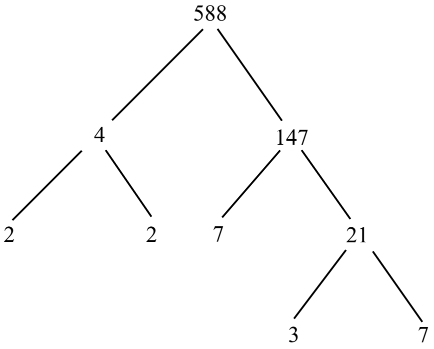


Fig. 1.2 Factorisation of 588 by splitting.

each of $p_1, p_2, \ldots, p_n$. Since n may be chosen as large as we like, this will show that there are not just finitely many primes.

Define the number N as follows:

$$N = (p_1 p_2 \ldots p_n) + 1.$$

Note that N has remainder 1 when divided by each of $p_1, p_2, \ldots, p_n$: in particular, none of $p_1, p_2, \ldots, p_n$ divides N exactly. By Theorem 1.3.3, N has a prime divisor p. Since p divides N, p cannot be equal to any of $p_1, p_2, \ldots, p_n$: thus we have shown that there exists a prime which is not on our original list, as required. □

Comment This is a beautiful and clever proof. The scheme of the proof is to show how, given any finite set of primes, we can construct a number (≥ 2) which is not divisible by any of them (and which, therefore, must have a prime factor not in our original set).

The integer N defined in the proof need not itself be prime: we simply showed that it has a prime divisor not equal to any of $p_1, p_2, \ldots, p_n$. In principle, one may find a 'p' as in the proof by factorising N. So the proof is, in principle, a recipe which, given any finite list of primes, will produce a 'new' prime (i.e. one not on the list).

When we write an integer as a product of prime numbers it is often convenient to group together the occurrences of the same prime: for example, rather than writing $72 = 2 \times 2 \times 2 \times 3 \times 3$ one writes $72 = 2^3 \times 3^2$.

The following characterisation of greatest common divisor and least common multiple is easily obtained.

Corollary 1.3.5 *Let a and b be positive integers. Let*

$$a = (p_1)^{n_1} (p_2)^{n_2} \ldots (p_r)^{n_r}$$
$$b = (p_1)^{m_1} (p_2)^{m_2} \ldots (p_r)^{m_r}$$

be the prime factorisations of a and b, where $p_1, p_2 \ldots, p_r$ are distinct primes and $n_1, n_2, \ldots, n_r, m_1, m_2, \ldots, m_r$ are non-negative integers (some perhaps zero, in order to allow a common list of primes to be used, see the example which follows the proof).

Then the greatest common divisor, d, of a and b is given by

$$d = (p_1)^{k_1}(p_2)^{k_2} \ldots (p_r)^{k_r},$$

where, for each i, k_i is the smaller of n_i and m_i, and the least common multiple, f, of a and b is given by

$$f = (p_1)^{t_1}(p_2)^{t_2} \ldots (p_r)^{t_r},$$

where, for each i, t_i is the larger of n_i and m_i.

Proof The characterisation of the greatest common divisor follows using Theorem 1.1.6(ii) since any number of the form p^n, with p prime, divides the greatest common divisor (a, b) exactly if it divides both a and b.

Similarly the characterisation of the lowest common multiple follows since a prime power, p^n, is a factor of a or of b exactly if it is a factor of their lowest common multiple. □

Comment We have been a bit brief here, leaving out the detailed argument but pointing out what you need to use. This is the first place where we have written 'Proof' yet have not really given a proof, only an indication of how the proof goes.

If you want to see a detailed argument then, in this case, probably it is better to write it down yourself rather than read it. Once you see what the result is saying (if you do not, try it with some numbers in place of the letters) and have understood the relevance of the statements we made in the 'proof', you will probably be able to see how a proof could go, though writing it down would take some organisation and, depending on how you do it, could be a little tedious.

The above result is often of practical use in calculating the greatest common divisor d of two integers, provided we do not need to express d as a linear combination of the numbers, and provided we can find the prime factorisations of the numbers quickly.

Example To find the greatest common divisor of 135 and 639 we factorise these to obtain that 135 is 5 times $27 = 3^3$ and that 639 is $9 = 3^2$ times 71. So $135 = 3^3 \cdot 5^1 \cdot 71^0$ and $639 = 3^2 \cdot 5^0 \cdot 71^1$. It follows that the greatest common divisor is $3^2 \cdot 5^0 \cdot 71^0 = 3^2 = 9$.

Example To find the lowest common multiple of 84 and 56 observe that $84 = 2^2 \cdot 3 \cdot 7$ and that $56 = 2^3 \cdot 7$. Therefore lcm $(84, 56) = 2^3 \cdot 3 \cdot 7 = 168$.

Along with geometry, the study of the arithmetic properties of integers (which, until rather late on, meant the positive integers) forms the most ancient part of mathematics. Significant discoveries were made in many of the early civilisations around the Mediterranean, in the Near East, in Asia and in South America but undoubtedly the greatest discoveries in ancient times were made by the Greeks. Probably the main factor in accounting for this is that their interest in numbers was motivated less by practical motives (such as commerce and astrological calculations) than by philosophical considerations. This relative freedom from particular applications gave them a rather abstract viewpoint from which, perhaps, they were more likely to discover general properties.

Almost all of what we have covered in Sections 1.1 and 1.3 may be found in Euclid's *Elements* and probably was of earlier origin. It should be remarked, however, that the presentation of these results in Euclid is very different from their presentation above, There are two main differences.

The first difference is peculiar to the Greek mathematicians, and it is that numbers were treated by them as lengths of line segments. Thus, for example, they would often represent the product of two numbers a and b as the area of a rectangle with sides of length a and b respectively.

Euclid describes the process of finding the greatest common divisor of a and b in terms of starting with two line segments, one of length a and the other of length b ($\neq a$); from the longer line one removes a segment of length equal to the length of the shorter line segment; one continues this process, always subtracting the current shorter length from the current longer one. Provided that the starting lengths, a and b, are integers this process will terminate, in the sense that at some stage one reaches two lines of equal length: this length is the 'common measure' (greatest common divisor) of a and b. The process described in 1.1.5 is just a somewhat telescoped version of this.

Actually, for a and b to have a common measure in the above sense it is not necessary that they be integers: it is enough that they be rational numbers (fractions). The earlier Greek mathematicians believed that *any* two line segments have a common measure in this sense, and an intellectual crisis arose when it was discovered that, on the contrary, the side of a square does not have a common measure with the diagonal of the square (or, as we would put it, the square root of 2 is irrational).

The second difference was the lack of a good algebraic notation. This was a weakness to a greater or lesser degree of all early mathematics, although the Indian mathematicians adopted a relatively symbolic notation quite early on.

In Europe Viète (1540–1603) was largely responsible for the beginnings of a reasonable symbolic notation.

In this connection, it is worthwhile pointing out that Euclid's proof of the infinity of primes (Corollary 1.3.4) goes (in modern terminology) more or less as follows.

