2 \times 3 \times \cdots \times n,$$

then the meaning may be clear to everyone. But to be precise (and to make it clear to a computer) we should use the recursive definition

$$1! = 1, \qquad n! = n \times (n-1)! \quad (n \geqslant 2).$$

Exercises 1.3

1 In the following cases calculate (where possible) the values of u_1, u_2, u_3, u_4, and u_5 given by the equations. If you cannot calculate the values explain why the definition is faulty.

(i) $u_1 = 1, \quad u_2 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geqslant 3).$

(ii) $u_1 = 1, \quad u_n = u_{n-1} + 2u_{n-2} \quad (n \geqslant 2).$

(iii) $u_1 = 0, \quad u_n = nu_{n-1} \quad (n \geqslant 2).$

2 Give a recursive definition of the 'nth power' 2^n for all $n \geqslant 1$.

3 Suppose u_n is defined by the equations

$$u_1 = 2, \qquad u_n = 2^{u_{n-1}} \quad (n \geqslant 2).$$

What is the least value of n for which it is not practicable to calculate u_n using a pocket calculator?

4 Write down explicit formulae for the expressions u_n defined by the following equations.

(i) $u_1 = 1, \quad u_n = u_{n-1} + 3 \quad (n \geqslant 2).$

(ii) $u_1 = 1, \quad u_n = n^2 u_{n-1} \quad (n \geqslant 2).$

1.4 The principle of induction

Suppose we are asked to prove the result

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

In other words, we have to show that the expression defined recursively on the left is equal to that defined explicitly by the formula on the right, for all positive integers n. We might proceed as follows.

The formula is certainly correct when $n = 1$, since $1 = 1^2$. Suppose it is correct for a specific value of n, say $n = k$, so that

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

We can use this fact to simplify the left-hand side when $n = k+1$, as follows:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k+1) &= 1 + 3 + 5 + \cdots + (2k-1) + (2k+1) \\ &= k^2 + (2k+1) \\ &= (k+1)^2. \end{aligned}$$

So if the result is correct when $n = k$ then it is correct when $n = k+1$. Now we began by remarking that it is correct when $n = 1$, hence it must be correct when $n = 2$. By the same argument, since it is correct when $n = 2$ it must be correct when $n = 3$. Continuing in this way we see that it is correct for all positive integers n.

The essence of this argument is often referred to as the *principle of induction*. It is a powerful technique, easy to apply, and we shall use it frequently. But first we should examine its logical basis, and in order to do so, a more general formulation is needed.

Let S denote the subset of $\mathbb{N}$ for which the result is correct: of course, our aim is to prove that S is the whole set $\mathbb{N}$. The first step is to show that 1 is in S, and then we show that if k is in S so is $k+1$. Then we huff and puff (Fig. 1.4) and conclude that $S = \mathbb{N}$. Fortunately the huffing and puffing is not essential, because the principle of induction is a consequence of the axioms for $\mathbb{Z}$ and $\mathbb{N}$ that have been so carefully chosen. Specifically, it is a consequence of the well-ordering axiom.

Theorem 1.4

Suppose that S is a subset of $\mathbb{N}$ satisfying the conditions

(i) $1 \in S$,

(ii) for each $k \in \mathbb{N}$, if $k \in S$ then $k+1 \in S$.

Then it follows that $S = \mathbb{N}$.

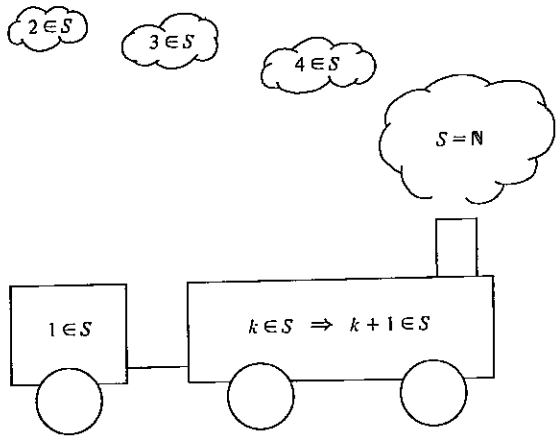


Fig. 1.4
The principle of induction.

