8
Divisibility and prime numbers

8.1 Divisibility

In this short section we extend the concept of a 'multiple' from the natural numbers to the integers. We also summarize several other terms that express the same idea.

Given any two integers x and y we say that x is a **multiple** of y, if

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

We also say that y is a **divisor** or **factor** of x, that y **divides** x, and that x is **divisible** by y. All these statements are expressed by the notation

$$y|x.$$

For example, each of the following statements is true:

$$17|51, \qquad -17|51, \qquad 17|-51, \qquad -17|-51.$$

Contents

Exercises 8.1

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

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

3 Prove that if x and y are non-zero integers such that $x|y$ and $y|x$ then either $x = y$ or $x = -y$. [Hint: you may assume that if a and b are integers such that $ab = 1$ then $a = b = 1$ or $a = b = -1$. But how would you prove this?]

8.2 Quotient and remainder

Given integers x and y it often happens that y does not divide x, which we can write as $y \nmid x$.

For example, 6 does not divide 27 exactly. But as children we are taught that 6 does 'go into' 27 four times with three left over. That is,

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

The number 4 is called the *quotient* and 3 is called the *remainder*. The important point is that the remainder must be less than 6. It is also true that, for instance

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

but we are told that we must take the least value, so that the amount 'left over' is as small as possible.

Since the number 0 must be allowed as a remainder (why?), we shall state the general result in terms of the set

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\}.$$

Theorem 8.2 Given positive integers a and b there exist q and r in $\mathbb{N}_0$ such that

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

Proof The set of 'remainders' is

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

Now, R is not empty because the identity $a = b0 + a$ shows that $a \in R$. Thus R is a non-empty subset of $\mathbb{N}_0$, and so it has a least member r. Specifically, since r is in R it follows that $a = bq + r$ for some q in $\mathbb{N}_0$.

It remains to show that $r < b$. Observe that

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

so that if $r \geq b$ 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 $r \geq b$ leads to this contradiction we must have $r < b$, as required. □

The **remainder** r defined by the theorem is unique, because it is the least member of R, and if a set of integers has a least member, then it is unique (Ex. 7.6.3). It follows that the **quotient** q is also unique (Ex. 8.2.2).

Exercises 8.2

1 Find the quotient q and remainder r when
(i) $a = 1001$, $b = 11$; (ii) $a = 12345$, $b = 234$.

2 Show that, under the conditions of the theorem, if $a = bq + r$ and $a = bq' + r$, then $q = q'$.

8.3 Representation of integers

An important consequence of the theorem on quotient and remainder is that it justifies the usual notation for integers. (This is comforting, because we have been using the notation throughout the book.)

Let $t \geq 2$ be a positive integer, called the **base**. For any positive integer x we have, by repeated application of the theorem,

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

Here each remainder is 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 $x = (r_n r_{n-1} \ldots r_1 r_0)_t$. Conventionally, $t = 10$ is the base for calculations carried out 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

$$(109)_{10} = (1101101)_2. \qquad \square$$

Exercises 8.3

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

2 Find the decimal (base 10) representations of
(i) $(11011101)_2$; (ii) $(4165)_7$.

8.4 The greatest common divisor

According to the definition given in Section 8.1, the set D_m of divisors of a positive integer m contains both positive and negative integers. For example,

$$D_{12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}.$$

Given two positive integers a, b we say that $D_a \cap D_b$ is the set of **common divisors** of a and b. The set $D_a \cap D_b$ is not empty, because it contains 1. Also, any

common divisor c satisfies $c \leq a$ and $c \leq b$, so the set has a greatest member. This justifies the following definition.