Suppose that there are only finitely many primes, say a, b and c. Consider the product $abc + 1$. This number has a prime divisor d. Since none of a, b, c divides $abc + 1$, d is a prime different from each of a, b, c. This is a contradiction. Hence the number of primes is not finite.

Nowadays, this proof would be criticised since it derives a contradiction only in the special case that there are just three primes (a, b, c): we would say 'suppose there were only finitely many primes $p_1, \ldots, p_n$'. But how could Euclid even say that in the absence of a notation for indices or subscripts? Since he did not even have the notation with which to express the general case, Euclid had to resort to a particular instance, but his readers would have understood that the argument itself was perfectly general. (Note, by the way, that Euclid's argument is presented as a proof by contradiction.)

Perhaps the high point of Greek work in number theory was the *Arithmetica* of Diophantus (who flourished around AD 250). Originally there were thirteen books comprising this work but only six have survived: it is not even known what kinds of problems were treated in the seven missing books. A major concern of the *Arithmetica* was the finding of integer or rational solutions to equations of various sorts. The methods were presented in the form of solutions to problems and, because of the inadequacy of the notation, in any given problem every unknown but one would be replaced by a particular numerical value (and the generality of the method would then have to be inferred). Many problems raised in that work are still unsolved today, despite the attention of some of the greatest mathematicians. On the other hand, work on these problems has given rise to extremely deep mathematics, and this has led to many successes, such as results of Gerd Faltings in 1983 answering old questions on integer solutions to equations and, in particular, Andrew Wiles' proof of 'Fermat's Last Theorem', which we discuss at the end of Section 1.6.

After the work of the Greeks, very little advance in number theory was made in Europe until interest was rekindled by Fermat and later by Euler. This was in contrast to the continuing advances made by Arab, Chinese and Indian mathematicians.

One problem which Fermat (1601–65) considered was that of finding various methods to generate sequences of prime numbers. He considered numbers of the form $2^n + 1$: such a number cannot be prime unless n is a power of 2 (see Exercise 1.3.7). Setting $F(k) = 2^{2^k} + 1$ one has that $F(0), F(1), \ldots, F(6)$ are

$$3, 5, 17, 257, 65\,537, 4\,294\,967\,297, 18\,446\,744\,073\,709\,551\,617.$$

In a letter of 1640 to Frénicle, Fermat lists the above numbers and expresses his belief that all are prime, and he conjectures that the sequence of integers $F(k)$ might be a sequence of primes. In fact, although $F(0)$, $F(1)$, $F(2)$, $F(3)$, $F(4)$ all are primes, $F(5)$ and $F(6)$ are not. It is rather surprising that Fermat and Frénicle failed to discover that $F(5)$ is not prime since, although this number is rather large, it is possible to find a factor by using an argument similar to that used by Fermat when he showed that $2^{37} - 1$ is not prime (see Exercise 1.6.10 below). In fact, such an argument was used by Euler almost a century later to show that $F(5)$ is not prime (in the process Euler rediscovered Fermat's Theorem, 1.6.3 below). Fermat persisted in his belief that $F(5)$ was prime, though he later added that he did not have a full proof. Actually no new **Fermat primes** (that is, numbers of the form $F(k)$ which are prime) have subsequently been discovered.

A better source of primes is provided by the Mersenne sequence $M(n)$, of numbers of the form $2^n - 1$. It may be shown that $M(n)$ can only be prime if n itself is prime (Exercise 1.3.6). The converse is false, that is, there are prime values of n for which $M(n)$ is not prime. One such value is $n = 37$ (another, as you may check is $n = 11$). Fermat showed that $M(37)$, which equals 137 438 953 471, is not prime, by an argument using the theorem which bears his name (Theorem 1.6.3 below). Exercise 1.6.10 asks you to do the same. There are currently 39 **Mersenne primes** known, the last 27 having been discovered (i.e. shown to be prime) by computer (now most commonly by networks of computers linked over the internet). The largest to date is $M(13\,466\,917)$, an integer whose decimal expansion has over four million digits! Discovered in 2001, it is currently (2003) the largest known prime.

Perhaps the most famous unsolved questions concerning prime numbers are the following.

(i) Are there an infinite number of prime pairs, that is, numbers of the form p, $p + 2$ with both numbers prime?

(ii) (Goldbach's conjecture) Can every integer greater than 2 be written as a sum of two primes?

The answers to these simply stated problems are unknown.

The second is stated as a question but the **conjecture** (what Goldbach expected to be true) is that every integer greater than 2 *can* be written as a sum of two primes. How can such a conjecture be verified (or shown to be wrong)? Of course we can check for 'small' values: it is easy enough to check that (say) each of the first hundred even integers greater than 2 may be written as a sum of two primes. With the aid of a computer one may extend one's search for counterexamples to much larger numbers. A **counterexample** to Goldbach's conjecture would be a number greater than 2 which cannot be written as a sum of two primes. So far, no counterexample to Goldbach's conjecture has been found. On the other hand still there is no general proof of its validity. So it could be that tomorrow some computer search will turn up a counterexample (or someone will find a proof that it is correct).

One of the attractions of number theory lies in the fact that such simply stated questions are still unanswered.

Exercises 1.3

1. Use the Sieve of Eratosthenes to find all prime numbers less than 250.
2. Show why, when using the sieve method to find all primes less than n, you need only strike out multiples of the primes whose square is less than or equal to n.
3. (a) Find the prime factorisations for the following integers (a calculator will be useful for the larger values): 136, 150, 255, 713, 3549, 4591.
   (b) Use your answers to find the greatest common divisor and least common multiple of each of the pairs: 136 and 150; 255 and 3549.
4. Let $p_1 = 2$, $p_2 = 3, \ldots$ be the list of primes, in increasing order. Consider products of the form

   $$(p_1 \times p_2 \times \cdots \times p_n) + 1$$

   (compare with the proof of Corollary 1.3.4).
   Show that this number is prime for $n = 1, \ldots, 5$.
   Show that when $n = 6$ this number is not prime. [Use your answer to Exercise 1.3.1. A calculator will speed the work of checking divisibility.]
5. By considering the prime decomposition of (ab, n), show that if a, b and n are integers with n relatively prime to each of a and b, then n is relatively prime to ab.
6. Show that if $2^n - 1$ is prime, then n must be prime.
7. Show that if $2^n + 1$ is prime, where $n \geq 1$, then n must be of the form 2^k for some positive integer k.
8. Prove that there are infinitely many primes of the form $4k + 3$. Argue by contradiction: supposing that there are only finitely many primes

$p_1 = 3$, $p_2 = 7, \ldots, p_n$ of that form, consider

$$N = 4(p_2 \times \cdots \times p_n) + 3.$$

9. Show that for any non-zero integers a and b

$$ab = \gcd(a, b)\operatorname{lcm}(a, b).$$

1.4 Congruence classes

Some of the problems in Diophantus' *Arithmetica* (see above, end of Section 1.3) concerned questions such as 'When may an integer be expressed as a sum of two squares'? (This is a natural question in view of the Greeks' geometric treatment of algebra, and Pythagoras' Theorem.) One of the first results of Fermat's reading of Diophantus was his proof that no number of the form $4k + 3$ can be a sum of two squares (although he was by no means the first to discover this, for example Bachet and Descartes already knew it).