Proof If the conclusion is false, $S \neq \mathbb{N}$ and the complementary set $\bar{S}$ defined by

$$\bar{S} = \{r \in \mathbb{N} \mid r \notin S\}$$

is not empty. By the well-ordering axiom, $\bar{S}$ has a least member m. Since 1 belongs to S, $m \neq 1$. It follows that $m-1$ is in $\mathbb{N}$, and since m is the least member of $\bar{S}$, $m-1$ must be in S. Then putting $k = m-1$ in condition (ii) we conclude that m is in S, which contradicts the assertion that m is in $\bar{S}$. Thus the statement that $S \neq \mathbb{N}$ leads to an absurdity, so we must have $S = \mathbb{N}$. □

In practice, we usually present a 'proof by induction' in rather more descriptive terms. The fact that the result is true when $n = 1$ is called the *induction basis*, and the assumption that it is true when $n = k$ is called the *induction hypothesis*. When these terms are used there is no need to introduce the set S explicitly.

Example The integer x_n is defined recursively by

$$x_1 = 2 \quad \text{and} \quad x_n = x_{n-1} + 2n \quad (n \geqslant 2).$$

Show that

$$x_n = n(n+1) \quad \text{for all } n \in \mathbb{N}.$$

Solution (*Induction basis*) The result is true when $n = 1$ since $2 = 1 \times 2$.
(*Induction hypothesis*) Suppose the result is true when $n = k$, that is,

$x_k = k(k+1)$. Then

$$\begin{aligned} x_{k+1} &= x_k + 2(k+1) && \text{(by recursive definition)} \\ &= k(k+1) + 2(k+1) && \text{(by induction hypothesis)} \\ &= (k+1)(k+2). \end{aligned}$$

So the result is true when $n = k+1$, and by the principle of induction, it is true for all positive integers n. □

There are several modified forms of the principle of induction. Sometimes it is convenient to take for the induction basis the value $n = 0$; on the other hand it may be appropriate to take a value like 2 or 3, since the first few cases may be exceptional. Each problem must be treated on its merits. Another useful modification is to take as induction hypothesis the assumption that the result is true for *all* relevant values $n \leqslant k$, rather than for $n = k$ alone. (This formulation is sometimes called the *strong* induction principle.) All these modifications can be justified by trivial changes in the proof of Theorem 1.4, as indicated in Ex. 1.4.6.

Exercises 1.4

1 Use the principle of induction to prove that

$$1^2 + 2^2 + \cdots + n^2 = \tfrac{1}{6}n(n+1)(2n+1)$$

for all positive integers n.

2 Make a table of values of

$$S_n = 1^3 + 2^3 + 3^3 + \cdots + n^3$$

for $1 \leqslant n \leqslant 6$. On the basis of your table suggest a formula for S_n. [Hint: the values of S_n are perfect squares.] Use the principle of induction to establish that the formula is correct for all $n \geqslant 1$. (If the method fails, your formula is wrong!)

3 Use the strong form of the principle of induction to show that if u_n is defined recursively by the rules

$$u_1 = 3, \qquad u_2 = 5, \qquad u_n = 3u_{n-1} - 2u_{n-2} \quad (n \geqslant 3),$$

then $u_n = 2^n + 1$ for all positive integers n.

4 Find the least positive integer n_0 for which it is true that $n! \geqslant 2^n$. Taking the case $n = n_0$ as the induction basis, show that the result holds for all $n \geqslant n_0$.

5 In the following cases find the appropriate value of n_0 for the induction basis and show that the statement is true for all $n \geqslant n_0$.

(i) $n^2+6n+8 \geqslant 0$; (ii) $n^3 \geqslant 6n^2$.

6 The following theorem incorporates all the modifications of the basic principle of induction outlined above.

Theorem 1.4* Suppose n_0 is any integer (not necessarily positive), and let X denote the set of integers $n \geqslant n_0$. Let S be a subset of X satisfying the conditions

(i) $n_0 \in S$,
(ii) if $x \in S$ for all x in the range $n_0 \leqslant x \leqslant k$ then $k+1 \in S$.

Then it follows that $S = X$.

Write out the proof of Theorem 1.4, and make the changes needed in order to prove Theorem 1.4*.

1.5 Quotient and remainder

As children we learn that when 6 'goes into' 27 the *quotient* is 4 and the *remainder* is 3, that is,

$$27 = 6 \times 4 + 3.$$

The important point is that the remainder must be less than 6. Although it is also true that, for instance

$$27 = 6 \times 3 + 9,$$

we are told that we must take the least value for the remainder, so that the amount 'left over' is as small as possible. The fact that the set of possible 'remainders' does have a least member is a consequence of the well-ordering axiom.