Definition If a and b are positive integers (or zero) we say that d is the **greatest common divisor (gcd)** of a and b provided that

$$\text{(i) } d|a \text{ and } d|b; \qquad \text{(ii) if } c|a \text{ and } c|b, \text{ then } c \leq d.$$

In other words, d is the greatest member of the set $D_a \cap D_b$. For example, if $a = 63$ and $b = 35$,

$$D_{63} = \{-63, -21, -9, -7, -3, -1, 1, 3, 7, 9, 21, 63\},$$
$$D_{35} = \{-35, -7, -5, -1, 1, 5, 7, 35\}.$$

So the greatest common divisor of 63 and 35 is 7. We write

$$\gcd(63, 35) = 7.$$

Note that every integer divides 0, so $\gcd(a, 0) = a$.

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

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

In order to prove this, observe 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 $a = bq + r$. So $D_a \cap D_b = D_b \cap D_r$, and the greatest members of these sets are the same.

Repeated application of this simple fact is the basis of the **Euclidean algorithm** for calculating the gcd.

Example Find the gcd of 2406 and 654.

Solution We have

$$\begin{aligned}
2406 = 654 \times 3 + 444, &\ \Rightarrow\ \gcd(2406, 654) &&= \gcd(654, 444)\\
654 = 444 \times 1 + 210, &\ \Rightarrow &&= \gcd(444, 210)\\
444 = 210 \times 2 + 24, &\ \Rightarrow &&= \gcd(210, 24)\\
210 = 24 \times 8 + 18, &\ \Rightarrow &&= \gcd(24, 18)\\
24 = 18 \times 1 + 6, &\ \Rightarrow &&= \gcd(16, 6)\\
18 = 6 \times 3. &\ \Rightarrow &&= \gcd(6, 0) = 6. \qquad \square
\end{aligned}$$

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

$$\begin{aligned} a &= bq_1 + r_1 \quad (0 \le r_1 < b) \\ b &= r_1 q_2 + r_2 \quad (0 \le r_2 < r_1) \\ r_1 &= r_2 q_3 + r_3 \quad (0 \le r_3 < r_2) \\ &\ldots . \end{aligned}$$

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:

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

In the last line, the term r_k is omitted, because it is zero, and the required gcd is r_{k-1}.

As well as being extremely useful in practice, this technique has important theoretical consequences.

Theorem 8.4 Let a and b be positive integers, 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

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

Definition If $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

In this case the Theorem asserts that there are integers m and n such that

$$ma + nb = 1.$$

This is a very useful fact. We shall use it in Section 8.6 to prove one of the most important theorems in the whole of mathematics. It also has simple consequences.

Example You are given an unlimited supply of water, a large container, and two jugs whose capacities are 7 litres and 9 litres. How would you put one litre of water in the container?

Solution The key is the fact that $\gcd(9, 7) = 1$. It follows that there are integers m, n such that $9m + 7n = 1$. In fact, we can take $m = 4$, $n = -5$. So, using the larger jug, we put four jugfuls of water in the container; then, using the smaller jug, we scoop out five jugfuls.

Obviously, a similar method works whenever the capacities of the jugs are coprime. □

Exercises 8.4

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 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 $d|c$.

4 Find integers x and y satisfying

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

8.5 Prime numbers

Definition A positive integer p is a **prime** if $p \geq 2$ and the only positive integers which divide p are 1 and p itself.

We have already used this definition on several occasions. For example, the primes less than 100 are shown in Fig. 7.1. Note that, according to the definition 1 is *not* a prime number.

If $m \geq 2$ is not a prime then $m = rs$, where r and s are integers strictly between 1 and m; if this holds we say that m is *composite*.

In elementary arithmetic a standard exercise is to 'factorize' a given positive integer. For example,

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

You may recall finding the prime factorization is not always as easy as this example might suggest. Even a relatively small number like 1807 presents some difficulty, and a number such as

$$2^{67} - 1$$

is really quite hard (Ex. 1.2.5).

Some of the practical difficulties are illustrated in the Exercises below.

Exercises 8.5

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

2 Show that 123456789 is not a prime. In fact, there is a number N such that $123456789 = 3 \times 3 \times N$. Find N and show that it is not a prime.