The result is not difficult for us to prove: we could give the proof now, but it will be much easier to describe after the following definition and observations.

The main concepts in this section are the idea of integers being congruent modulo some fixed integer and the notion of congruence class. The first concept was fairly explicit in the work of Fermat and his contemporaries, and both concepts occur in Euler's later works in the mid-eighteenth century, but the notation which we use now was introduced by Carl Friedrich Gauss (1777–1855) in his *Disquisitiones Arithmeticae* published in 1801, which begins with a thorough treatment of these ideas.

Definition Suppose that n is an integer greater than 1, and let a, b be integers. We say that a is **congruent** to b **mod(ulo)** n if a and b have the same remainder when divided (according to 1.1.1) by n. We write

$$a \equiv b \bmod n$$

if this is so.

The definition may be more usefully formulated as follows:

$$a \equiv b \bmod n \text{ if and only if } n \text{ divides } a - b.$$

Examples $-1 \equiv 4 \bmod 5$

$$6 \equiv 18 \bmod 12$$

$$19 \equiv -5 \bmod 12.$$

The notion of two integers being congruent modulo some fixed integer is actually one with which we are familiar from special cases in everyday life. For example, if we count days from now, then day k and day m will be the same day of the week if, when divided by 7, k and m have the same remainder, that is, if $k \equiv m \bmod 7$. Similarly a clock works, in hours, modulo 12 (or 24). Christmas in 1988 fell on a Sunday: therefore Christmas 1989 fell on a Monday since there were 365 days in 1989 (not a leap year), and 365 is congruent to 1 modulo 7: therefore the day of the week on which Christmas fell moved one day forward. For another example, take measurements of angles, where it is often appropriate to work modulo 360 degrees.

Notes (i) The condition 'n divides a' can be written as '$a \equiv 0 \bmod n$.'

(ii) The properties of congruence '$\equiv$' are very similar to those of the usual equality sign '$=$'. For example it is permissible to add to, or subtract from, both sides of any congruence the same quantity, or to multiply both sides by a constant. Thus if a, b and c are integers and if

$$a \equiv b \bmod n$$

so, by definition, a and b have the same remainder when divided by n, then

$$\begin{aligned} a + c &\equiv b + c \bmod n \\ a - c &\equiv b - c \bmod n, \quad \text{and} \\ ca &\equiv cb \bmod n. \end{aligned}$$

However, the situation for division is more complicated, as we shall see.

Now we may return to the problem at the beginning of this section. Let us take any integer m and square it: what are the possibilities for m^2 modulo 4? It is an easy consequence of the rules above that the value of m^2 modulo 4 depends only on the value of m modulo 4. For example, if $m \equiv 3 \bmod 4$ so $m = 4k + 3$ for some k in $\mathbb{Z}$, then

$$m^2 = (4k + 3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k) + 9 \equiv 9 \equiv 1 \bmod 4.$$

If m is respectively congruent to 0, 1, 2, 3 modulo 4 then m^2 is respectively congruent to 0, 1, 4, 9 modulo 4, and these are in turn congruent to 0, 1, 0, 1 modulo 4. Therefore if an integer k is the sum of two squares, say $k = n^2 + m^2$, then, modulo 4, the possibilities for k are

$$(0 \text{ or } 1) + (0 \text{ or } 1).$$

In particular, it is impossible for k to be congruent to 3 modulo 4. In other words, a sum of two squares cannot be of the form $4k + 3$.

Consider ‘equations’ involving this notion: such equations are called **congruences**. For a specific example take

$$2x \equiv 0 \bmod 4.$$

What should be meant by a *solution* to this congruence?

Notice that there are infinitely many integer values for ‘x’ which will solve it:

$$\ldots, -4, -2, 0, 2, 4, 6, \ldots.$$

These ‘solutions’ may, however, be divided into two classes, namely:

$$\ldots, -8, -4, 0, 4, 8, \ldots \text{ and } \ldots, -6, -2, 2, 6, 10, \ldots$$

where, within each class, all the integers are congruent to each other modulo 4, but no integer in the one class is congruent modulo 4 to any integer in the other class. So in some sense the congruence

$$2x \equiv 0 \bmod 4$$

may be thought of as having essentially two solutions, where each solution is a ‘congruence class’ of integers. We make the following definition.

Definition Fix an integer n greater than 1 and let a be any integer. The **congruence class** of a **modulo** n is the set of all integers which are congruent to a modulo n:

$$[a]_n = \{b : b \equiv a \bmod n\}.$$

The set of all congruence classes modulo n is referred to as the **set of integers modulo** n and is denoted $\mathbb{Z}_n$. Observe that this is a set with n elements, for there are exactly n possibilities for the remainder when an integer is divided by n. By the **zero congruence class** we mean the congruence class of 0 (that is, the congruence class consisting of all multiples of n).

Note that

$$[a]_n = [b]_n \text{ if and only if } a \equiv b \bmod n.$$

Example 1 When n is 2, there are two congruence classes namely $[0]_2$, which is the set of even integers and $[1]_2$ (the set of odd integers).

Example 2 When n is 10, the positive integers in a given congruence class are those which have the same last digit when written (as usual) in base 10.

The solutions to

$$2x \equiv 0 \bmod 4$$

are, therefore, the congruence classes $[0]_4$ and $[2]_4$.

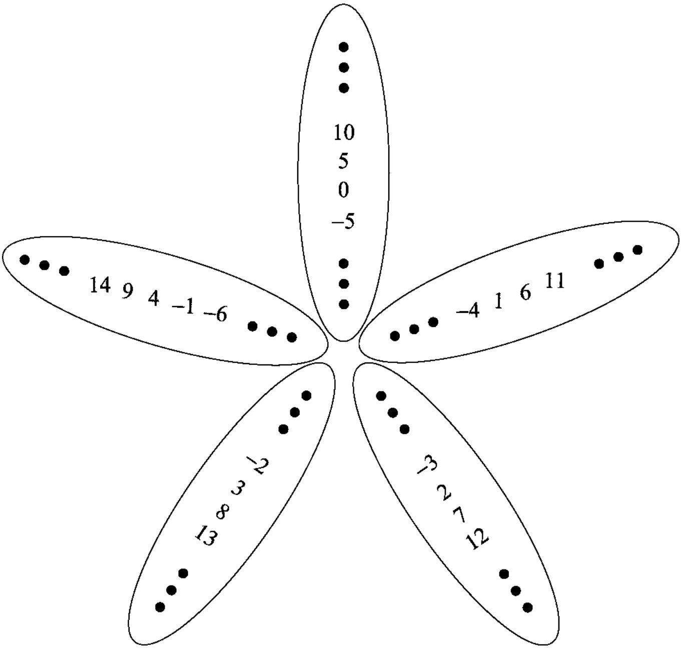


Fig. 1.3 Congruence classes in $\mathbb{Z}_5$.