Theorem 1.5 If we are given integers a and b with $b \in \mathbb{N}$, then there are integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leqslant r < b.$$

Proof We shall apply the well-ordering axiom to the set of 'remainders'

$$R = \{x \in \mathbb{N}_0 \mid a = by + x \text{ for some } y \in \mathbb{Z}\}.$$

First we show that R is not empty. If $a \geqslant 0$ the identity

$$a = b0 + a$$

shows that $a \in R$, while if $a < 0$ the identity

$$a = ba + (1-b)a$$

shows that $(1-b)a \in R$. (In both cases it is necessary to check that the stated member of R is non-negative.)

Now, since R is a non-empty subset of $\mathbb{N}_0$, it has a least member r, and since r is in R it follows that $a = bq + r$ for some q in $\mathbb{Z}$. Furthermore

$$a = bq + r \quad \Rightarrow \quad a = b(q+1) + (r-b)$$

so that if $r \geqslant b$ then $r-b$ is in R. But $r-b$ is less than r, contrary to the definition of r as the least member of R. Since the assumption $r \geqslant b$ leads to a contradiction we must have $r < b$, as required. □

It is easy to see that the quotient q and the remainder r obtained in the theorem are unique. For suppose that q' and r' also satisfy the conditions, that is

$$a = bq' + r' \quad \text{and} \quad 0 \leqslant r' < b.$$

If $q' < q$ then $q - q' \geqslant 1$ so that we have

$$r' = a - bq' = (a - bq) + b(q - q') \geqslant r + b.$$

Since $r + b \geqslant b$, it follows that $r' \geqslant b$ contradicting the second property of r'. Hence the assumption $q' < q$ is false. The same argument with q and q' interchanged shows that $q < q'$ is false. So we must have $q = q'$, and consequently $r = r'$ also, since

$$r = a - bq = a - bq' = r'.$$

One important consequence of Theorem 1.5 is that it justifies our usual method of representing integers. Let $t \geqslant 2$ be a given integer, called the **base** for calculation. For any positive integer x we have, by repeated application of Theorem 1.5,

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\cdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Here each remainder r_i is one of the integers $0, 1, \ldots, t-1$, and we

stop when $q_n = 0$. Eliminating the quotients q_i we obtain

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0.$$

We have represented x (with respect to the base t) by the sequence of remainders, and we write $x = (r_n r_{n-1} \cdots r_1 r_0)_t$. Conventionally $t = 10$ is the base for calculations done by hand, and we omit the subscript, so we have the familiar notation

$$1984 = (1 \times 10^3) + (9 \times 10^2) + (8 \times 10) + 4.$$

This positional notation requires symbols only for the integers $0, 1, \ldots, t-1$. When $t = 2$ it is particularly suited for machine calculations, since the symbols 0 and 1 can be represented physically by the absence or presence of a pulse of electricity or light.

Example What is the representation in base 2 of $(109)_{10}$?

Solution Dividing repeatedly by 2 we obtain

$$\begin{aligned} 109 &= 2 \times 54 + 1 \\ 54 &= 2 \times 27 + 0 \\ 27 &= 2 \times 13 + 1 \\ 13 &= 2 \times 6 + 1 \\ 6 &= 2 \times 3 + 0 \\ 3 &= 2 \times 1 + 1 \\ 1 &= 2 \times 0 + 1. \end{aligned}$$

Hence

$$(109)_{10} = (1101101)_2.$$ □

Exercises 1.5

1 Find q and r satisfying Theorem 1.5 when

(i) $a = 1001$, $b = 11$; (ii) $a = 12345$, $b = 234$.

2 Find the representations of $(1985)_{10}$ in base 2, in base 5, and in base 11.

3 Find the usual (base 10) representations of

(i) $(11011101)_2$; (ii) $(4165)_7$.

1.6 Divisibility

Given any two integers x and y we say that y is a **divisor** of x, and write $y \mid x$, if

$$x = yq \quad \text{for some } q \in \mathbb{Z}.$$

We also say that y is a **factor** of x, that y **divides** x, that x is **divisible** by y, and that x is a **multiple** of y.