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

8.6 Existence and uniqueness of prime factorization

Given any natural number $n > 1$, there is a prime factorization of n. This is a consequence of the following general argument. It is based on a fundamental property of natural numbers (Section 4.7): if there is a natural number with a certain property, then there is a least one.

Suppose there is a 'bad' natural number (a number greater than 1 that cannot be expressed as a product of primes). Then there is a least one, m. Now m cannot be a prime p, because if so we have the trivial factorization $m = p$. So $m = rs$ where $1 < r < m$ and $1 < s < m$. Since m is the least 'bad' number, both r and s do have factorizations. But in that case the equation $m = rs$ yields an expression for m as a product of primes, contradicting the fact that m is 'bad'. Hence there are no 'bad' numbers.

We now turn to the question of uniqueness. If we are asked to factorize 990, we might proceed as follows:

$$990 = 2 \times 495 = 2 \times 5 \times 99 = \ldots .$$

On the other hand, we might start in a different way:

$$990 = 11 \times 90 = 11 \times 2 \times 45 = \ldots .$$

You are probably confident that the 'answers' will be the same, although possibly the order of the factors will differ. However, this fact must be proved. A good way to understand what might go wrong is to think in terms of larger numbers, such as the numbers x and y defined below:

$$x = 56909 \times 127643, \quad y = 73951 \times 98227.$$

Here x and y are products of prime numbers, and in this case they are close but not equal. But is it true that one product of primes can never be equal to another one?

In this section we prove that there is a *unique* prime factorization for any integer greater than 1. The key step is the following result.

Theorem 8.6.1 If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that

$$p|x_1 x_2 \ldots x_n$$

then $p|x_i$ for some x_i $(1 \leq i \leq n)$.

Proof We use the principle of induction. The result is plainly true when $n = 1$ but, for reasons that will appear, it is convenient to start by proving the case $n = 2$.

Suppose then that $p|x_1x_2$. We shall prove that if p does not divide x_1 then p must divide x_2. Now, if p does not divide x_1 then (since 1 and p are the only positive divisors of p) we must have $\gcd(p, x_1) = 1$. From Theorem 8.4 there are integers r and s such that $rp + sx_1 = 1$. Hence

$$x_2 = (rp + sx_1)x_2 = (rx_2)p + s(x_1x_2).$$

Since p divides both terms it follows that $p|x_2$, as required.

Suppose the result holds when $n = k$, and consider the case $n = k + 1$, that is, when p is a divisor of a product $x_1x_2 \dots x_kx_{k+1}$. Define $X = x_1x_2 \dots x_k$, so that $p|Xx_{k+1}$. If $p|X$ then, by the induction hypothesis, $p|x_i$ for some x_i in the range $1 \leq i \leq k$. On the other hand, if p does not divide X, then by the result for the case $n = 2$, we must have $p|x_{k+1}$. Thus the induction step is done, and the result holds for all n. □

A very common error is to assume that the theorem remains true when the prime p is replaced by any positive integer. But that is clearly absurd: for example $3 \times 8 = 24$ and

$$6|24 \quad \text{but} \quad 6 \nmid 3 \quad \text{and} \quad 6 \nmid 8.$$

Examples such as this show that the theorem expresses a significant property of primes, not shared by non-primes. Indeed, this property plays a crucial part in our main result.

Theorem 8.6.2 (*The Fundamental Theorem of Arithmetic*) A positive integer $n \geq 2$ has a unique prime factorization, apart from the order of the factors.