There are many ways of representing a given congruence class: for example we could equally well have written any of $\dots, [-4]_4, [4]_4, [8]_4, \dots$ in place of $[0]_4$; similarly $\dots, [-2]_4, [2]_4, [6]_4, \dots$ all equal $[2]_4$.

Since every element of $\mathbb{Z}_n$ may be represented in infinitely many ways it is useful to fix a set of standard representatives (by a **representative** of a congruence class we mean any integer in that class): these are usually taken to be the integers from 0 to $n - 1$. Thus

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-2]_n, [n-1]_n\}.$$

For example

$$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\} \qquad \text{(see Fig. 1.3)},$$
$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}.$$

We may drop the subscript 'n' when doing so leads to no ambiguity. Also for convenience sometimes we denote the congruence class $[a]_n$ simply by a, provided it is clear from the context that $[a]_n$ is meant.

One may say that the notions of congruence modulo n and congruence classes were implicit in early work in number theory in the sense that if one refers to, say, ‘integers of the form $4n + 3$’ then one is implicitly referring to the congruence class $[3]_4$. These notions only became explicit with Euler: as his work in number theory developed, he became increasingly aware that he was working not with numbers, but with certain sets of numbers. However, the *Tractatus de Numerorum Doctrina*, in which he systematically developed these notions (around 1750), was not published by him, although he did incorporate many of the results in various of his papers. The *Tractatus* was printed posthumously in 1830 but by then it had been superseded by Gauss’ *Disquisitiones Arithmeticae* (1801). In that work Gauss went considerably further than Euler had. The notations that we use here for congruence and for congruence classes were introduced by Gauss.

Consideration of $\mathbb{Z}_n$ would be rather pointless if we could not do arithmetic modulo n: in fact $\mathbb{Z}_n$ inherits the arithmetic operations of $\mathbb{Z}$, as follows.

Definition Fix an integer n greater than 1 and let a, b be any integers. Define the **sum** and **product** of the congruence classes of a and b by:

$$[a]_n + [b]_n = [a + b]_n,$$
$$[a]_n \times [b]_n = [a \times b]_n.$$

(As usual $[a]_n \cdot [b]_n$ or just $[a]_n[b]_n$ may also be used to denote the product.)

There is a potential problem with this definition. We have defined the sum (and product) of two congruence classes by reference to particular representatives of the classes. How can we be sure that if we chose to represent $[a]_n$ in some other form (say as $[a + 99n]_n$) then we would get the same congruence class for the sum? Well, we can check.

Before giving the general proof, let us illustrate this point with an example. Suppose that we take $n = 6$ and we wish to compute $[3]_6 + [5]_6$. By the definition above, this is $[3 + 5]_6 = [8]_6 = [2]_6$. But $[3]_6 = [21]_6$ so we certainly want to have $[3]_6 + [5]_6 = [21]_6 + [5]_6$. We have just seen that the term on the left is equal to $[2]_6$, so if our definition of addition of congruence classes is a good one then the term on the right-hand side should turn out to be the same. We check: $[21]_6 + [5]_6 = [26]_6 = [2]_6$, so no problem has appeared. Of course we also have $[3]_6 = [-9]_6$, so it should also be that $[-9]_6 + [5]_6 = [2]_6$, and you may check that this is so. These are just two cases checked: but there are infinitely many representatives for $[3]_6$ (and for $[5]_6$). So we need a general proof that the definitions are good: such a proof is given next.

Theorem 1.4.1 *Let n be an integer greater than* 1 *and let a, b and c be any integers. Suppose that*

$$[a]_n = [c]_n.$$

Then:

(i) $[a+b]_n = [c+b]_n$, *and*
(ii) $[ab]_n = [cb]_n$.

Proof (i) Since $[a]_n = [c]_n$, n divides $c-a$. So we can write

$$c = a + kn$$

for some integer k. Therefore

$$\begin{aligned} [c+b]_n &= [a+kn+b]_n \\ &= [a+b+kn]_n \\ &= [a+b]_n \text{ (by definition of congruence class)} \end{aligned}$$

as required.

(ii) With the above notation, we have that

$$\begin{aligned} [cb]_n &= [(a+kn)b]_n \\ &= [ab+nkb]_n \\ &= [ab]_n. \quad \square \end{aligned}$$

Comment The proof itself is, we hope, easy to follow line by line. In the discussion before the result we tried to explain the purpose of the theorem and proof. Experience suggests, however, that students often find this rather baffling so we say just a little more.

We are going to make $\mathbb{Z}_n$ into an algebraic structure: in particular we want to add and multiply congruence *classes*. In the statement of Theorem 1.4.1 we started by saying 'Suppose that $[a]_n = [c]_n$', in other words, suppose that a and c belong to the same congruence class. Then in (i) we take an element b in a possibly different class and add it to each of a and c. The assertion we prove is that the two resulting integers, $a+b$ and $c+b$, belong to the same class. Part (ii) says the corresponding thing for multiplication.

By symmetry we can also replace b by an element d in the same class as b, so the next result is an immediate corollary.

Corollary 1.4.2 *If*

$$[a]_n = [c]_n \textit{ and } [b]_n = [d]_n$$

then

(i) $[a+b]_n = [c+d]_n$, *and*
(ii) $[ab]_n = [cd]_n$.

Therefore we may write

$$[a]_n + [b]_n = [a+b]_n, \; \textit{and}$$
$$[a]_n[b]_n = [ab]_n$$

without ambiguity.

Example Show that 11 divides $10! + 1$ (recall from Section 1.2 that $10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$). It is not necessary to compute $10! + 1$ and then find the remainder modulo 11, rather we reduce modulo 11 as we go along:

$$2 \times 3 \times 4 = 24 \equiv 2 \bmod 11,$$

$$\begin{aligned}
6! &= (2 \times 3 \times 4) \times 5 \times 6 \equiv 2 \times 5 \times 6 \bmod 11\\
&\equiv 60 \bmod 11\\
&\equiv 5 \bmod 11,\\
6! \times 7 &\equiv 5 \times 7 \bmod 11\\
&\equiv 35 \bmod 11\\
&\equiv 2 \bmod 11,\\
7! \times 8 &\equiv 2 \times 8 \bmod 11\\
&\equiv 16 \bmod 11\\
&\equiv 5 \bmod 11,\\
8! \times 9 \times 10 &\equiv 5 \times 9 \times 10 \bmod 11\\
&\equiv 5 \times (-2) \times (-1) \bmod 11\\
&\equiv 10 \bmod 11.
\end{aligned}$$

Therefore $10! + 1 \equiv 10 + 1 \equiv 0 \bmod 11$, as required.