When $y \mid x$ we can use the symbol $\frac{x}{y}$ (or x/y) to denote the integer q such that $x = yq$. When y is not a divisor of x we have to assign a new meaning to the fraction x/y, since it is not an integer. The reader is undoubtedly familiar with rules for dealing with fractions, and we shall use those rules from time to time, but it is important to remember that fractions have not yet been formally defined within the framework of this book. It is even more important to remember that x/y is not a member of $\mathbb{Z}$ unless y divides x.

Example Show that if c, d, and n are integers such that

$$d \mid n \quad \text{and} \quad c \mid \frac{n}{d}$$

then

$$c \mid n \quad \text{and} \quad d \mid \frac{n}{c}.$$

Solution Since $d \mid n$ there is an integer s such that $n = ds$, and n/d denotes the integer s. Since $c \mid n/d$ there is an integer t such that

$$s = \frac{n}{d} = ct.$$

It follows that

$$n = ds = d(ct) = c(dt)$$

so that $c \mid n$ and n/c denotes the integer dt. Finally, since $n/c = dt$ we have $d \mid n/c$, as required. □

Exercises 1.6

1 Prove that $x \mid 0$ for every $x \in \mathbb{Z}$, but $0 \mid x$ only when $x = 0$.

2 Show that if $c \mid a$ and $c \mid b$, then $c \mid xa + yb$ for any integers x, y.

3 Show that if a and b are integers such that $ab = 1$ then $a = b = 1$ or $a = b = -1$. [Hint: either both a and b are positive or both are negative.] Deduce that if x and y are integers such that $x|y$ and $y|x$ then $x = y$ or $x = -y$.

4 Use the principle of induction to prove that, for all $n \geqslant 0$,

(i) n^2+3n is divisible by 2; (ii) n^3+3n^2+2n is divisible by 6.

1.7. The greatest common divisor

If a and b are integers we say that the integer d is a **greatest common divisor**, or **gcd**, of a and b if

(i) $d|a$ and $d|b$; (ii) if $c|a$ and $c|b$, then $c|d$.

Condition (i) says that d is a common divisor of a and b, and condition (ii) says that any common divisor of a and b is also a divisor of d. For example, 6 is a common divisor of 60 and 84, but it is *not* a greatest common divisor, since $12|60$ and $12|84$ but $12 \nmid 6$. (The symbol $\nmid$ means 'does not divide'.)

Conditions (i) and (ii) are not quite sufficient to ensure that two given integers have a unique gcd. For if d and d' both satisfy both conditions it follows that

$$d|d' \quad \text{and} \quad d'|d.$$

Hence, by Ex. 1.6.3, $d = d'$ *or* $d = -d'$. Thus, in order to get a unique gcd it is sufficient to impose a third condition:

(iii) $d \geqslant 0$.

We say that the unique integer d satisfying (i), (ii), and (iii) is *the* gcd of a and b, and write $d = \gcd(a, b)$. For example, $12 = \gcd(60, 84)$.

There is a very famous method for calculating the gcd of two given integers, based on the quotient and remainder technique. It depends on the fact that

$$a = bq + r \quad \Rightarrow \quad \gcd(a, b) = \gcd(b, r).$$

In order to prove this we remark that if d divides a and b then it surely divides $a - bq$; and $a - bq = r$, so d divides r. Thus any common divisor of a and b is also a common divisor of b and r. Conversely, if d divides b and r it also divides $a = bq + r$. Repeated

application of this simple fact provides the method for calculating the gcd.

Example Find the gcd of 2406 and 654.

Solution We have

$$\begin{aligned}
\gcd(2406, 654) &= \gcd(654, 444) && \text{since} \quad 2406 = 654\times 3 + 444,\\
&= \gcd(444, 210) && \text{since} \quad 654 = 444\times 1 + 210,\\
&= \gcd(210, 24) && \text{since} \quad 444 = 210\times 2 + 24,\\
&= \gcd(24, 18) && \text{since} \quad 210 = 24\times 8 + 18,\\
&= \gcd(18, 6) && \text{since} \quad 24 = 18\times 1 + 6,\\
&= 6 && \text{since} \quad 18 = 6\times 3.
\end{aligned}$$

□

In general, in order to calculate the gcd of integers a and b (both $\geqslant 0$) we define q_i and r_i recursively by the equations

$$\begin{aligned}
a &= bq_1 + r_1 \quad (0 \leqslant r_1 < b)\\
b &= r_1q_2 + r_2 \quad (0 \leqslant r_2 < r_1)\\
r_1 &= r_2q_3 + r_3 \quad (0 \leqslant r_3 < r_2)\\
&\cdots
\end{aligned}$$