Proof If there is a number for which the theorem is false, then there is a least one N. That is,

$$N = p_1p_2 \dots p_k \quad \text{and} \quad N = q_1q_2 \dots q_l,$$

where the p_i $(1 \leq i \leq k)$ are primes, not necessarily distinct, and the q_j $(1 \leq j \leq l)$ are primes, not necessarily distinct. Write

$$N = p_1N', \quad \text{where} \quad N' = p_2 \dots p_k.$$

Since $p_1|N$, and $N = q_1q_2 \dots q_l$ it follows from the previous theorem that p_1 divides one of these factors, say q_j. In fact, since q_j is a prime, $p_1 = q_j$ (Ex. 8.5.5). Thus we can cancel the equal terms p_1 and q_j from the two expressions for N, obtaining

$$N' = p_2 \dots p_k = q_1q_2 \dots q_{j-1}\ q_{j+1} \dots q_l.$$

So N' has two prime factorizations. But $N' < N$, so the factorizations must be the same, apart from the order of the factors. If we now re-introduce the (equal) factors p_1 and q_j, we conclude that the original factorizations of N must be the same, apart from the order of the factors. This contradicts the definition of N. Hence there can be no such N, and the theorem is true for all $n \geq 2$. □

We often collect equal primes in the factorization of n and write

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

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

Exercises 8.6

1 Find the prime factorizations of 201, 1001, and 201000.

2 Find the prime factorization of 123456786.

3 Show that if $n \geq 2$ and n is not a prime then there is a prime p such that $p|n$ and $p^2 \leq n$. Hence show that if 467 were not a prime then it would have a prime divisor $p \leq 19$. Deduce that 467 is a prime.

4 Suppose that we wish to test whether the number 123456791 is a prime, by checking all possible prime divisors up to a certain number X. On the basis of Ex. 3, what value of X (approximately) is sufficient?

5 Let H be the set $\{4n + 1 \mid n \in \mathbb{N} \cup \{0\}\} = \{1, 5, 9, 13, \dots\}$. Show that H is *closed under multiplication*; in other words, that the product of two members of H is also in H.

A member of H (other than 1) that is not the product of two members of H other than 1 and itself is called an *H-prime*. Find three distinct H-primes a, b and c such that $441 = ab = c^2$.

Is it true that every element of H has a factorization into H-primes? Is it true that every element of H has a *unique* factorization into H-primes?

Explain why the proof that every integer has a unique prime factorization does not work in this situation.

8.7 Miscellaneous Exercises

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

2 Show that 725 and 441 are co-primes and hence find integers x and y such that $725x + 441y = 1$.

3 Find a solution in integers to the equation

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

4 Let $\gcd(a, b) = d$ and $a = da'$, $b = db'$. Show that $\gcd(a', b') = 1$.

5 The Fibonacci number f_n is defined recursively by the equations

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

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

6 Show that $\gcd(f_{n+2}, f_n) = 1$, and

$$\gcd(f_{n+3}, f_n)) = \begin{cases} 2 & \text{if } n \equiv 0 \bmod 3; \\ 1 & \text{otherwise.} \end{cases}$$

$$\gcd(f_{n+4}, f_n) = \begin{cases} 3 & \text{if } n \equiv 0 \bmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

7 Is it true that the gcd of any two Fibonacci numbers is another Fibonacci number?

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

$$l \times \gcd(a, b) = ab.$$

Explain why this definition works and show that

(i) $a|l$ and $b|l$;

(ii) if m is a positive integer such that $a|m$ and $b|m$, then $l|m$.

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

$$d = x_1 a_1 + x_2 a_2 + \dots + x_n a_n.$$

11 Define a relation R on the set of positive integers by the rule

$$aRb \iff \gcd(a, b) > 1.$$

Is R reflexive? Is R symmetric? Is R transitive?

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

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

13 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.

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

15 Suppose we have a set of n weights, with mass $1, 2, 4, \ldots, 2^{n-1}$ grams. Show that it is possible to balance any object whose mass is an integral number of grams in the range from 1 to $2^n - 1$ grams, and that no other set of n weights will do this.

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

(i) the prime factorization of n has no repeated factors;

(ii) for all primes p, $p|n$ if and only if $(p - 1)|n$.

Prove that $n = 1806$.