Example In the last stage of the computation above, we simplified by replacing 9 and 10 mod 11 by -2 and -1 respectively. Similarly, if we wish to compute the standard representative of, say $([13]_{18})^3$ then we can make use of the fact that $13 \equiv -5 \bmod 18$:

$$13^3 \equiv (-5)^3 \equiv 25 \times (-5) \equiv 7 \times (-5) \equiv -35 \equiv 1 \bmod 18$$

(for the last step we added a suitable multiple of 18, in this case 36).

We can make addition and multiplication tables for $\mathbb{Z}_n$ as given below when n is 8, where the entry in the intersection of the a-row and b-column is $[a]_n + [b]_n$ (or $[a]_n \times [b]_n$, as appropriate). Note that we abbreviate $[a]_8$ to a in these tables.

Addition and multiplication tables for $\mathbb{Z}_8$

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Definition Fix an integer n greater than 1, and let a be any integer. We say that $[a]_n$ is **invertible** (or a is **invertible modulo** n) if there is an integer b such that

$$[a]_n[b]_n = [1]_n$$

(that is, such that $ab \equiv 1 \bmod n$), in which case $[b]_n$ is the **inverse** of $[a]_n$, and we write $[b]_n = [a]_n^{-1}$. We say that a non-zero congruence class $[a]_n$ is a **zero-divisor** if there exists an integer b with

$$[b]_n \neq [0]_n \text{ and } [a]_n[b]_n = [0]_n$$

(in which case, note, $[b]_n$ also is a zero-divisor).

Example In $\mathbb{Z}_8$ there are elements, such as $[5]_8$, other than $\pm[1]_8$ with multiplicative inverses. Also there are elements other than $[0]_8$ which are zero-divisors, for instance $[2]_8$ (because $[2]_8[4]_8 = [0]_8$).

How do we tell if a given congruence class has an inverse? and if the class is invertible how may we set about finding its inverse?

Theorem 1.4.3 *Let n be an integer greater than or equal to 2, and let a be any integer. Then $[a]_n$ has an inverse if and only if the greatest common divisor of a and n is 1. In fact, if r and s are integers such that*

$$ar + ns = 1$$

then the inverse of $[a]_n$ is $[r]_n$.

Proof Since n is fixed, we will leave off the subscripts from congruence classes. Suppose first that $[a]$ has an inverse, $[k]$ say. So $[ak]$ is equal to $[1]$. Hence

$$ak \equiv 1 \bmod n,$$

that is, n divides $ak - 1$. Therefore, for some integer t,

$$ak - 1 = nt.$$

Hence

$$ak - nt = 1,$$

which, by Corollary 1.1.3, means that the greatest common divisor, (a, n), of a and n is 1.

Suppose, conversely, that (a, n) is 1 and that r and s are integers such that

$$ar + ns = 1.$$

It follows that $ar - 1$ is divisible by n, and so

$$ar \equiv 1 \bmod n,$$

that is,

$$[a][r] = [1],$$

as required. □

Comment The important thing here is to look at the equation $ar + ns = 1$ and to realise that if it is 'reduced modulo n' then, because n becomes 0, the term ns disappears and we are left with the equation $[ar]_n = [1]_n$, that is $[a]_n[r]_n = [1]_n$ so there, plainly before us, is an inverse for $[a]_n$.

It is 'if and only if' because the argument just outlined (that if the gcd is 1 then a has an inverse modulo n) reverses: from the conclusion, that a has an inverse mod n, we can work back to the assumption that $(a, n) = 1$.

Since we already have a method for expressing the greatest common divisor of two integers as an integral linear combination of them, the above theorem provides us with a practical method for finding out if a congruence class is invertible and, at the same time, calculating its inverse.

Example 1 We saw in Section 1.1 that

$$1 = -91 \cdot 507 + 118 \cdot 391$$

and so the inverse of 391 modulo 507 is 118.

Example 2 If a is 215 and n is 795, since 5 divides both these integers, their greatest common divisor is not 1 and so 215 has no inverse modulo 795.

Example 3 Let a be 23 and let n be 73. The matrix method for finding the gcd of a and n gives

$$\left(\begin{array}{cc|c} 1 & 0 & 73 \\ 0 & 1 & 23 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -3 & 4 \\ 0 & 1 & 23 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -3 & 4 \\ -5 & 16 & 3 \end{array}\right) \to \left(\begin{array}{cc|c} 6 & -19 & 1 \\ -5 & 16 & 3 \end{array}\right).$$

From the top row we have

$$6 \cdot 73 - 19 \cdot 23 = 1.$$

'Reduce this equation modulo 73' to obtain

$$[-19]_{73}[23]_{73} = [1]_{73}$$

and so the inverse of 23 modulo 73 is -19.

It is usual to express the answer using the standard representative, and so normally we would say that the inverse of 23 modulo 73 is 54 ($= -19 + 73$) and write $[23]_{73}^{-1} = [54]_{73}$.

Example 4 When the numbers involved are small it can be cumbersome to use the matrix method, and inverses can often be found quite easily by inspection. For example, if we wish to find the inverse of 8 modulo 11, then we are looking for an integer multiple of 8 which has remainder 1 when divided by 11, so we can inspect multiples of 11, plus 1, for divisibility by 8: one observes that

$$55 + 1 = 56 = 7 \times 8,$$

and so it follows that the inverse of 8 modulo 11 is 7. Similarly, observing that

$$11^2 = 121 \equiv 1 \bmod 20$$

one sees that $[11]_{20}$ is its own inverse (is 'self-inverse'):

$$[11]_{20}^{-1} = [11]_{20}.$$

A method for finding inverses modulo n (when they exist) is found in Bachet's *Problèmes plaisants et délectables* (1612), but Brahmagupta, who flourished about AD 628, had already given the general solution.

We now give three results which may be regarded as consequences of Theorem 1.4.3. The first of these considers the problem of cancelling in congruences.

Corollary 1.4.4 *Let n be an integer greater than or equal to 2, and let a, b, c be any integers. If n and c are relatively prime and if*

$$ac \equiv bc \bmod n,$$

then

$$a \equiv b \bmod n.$$

Proof The congruence may be written as the equation

$$[a]_n[c]_n = [b]_n[c]_n.$$

Since n and c are relatively prime, it follows by Theorem 1.4.3 that $[c]_n^{-1}$ exists. So we multiply each side of the equation on the right by $[c]_n^{-1}$ to obtain

$$[a]_n[c]_n[c]_n^{-1} = [b]_n[c]_n[c]_n^{-1}.$$

Hence $\quad [a]_n[1]_n = [b]_n[1]_n$

and so $\quad [a]_n = [b]_n.$

Therefore $\quad a \equiv b \bmod n$ as required. □

Comment The idea of dividing each side of an equation by the same thing is surely familiar and is used elsewhere in this book (e.g. in the last part of the proof of the next result). Care must be taken, however, because dividing by something is really multiplying by the inverse of that thing and not every congruence class has an inverse. Dividing can be hazardous – it is easy, if you are not experienced, to 'divide by 0': better to multiply by the inverse since doing that explicitly points up the issue of whether the inverse exists.