It is clear that the process must stop eventually, since each remainder r_i is strictly less than the preceding one. So the final steps are as follows:

$$\begin{aligned}
r_{k-4} &= r_{k-3}q_{k-2} + r_{k-2} \quad (0 \leqslant r_{k-2} < r_{k-3})\\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} \quad (0 \leqslant r_{k-1} < r_{k-2})\\
r_{k-2} &= r_{k-1}q_k,
\end{aligned}$$

where r_k vanishes, and the required gcd is r_{k-1}. This procedure is known as the **Euclidean algorithm**, after the Greek mathematician Euclid (c. 300 BC). It is extremely useful in practice, and has important theoretical consequences.

Theorem 1.7 Let a and b be integers with $b \geqslant 0$, and let $d = \gcd(a, b)$. Then there are integers m and n such that

$$d = ma + nb.$$

Proof According to the calculation given above $d = r_{k-1}$, and using the penultimate equation we have

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Thus d can be written in the form $m'r_{k-2}+n'r_{k-3}$, where $m'=-q_{k-1}$ and $n'=1$. Substituting for r_{k-2} in terms of r_{k-3} and r_{k-4} we obtain

$$d=m'(r_{k-4}-r_{k-3}q_{k-2})+n'r_{k-3}$$

which can be written in the form $m''r_{k-3}+n''r_{k-4}$, with $m''=n'-m'q_{k-2}$ and $n''=m'$. Continuing in this way we eventually obtain an expression for d in the required form. □

For example, from the calculation used to find the gcd of 2406 and 654 we obtain

$$\begin{aligned}
6 &= \mathbf{24}-\mathbf{18}\times 1 = 1\times\mathbf{24}+(-1)\times\mathbf{18}\\
&= \mathbf{24}+(-1)\times(\mathbf{210}-\mathbf{24}\times 8)=(-1)\times\mathbf{210}+9\times\mathbf{24}\\
&= -\mathbf{210}+9\times(\mathbf{444}-\mathbf{210}\times 2)=9\times\mathbf{444}+(-19)\times\mathbf{210}\\
&= 9\times\mathbf{444}+(-19)\times(\mathbf{654}-\mathbf{444}\times 1)=(-19)\times\mathbf{654}+28\times\mathbf{444}\\
&= (-19)\times\mathbf{654}+28\times(\mathbf{2406}-\mathbf{654}\times 3)=28\times\mathbf{2406}+(-103)\times\mathbf{654}.
\end{aligned}$$

Thus the required expression $d=ma+nb$ is

$$6=28\times 2406+(-103)\times 654.$$

If $\gcd(a,b)=1$ then we say that a and b are **coprime**, and in this case Theorem 1.7 asserts that there are integers m and n such that

$$ma+nb=1.$$

This remark is very useful. For example, we are all familiar with the idea that a fraction can be reduced to its 'lowest terms', that is, to the form a/b with a and b coprime. The following *Example* establishes that this form is unique, and, as we shall see, the key fact in the proof is that we can express 1 as $ma+nb$.

Example Suppose that a, a', b, b' are positive integers satisfying

$$\text{(i)}\quad ab'=a'b; \qquad \text{(ii)}\quad \gcd(a,b)=\gcd(a',b')=1.$$

Then $a=a'$ and $b=b'$.

(Condition (i) could be written as $a/b=a'/b'$, but we prefer to use a form which does not assume anything about fractions.)

Solution Since $\gcd(a,b)=1$ there are integers m and n such that $ma+nb=1$. Consequently

$$b'=(ma+nb)b'=mab'+nbb'=(ma'+nb')b,$$

and so $b\mid b'$. By a similar argument using the fact that $\gcd(a',b')=1$, we deduce that $b'\mid b$. Hence either $b=b'$ or $b=-b'$, and since b and b' are both positive we must have $b=b'$. Now (i) yields $a=a'$ and the result is proved. □

Exercises 1.7

1 Find the gcd of 721 and 448 and express it in the form $721m+448n$ with $m, n\in\mathbb{Z}$.

2 Show that if there are integers m and n such that $mu+nv=1$, then $\gcd(u,v)=1$.

3 Use Theorem 1.7 and Ex. 2 to prove that if $\gcd(a,b)=d$, then

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

4 Let a and b be positive integers and let $d=\gcd(a,b)$. Prove that there are integers x and y which satisfy the equation $ax+by=c$ if and only if $d\mid c$.

5 Find integers x and y satisfying

$$966x+686y=70.$$

1.8 Factorization into primes

A positive integer p is said to be a **prime** if $p\geqslant 2$ and the only positive integers which divide p are 1 and p itself. Thus an integer $m\geqslant 2$ is not a prime if and only if we can write $m=m_1m_2$, where m_1 and m_2 are integers strictly between 1 and m.

We remark that according to the definition 1 is *not* a prime. The first few primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

The reader is almost certainly familiar with the idea that any positive integer can be expressed as a product of primes; for example,

$$825=3\times 5\times 5\times 11.$$

The existence of such a *prime factorization* for any positive integer $n\geqslant 2$ is a consequence of the well-ordering axiom. For let B be the set of positive integers $n\geqslant 2$ which do *not* have a prime factorization; if B is not empty then, by the well-ordering axiom, it has a

least member m. If m were a prime p we should have the trivial prime factorization $m = p$; thus m is not a prime and $m = m_1 m_2$ where $1 < m_1 < m$ and $1 < m_2 < m$. Since m is supposed to be the least integer ($\geqslant 2$) which has no prime factorization, both m_1 and m_2 do have prime factorizations. But then the equation $m = m_1 m_2$ yields a prime factorization of m, contradicting the assumption that m is a member of B. Hence B must be empty, and the assertion is proved.

Exercises 1.8

1 Find all the primes p in the range $100 \leqslant p \leqslant 120$.

2 Write down prime factorizations of 201, 1001, and 201000.

3 Show that if p and p' are primes, and $p \mid p'$, then $p = p'$.

4 Show that if $n \geqslant 2$ and n is not prime then there is a prime p such that $p \mid n$ and $p^2 \leqslant n$.

5 Use the result of Ex. 4 to show that if 467 were not prime then it would have a prime divisor $p \leqslant 19$. Deduce that 467 is prime.

The ease with which we establish the existence of prime factorizations conceals two important difficulties. First, the problem of finding the prime factors is by no means straightforward; and secondly, it is not obvious that there is a *unique* prime factorization for any given integer $n \geqslant 2$. The next result is a key step in the proof of uniqueness.

Theorem 1.8.1 If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that

$$p \mid x_1 x_2 \ldots x_n$$

then $p \mid x_i$ for some x_i $(1 \leqslant i \leqslant n)$.

Proof We use the principle of induction. The result is manifestly true when $n = 1$ (induction basis). For the induction hypothesis, suppose it is true when $n = k$.

Suppose that $p \mid x_1 x_2 \ldots x_k x_{k+1}$, and let $x = x_1 x_2 \ldots x_k$. If $p \mid x$ then, by the induction hypothesis, $p \mid x_i$ for some x_i in the range $1 \leqslant i \leqslant k$. If $p \nmid x$ then (since p has no divisors except 1 and itself) we have $\gcd(p, x) = 1$. By Theorem 1.7 there are integers r and s such that $rp + sx = 1$. Hence we have

$$x_{k+1} = (rp + sx)x_{k+1} = (rx_{k+1})p + s(xx_{k+1}),$$

and since p divides both terms it follows that $p \mid x_{k+1}$. Thus in either case p divides one of the x_i $(1 \leqslant i \leqslant k+1)$, and by the principle of induction the result is true for all positive integers n. □

A very common error is to assume that Theorem 1.8.1 remains true when the prime p is replaced by an arbitrary integer. But that is clearly absurd: for example

$$6 \mid 3 \times 8 \quad \text{but} \quad 6 \nmid 3 \quad \text{and} \quad 6 \nmid 8.$$

Examples like this help us to understand that Theorem 1.8.1 expresses a very significant property of primes. Indeed, we shall see that this property plays a crucial part in the next result, which is sometimes called the *Fundamental theorem of arithmetic.*

Theorem 1.8.2 The prime factorization of a positive integer $n \geqslant 2$ is unique, apart from the order of the prime factors.