Note The assumption in 1.4.4 that $(c, n) = 1$ is needed. For example $30 \equiv 6 \bmod 8$, but if we try to divide both sides by 2 (which is *not* relatively prime to 8) then we get '$15 \equiv 3 \bmod 8$', which is false. On the other hand since $(3,8) = 1$ we *can* divide both sides by 3 to obtain the congruence $10 \equiv 2 \bmod 8$.

Corollary 1.4.5 *Let n be an integer greater than* 1. *Then each non-zero element of $\mathbb{Z}_n$ is either invertible or a zero-divisor, but not both.*

Proof Suppose that $[a]_n$ is not invertible. So, by Theorem 1.4.3, the greatest common divisor, d, of n and a is greater than 1. Since d divides a and n we have that $a = kd$ for some k and also $n = td$ where t is a positive integer necessarily less than n. It follows that $at = ktd$ is divisible by n. Hence

$$[a]_n[t]_n = [0]_n$$

and so, since $[t]_n \neq [0]_n$, $[a]_n$ is indeed a zero-divisor.

To see that an element cannot be both invertible and a zero-divisor, suppose that $[a]_n$ is invertible. Then, given any equation $[a]_n[b]_n = [0]_n$, we can multiply both sides by $[a]_n^{-1}$ and simplify to obtain $[b]_n = [0]_n$, so, from the definition, $[a]_n$ is not a zero-divisor. □

Comment If the first part of the argument is not clear to you then run through it with some numbers in place of n and a (and hence d).

Example This corollary implies that every non-zero congruence class in, for example, $\mathbb{Z}_{14}$ is invertible or a zero-divisor, but not both. By Theorem 1.4.3 the invertible congruence classes are $[1]_{14}$, $[3]_{14}$, $[5]_{14}$, $[9]_{14}$, $[11]_{14}$ and $[13]_{14}$. By Corollary 1.4.5 all the rest are zero-divisors. We can see all this explicitly: for invertibility we have $[1]_{14}^2 = [1]_{14}$, $[3]_{14} \cdot [5]_{14} = [1]_{14}$, $[9]_{14} \cdot [11]_{14} = [1]_{14}$, $[13]_{14}^2 = [-1]_{14}^2 = [1]_{14}$; also $[2]_{14} \cdot [7]_{14} = [0]_{14}$ and so each of $[4]_{14}$, $[6]_{14}$, $[8]_{14}$, $[10]_{14}$, $[12]_{14}$, multiplied by $[7]_{14}$ gives $[0]_{14}$ and hence is a zero-divisor.

The result shows that these new arithmetic structures $\mathbb{Z}_n$ can be rather strange: they can have elements which are not zero but which multiply together to give zero, so working in them requires some care.

The next result says that if we are working modulo a prime then things are better (but we still have to remember that non-zero elements can *add* together to give zero: there is no concept in $\mathbb{Z}_n$ of an element being ‘greater than zero’).

This next result, in essentially this form, was given by Euler.

Corollary 1.4.6 *Let p be a prime. Then every non-zero element of $\mathbb{Z}_p$ is invertible.*

Proof If $[a]_p$ is non-zero then p does not divide a and so a and p are relatively prime. Then the result follows by Theorem 1.4.3. □

To conclude this section, we consider a special subset of $\mathbb{Z}_n$.

Definition Let n be an integer greater than 1. We denote by G_n (some authors write $\mathbb{Z}_n^*$) the set of invertible congruence classes of $\mathbb{Z}_n$. By 1.4.3 $[a]_n$ is in G_n if and only if a is relatively prime to n.

Theorem 1.4.7 *Let n be an integer greater than or equal to 2. The product of any two elements of G_n is in G_n.*

Proof Suppose that $[a]$ and $[b]$ are in G_n. So each of a and b is relatively prime to n. Since any prime divisor, p, of ab must also divide one of a or b (by 1.3.1) it follows that ab and n have no prime common factor and hence no common factor greater than 1. Therefore, by 1.4.3, ab is invertible modulo n. □

Example When n is 20, G_n consists of the classes

$$[1], [3], [7], [9], [11], [13], [17], [19].$$

We can form the multiplication table for G_{20} as follows, where we write $[a]_{20}$ more simply as a.

	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

Observe the way in which the above 8 by 8 table breaks into four 4 by 4 blocks. We shall see later (in Section 5.3) why this happens.

Of course, 1.4.7 may be extended (by induction) to the statement that the product of any finite number of, possibly repeated, elements of G_n lies in G_n. A particular case of this is obtained when all the elements are equal: that is, if a is any member of G_n then every positive power a^k is in G_n. It is easy to show (again, by induction) that the inverse of a^k is $(a^{-1})^k$: for this, the notation a^{-k} is employed.

Exercises 1.4

1. Determine which of the following are true (a calculator will be useful for the larger numbers):
   (i) $8 \equiv 48 \bmod 14$, (ii) $-8 \equiv 48 \bmod 14$,
   (iii) $10 \equiv 0 \bmod 100$, (iv) $7754 \equiv 357482 \bmod 3643$,
   (v) $16023 \equiv 1325227 \bmod 25177$, (vi) $4015 \equiv 33303 \bmod 1295$.
2. Construct the addition and multiplication tables for $\mathbb{Z}_n$ when n is 6 and when n is 7.
3. Find the following inverses, if they exist:
   (i) the inverse of 7 modulo 11;
   (ii) the inverse of 10 modulo 26;
   (iii) the inverse of 11 modulo 31;
   (iv) the inverse of 23 modulo 31;
   (v) the inverse of 91 modulo 237.
4. Write down the multiplication table for G_n when n is 16 and when n is 15.
5. Show that no integer of the form $8n + 7$ can be written as a sum of three squares.
6. Let p be a prime number. Show that the equation $x^2 = [1]_p$ has just two solutions in $\mathbb{Z}_p$.
7. Let p be a prime number. Show that

$$(p-1)! \equiv -1 \bmod p.$$

8. Choose a value of n and count the number of elements in G_n. Try this with various values of n. Can you discover any rules governing the relation between n and the number of elements in G_n? [In Section 1.6 below we give rules for computing the number of elements in G_n directly from n.]
9. The observation that $10 \equiv 1 \bmod 9$ is the basis for the procedure of 'casting out nines'. The method is as follows.
   Given an integer X written in base 10 (as is usual), compute the sum of the digits of X: call the result the **digit sum** of X. If the digit sum is greater than 9, we form the digit sum again. Continue in this way to obtain the **iterated digit sum** which is at most 9. (Thus 5734 has digit sum 19 which has digit sum 10 which has digit sum 1, so the iterated digit sum of 5734 is 1.)
   Now suppose that we have a calculation which we want to check by hand: say, for example, someone claims that

   $$873\,985 \times 79\,041 = 69\,069\,967\,565.$$

   Compute the iterated digit sums of 873 985 and 79 041 (these are 4 and 3 respectively), multiply these together (to get 12), and form the iterated digit sum of the product (which is 3). Then the result should equal the iterated digit sum of 69 069 967 565 (which is 5). Since it does not, the 'equality' is incorrect. If the results had been equal then all we could say would be that no error was detected.
   (i) Using the method of casting out nines what can you say about the following computations?

   $$56\,563 \times 9961 = 563\,454\,043;$$
   $$1234 \times 5678 \times 901 = 6\,213\,993\,452;$$
   $$333 \times 666 \times 999 = 221\,556\,222.$$

   (ii) The following equation is false but you are told that only the underlined digit is in error. What is the correct value for that digit?

   $$674\,532 \times 9764 = 6\,586\,1\underline{4}0\,448.$$

   (iii) Justify the method of casting out nines.