Proof By the well-ordering axiom, if there is an integer for which the theorem is false, then there is a least such integer $n_0 \geqslant 2$. Suppose then that

$$n_0 = p_1 p_2 \ldots p_k \quad \text{and} \quad n_0 = p'_1 p'_2 \ldots p'_l,$$

where the p_i $(1 \leqslant i \leqslant k)$ are primes, not necessarily distinct, and the p'_j $(1 \leqslant j \leqslant l)$ are primes, not necessarily distinct. The first equation implies that $p_1 \mid n_0$, and the second equation implies that $p_1 \mid p'_1 p'_2 \ldots p'_l$. Hence, by Theorem 1.8.1, p_1 divides p'_j for some j $(1 \leqslant j \leqslant l)$. By re-ordering the second factorization we may assume that $p_1 \mid p'_1$, and since p_1 and p'_1 are primes, it follows that $p_1 = p'_1$ (Ex. 1.8.3). So, by Axiom **I7**, we may cancel the equal factors p_1 and p'_1, and obtain

$$p_2 p_3 \ldots p_k = p'_2 p'_3 \ldots p'_l = n_1, \text{ say.}$$

But the factorizations of n_0 were alleged to be different, and we have cancelled only the equal factors p_1 and p'_1, so n_1 has two different prime factorizations. This contradicts the definition of n_0 as the least such integer. Hence the theorem is true for all $n \geqslant 2$. □

In practice we often collect equal primes in the factorization of n and write

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}.$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ are positive integers. For example, $7000 = 2^3 \times 5^3 \times 7$.

Example Show that if m and n are integers such that $m \geqslant 2$ and $n \geqslant 2$, then $m^2 \neq 2n^2$.

Solution Suppose that the prime factorization of n contains the prime 2 raised to the power x (where x is zero if 2 is not a prime factor of n). Then $n = 2^x h$, where h is a product of primes greater than 2, so

$$2n^2 = 2(2^x h)^2 = 2^{2x+1} h^2.$$

Thus 2 is raised to an *odd* power in the prime factorization of $2n^2$.

On the other hand, if $m = 2^y g$, where g is a product of primes greater than 2, then

$$m^2 = (2^y g)^2 = 2^{2y} g^2,$$

so 2 is raised to an *even* power (possibly zero) in the prime factorization of m^2. It follows that if $m^2 = 2n^2$ we should have two different prime factorizations of the same integer, contrary to Theorem 1.8.2. Hence $m^2 \neq 2n^2$. □

It is clear that the conclusion of the *Example* holds if we allow either or both of m and n to be 1. So we may express the result by saying that there are no positive integers m and n such that

$$\left(\frac{m}{n}\right)^2 = 2$$

or equivalently, by saying that the square root of 2 cannot be expressed as a fraction m/n.

Exercises 1.8 (continued)

6 Let m and n be positive integers whose prime factorizations are

$$m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \ldots p_r^{f_r}.$$

Show that the gcd of m and n is $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ where, for each i in the range $1 \leqslant i \leqslant r$, k_i is the smaller of e_i and f_i.

7 Show that if m and n are positive integers, such that $m \geqslant 2$, $n \geqslant 2$, and $m^2 = kn^2$, then k is the square of an integer.

8 Use the identity

$$2^{rs} - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + \cdots + 2^r + 1)$$

to show that if $2^n - 1$ is prime then n is prime.

9 Find the least value of n for which the converse of Ex. 8 is false: that is, n is prime but $2^n - 1$ is not.

1.9 Miscellaneous Exercises

1 Use the principle of induction to show that $2^n > n + 1$ for all integers $n \geqslant 2$.

2 Show that

$$1^4 + 2^4 + \cdots + n^4 = \tfrac{1}{30} n(n+1)(2n+1)(3n^2 + 3n - 1).$$

3 Show that $4^{2n} - 1$ is divisible by 15 for all integers $n \geqslant 1$.

4 Find the gcd of 1320 and 714, and express the result in the form $1320x + 714y$ $(x, y \in \mathbb{Z})$.

5 Show that 725 and 441 are coprime and hence find integers x and y such that $725x + 441y = 1$.

6 Find a solution in integers to the equation

$$325x + 26y = 91.$$

7 The integer f_n is defined recursively by the equations

$$f_1 = 1, \qquad f_2 = 1, \qquad f_{n+1} = f_n + f_{n-1} \quad (n \geqslant 2).$$

Prove that $\gcd(f_{n+1}, f_n) = 1$ for all $n \geqslant 1$.

8 Let a and b be any two positive integers. Define the **least common multiple** of a and b to be the integer

$$l = \frac{ab}{\gcd(a, b)}.$$

Show that

(i) $a \mid l$ and $b \mid l$;
(ii) if m is a positive integer such that $a \mid m$ and $b \mid m$, then $l \mid m$.