1.5 Solving linear congruences

A **linear congruence** is an 'equation' of the form

$$ax \equiv b \bmod n$$

where x is an integer variable. Written in terms of congruence classes this becomes the equation

$$[a]_n X = [b]_n$$

where a solution X is now to be a congruence class.

Such an equation may have

(i) no solution (as, for example, $2x \equiv 1 \bmod 4$),
(ii) exactly one solution (for example $2x \equiv 1 \bmod 5$), or
(iii) more than one solution (for example the congruence $2x \equiv 0 \bmod 4$ discussed at the beginning of Section 1.4).

The first result shows how to distinguish between these cases and how to find all solutions for such a congruence (if there are any). This result was first given by Brahmagupta (c. 628). Of course he did not express it as we have done: rather he gave the criterion for solvability of, and the general solution of, $ak + nt = b$, where a, n, b are fixed integers and k and t are integer unknowns. (Note that if we have solved $ax \equiv b \bmod n$ then if k is a solution for x we have that n divides $ak - b$, that is, $ak - b = ns$ for some integer s so, writing t for $-s$, we have $ak + nt = b$. Since a, k, n and b are known we compute t from this equation. Therefore solving $ak + nt = b$ for k and t is equivalent to solving the congruence $ax \equiv b \bmod n$ for x.) An equation of the form $ak + nt = b$ is 'indeterminate' in the sense that, since it is just one equation with two unknowns, it has infinitely many solutions if it has any at all. One sees, however, that the solutions form themselves into complete congruence classes.

Theorem 1.5.1 *The linear congruence*

$$ax \equiv b \bmod n$$

has solutions if and only if the greatest common divisor, d, of a and n divides b. If d does divide b there are d solutions up to congruence modulo n, and these solutions are all congruent modulo n/d.

Proof Suppose that there is a solution, c say, to

$$ax \equiv b \bmod n.$$

Then, since

$$ac \equiv b \bmod n,$$

we have that n divides $ac - b$; say

$$ac - b = nk.$$

Rearrange this to obtain

$$b = ac - nk.$$

The greatest common divisor d of a and n divides both terms on the right-hand side of this equation, and hence we deduce that d divides b, as claimed.

Conversely, suppose d divides b, say $b = de$. Write d as a linear combination of a and n; say

$$d = ak + nt.$$

Multiply this by e to obtain

$$b = ake + nte.$$

This gives

$$a(ke) \equiv b \bmod n,$$

and so the congruence has a solution, ke, as required. Therefore the first assertion of the theorem has been proved.

Suppose now that c is a solution of

$$ax \equiv b \bmod n.$$

So as before we have

$$ac = b + nk$$

for some integer k. By the above, d divides b and hence we may divide this equation by d to get the equation in integers

$$(a/d)\,c = b/d + (n/d)k.$$

Thus

$$(a/d)\,c \equiv b/d \bmod\ (n/d).$$

That is, every solution of the original congruence is also a solution of the congruence

$$(a/d)\,x \equiv b/d \bmod (n/d).$$

Conversely it is easy to see (by reversing the steps) that every solution to this second congruence is also a solution to the original one. So the solution is really a congruence class modulo n/d. Such a congruence class splits into d distinct congruence classes modulo n. Namely if c is a solution then the congruence classes of

$$c, c + (n/d), c + 2\,(n/d), c + 3\,(n/d), \ldots, c + (d-1)\,(n/d)$$

are distinct solutions modulo n, and are all the solutions modulo n. □

Comment We strongly suggest working through the above proof with particular values for a, b and n (say, the values from Example 3 (or 4) below). Try running the proof with particular numbers parallel to the proof with letters to see how the general and special cases relate to each other.

This yields the following method for solving a linear congruence.

To find all solutions of the linear congruence $ax \equiv b \bmod n$.

1. Calculate $d = (a, n)$.
2. Test whether d divides b.
   (a) If d does not divide b then there is no solution.
   (b) If d divides b then there are d solutions mod n.
3. To find the solutions in case (b), 'divide the congruence throughout by d' to get
$$(a/d)\,x \equiv (b/d) \bmod (n/d).$$
   Notice that since a/d and n/d have greatest common divisor 1, this congruence will have a unique solution.
4. Calculate the inverse $[e]_{n/d}$ of $[a/d]_{n/d}$ (by inspection or by the matrix method).
5. Multiply to get
$$[x]_{n/d} = [e]_{n/d}[b/d]_{n/d}$$
   and calculate a solution, c, for x.
6. The solutions to the original congruence will be the classes modulo n of
$$c, c + (n/d), \ldots, c + (d-1)(n/d).$$

Example 1 Solve the congruence

$$6x \equiv 5 \bmod 17.$$

Since $(6, 17) = 1$ and 1 divides 5 there is, by Theorem 1.5.1, a unique solution modulo 17. It is found by calculating $[6]_{17}^{-1}$ (found by inspection to be $[3]_{17}$) and multiplying both sides by this inverse. We obtain

$$x \equiv 3 \times 5 \equiv 15 \bmod 17$$

as the solution (unique up to congruence mod 17). (Therefore the values of x which are solutions are $\ldots, -19, -2, 15, 32, \ldots$.)

Example 2 To solve

$$6x \equiv 5 \bmod 15$$

note that $(6, 15) = 3$ and 3 does not divide 5, so by 1.5.1 there is no solution.

Example 3 In the congruence

$$6x \equiv 9 \bmod 15,$$

$(6, 15) = 3$ and 3 divides 9, so by 1.5.1 there are three solutions up to congruence modulo 15.