9 Establish the following properties of the gcd.

(i) $\gcd(ma, mb) = m \gcd(a, b)$.
(ii) If $\gcd(a, x) = d$, and $\gcd(b, x) = 1$, then $\gcd(ab, x) = d$.

10 You have an unlimited supply of water, a drain, a large container, and two jugs which contain 7 litres and 9 litres respectively. How would you arrange to put one litre of water in the container? Explain the relationship between your method and Theorem 1.7.

11 By following the outline of the definition of gcd (a, b), frame a definition of the gcd of n integers $a_1, a_2, \ldots, a_n$. Prove that if $d = \gcd(a_1, a_2, \ldots, a_n)$ then there are integers $x_1, x_2, \ldots, x_n$ such that

$$d = x_1a_1 + x_2a_2 + \cdots + x_na_n.$$

12 Let n be a positive integer with the following properties:

(i) n is square-free (that is, the prime factorization of n has no repeated factors);
(ii) for all primes p, $p \mid n$ if and only if $p-1 \mid n$.

Find the value of n.

13 The integer u_n is defined by the equations

$$u_1 = 2, \qquad u_{n+1} = u_n^2 - u_n + 1 \quad (n \geqslant 1).$$

Find the least value of n for which u_n is not prime and find the factors of this u_n. Is u_6 prime?

14 Show that the integers defined in Ex. 13 satisfy

$$u_{n+1} = 1 + u_1u_2 \ldots u_n.$$

Deduce that u_{n+1} has a prime factor which is different from any prime factor of any one of $u_1, u_2, \ldots, u_n$. Hence show that the set of primes has no greatest member.

15 Is 65537 a prime?

16 Prove that if n is a positive integer, none of the n consecutive integers starting with $(n+1)!+2$ is a prime.

17 Prove that there are no integers x, y, z, t for which

$$x^2 + y^2 - 3z^2 - 3t^2 = 0.$$

18 Prove that if $\gcd(x, y) = 1$, and $xy = z^2$ for some integer z, then $x = n^2$ and $y = m^2$ for some integers m and n.

19 Show that if $\gcd(a, b) = 1$ then $\gcd(a+b, a-b)$ is either 1 or 2.

20 Show that it is possible to balance any integral weight from 1 to $2^n - 1$ grams if we are given weights of $1, 2, 4, \ldots, 2^{n-1}$ grams. Show that no other set of n weights will do this.

2 Functions and counting

2.1 Functions

Suppose that X and Y are sets. We say that we have a **function** f **from** X **to** Y if for each x in X we can specify a unique element in Y, which we denote by $f(x)$. This situation is illustrated in Fig. 2.1; and from this picture we derive the standard notation $f: X \to Y$ for a function f from X to Y.

It is helpful to think of f as a rule which assigns to each object x in X a unique object $f(x)$ in Y. The object $f(x)$ is usually called the **value** of f at x. The important points are that $f(x)$ is defined for every x in X, and that there is just one such object for each x.

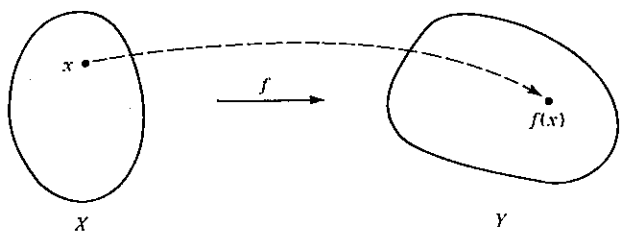
The most common functions in elementary mathematics are those for which X and Y are the sets $\mathbb{N}$ or $\mathbb{Z}$ or some other set of numbers. In this case the simplest method of specifying a function is by means of a formula. For example, the rule

$$f(n) = 3n + 4 \quad (n \in \mathbb{N})$$

defines the function f from $\mathbb{N}$ to $\mathbb{N}$ whose value at n is $3n+4$. Some functions may require a split definition, such as the function g from $\mathbb{Z}$ to $\mathbb{Z}$ given by the rule

$$g(x) = \begin{cases} x & \text{if } x \geqslant 0, \\ -x & \text{if } x < 0. \end{cases}$$

This function assigns to each integer x its *absolute value*, usually written $|x|$. For instance, $|5| = |-5| = 5$.



ion $f: X \to Y$.