To find these we find the solutions up to congruence modulo 5 ($5 = 15/3$), and we do this by dividing the whole congruence by the greatest common divisor of 6 and 15. This gives

$$2x \equiv 3 \bmod 5.$$

Now, $(2, 5) = 1$ so there is a unique solution (this is the point of dividing through by the gcd). One quickly sees that

$$x \equiv 4 \bmod 5$$

is the unique solution mod 5. The proof of 1.5.1 shows that the solutions of the original congruence are therefore the members of the congruence class $[4]_5$. In order to describe the solutions in terms of congruence classes modulo 15, we note that $[4]_5$ splits up as

$$[4]_{15}, [4 + 5]_{15}, [4 + 10]_{15}$$

that is, as

$$[4]_{15}, [9]_{15}, [14]_{15}.$$

Example 4 Solve the congruence

$$432x \equiv 12 \bmod 546.$$

The first task is to calculate the greatest common divisor of 432 and 546. Since we do not need to express this as a linear combination of 432 and 546 it is not necessary to use the matrix method: it is enough to factorise these numbers. We have that 432 is 6 times 72 while 546 is 6 times 91: since 91 is 7 × 13 and 72 is 8 × 9 one sees that 432 and 546 have no common factor greater than 6. Dividing the congruence by 6 gives

$$72x \equiv 2 \bmod 91.$$

The next task is to find the inverse of 72 modulo 91, and unless the reader is unusually gifted at arithmetic calculations, this is best done using the matrix method:

$$\left(\begin{array}{cc|c} 1 & 0 & 91 \\ 0 & 1 & 72 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 19 \\ 0 & 1 & 72 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -1 & 19 \\ -3 & 4 & 15 \end{array}\right) \to \left(\begin{array}{cc|c} 4 & -5 & 4 \\ -3 & 4 & 15 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 4 & - 5 & 4 \\ -15 & 19 & 3 \end{array}\right) \to \left(\begin{array}{cc|c} 19 & -24 & 1 \\ -15 & 19 & 3 \end{array}\right).$$

The top line of this matrix corresponds to the equation $19 \cdot 91 - 24 \cdot 72 = 1$ so it follows that the inverse of 72 modulo 91 is -24, or 67. So multiply both sides of the congruence by 67 to obtain

$$\begin{aligned} x &\equiv 2 \times 67 \bmod 91 \\ &\equiv 134 \bmod 91 \\ &\equiv 43 \bmod 91. \end{aligned}$$

Finally, to describe the solutions in terms of congruence classes modulo 546, we have that $[43]_{91}$ splits into six congruence classes modulo 546, namely

$$[43]_{546}, [134]_{546}, [225]_{546}, [316]_{546}, [407]_{546}, [498]_{546}.$$

Next we consider how to solve systems of linear congruences.

Suppose that we wish to find an integer which, when divided by 7 has a remainder of 3, and when divided by 25 has a remainder of 6. Is there such an integer? and if so how does one find it?

This question may be formulated in terms of congruences as:
find an integer x that satisfies

$$x \equiv 3 \bmod 7 \text{ and } x \equiv 6 \bmod 25.$$

The next theorem implies that there is a simultaneous solution to these congruences, and its proof tells us how to find a solution.

The theorem may have been known to the eighth century Buddhist monk Yi Xing. Certainly it appears in Qín Jiǔsháo's *Shù shū jiǔ zhāng* (*Mathematical Treatise in Nine Sections*) of 1247.

Theorem 1.5.2 (Chinese Remainder Theorem) *Suppose that $m \geq 2$ and $n \geq 2$ are relatively prime integers and that a and b are any integers. Then there is a simultaneous solution to the congruences*

$$\begin{aligned} x &\equiv a \bmod m, \\ x &\equiv b \bmod n. \end{aligned}$$

The solution is unique up to congruence mod mn.

Proof Since m and n are relatively prime, there exist integers k and t such that

$$mk + nt = 1. \qquad (*)$$

Then it is easily checked that $c = bmk + ant$ is a simultaneous solution for the congruences. For,

$$c \equiv ant \bmod m$$

and, from equation (∗)

$$nt \equiv 1 \bmod m.$$

Hence

$$c \equiv a \times 1 = a \bmod m.$$

The proof that c is congruent to b modulo n is similar.

To show that the solution is unique up to congruence modulo mn, suppose that each of c, d is a solution to both congruences. Then

$$c \equiv a \bmod m \text{ and } d \equiv a \bmod m.$$

Hence

$$c - d \equiv 0 \bmod m.$$

Similarly

$$c - d \equiv 0 \bmod n.$$

That is, $c - d$ is divisible by both m and n. Since m and n are relatively prime it follows by Theorem 1.1.6(ii) that $c - d$ is divisible by mn, and hence c and d lie in the same congruence class mod mn.

Conversely, if c is a solution to both congruences and if

$$d \equiv c \bmod mn$$

then d is of the form $c + kmn$, and so the remainder when d is divided by m or n is the same as the remainder when c is divided by m or n. So d solves both congruences, as required. □

Comment For the first part of the proof (existence of a solution) notice that the equation $mk + nt = 1$, when reduced modulo n, becomes $[mk]_n = [1]_n$ so, if we multiply both sides by $[b]_n$ we obtain $[bmk]_n = [b]_n$. That is where the term bmk in $c = bmk + ant$ comes from, similarly (reducing mod m) for the other term.

Example Consider the problem, posed before the statement of Theorem 1.5.2, of finding a solution to the congruences

$$x \equiv 3 \bmod 7 \text{ and } x \equiv 6 \bmod 25.$$

First, find a combination of 7 and 25 which is 1: one such combination is

$$7(-7) + 25 \times 2 = 1.$$

Then we multiply these two terms by 6 and 3 respectively. (Note the 'swop over'!) This gives us

$$6 \cdot 7 \cdot (-7) + 3 \cdot 25 \cdot 2 = -144.$$

So the solution is $[-144]_{175}$ ($175 = 7 \cdot 25$). We should put this in standard form by adding a suitable multiple of 175: we obtain that the solution is $[31]_{175}$.

Alternatively, there is a method for solving this type of problem which does not involve having to remember how to construct the solution. We repeat the above example to illustrate this method.

A solution of the first congruence is of the form

$$x = 3 + 7k,$$

so if x satisfies the second congruence, we have

$$3 + 7k \equiv 6 \bmod 25.$$

Now solve this congruence for k: we have

$$7k \equiv 3 \bmod 25.$$

The inverse of 7 modulo 25 is 18 (by inspection), so

$$\begin{aligned} k &\equiv 3 \times 18 \bmod 25 \\ &\equiv 4 \bmod 25. \end{aligned}$$

Thus, for some integer r,

$$\begin{aligned} x &= 3 + 7(4 + 25r) \\ &= 3 + 28 + 175r \\ &= 31 + 175r \end{aligned}$$

as before.

Each of these methods allows us to solve systems of more than two congruences, so long as the 'moduli' are pairwise relatively prime, by solving two congruences at a time. Actually in the *Mathematical Treatise in Nine Sections* there are examples to show that the idea behind the method may sometimes be applied even if the moduli are not all pairwise relatively prime (see [Needham, Section 19 (i) (4)] or [Li Yan and Du Shiran, p. 165]).

Example Solve the simultaneous congruences

$$\begin{aligned} x &\equiv 2 \bmod 7 \\ x &\equiv 0 \bmod 9 \\ 2x &\equiv 6 \bmod 8. \end{aligned}$$

Observe that the third congruence is not in an immediately usable form, so we first solve it to obtain the two (since $(2, 8) = 2$) solutions:

$$x \equiv 3 \bmod 8 \text{ and } x \equiv 7 \bmod 8.$$

So now we have two sets of three congruences to solve, and we could treat these as entirely separate problems, only combining the solutions at the end. We may note, however, that there is no need to separate the solution for the third congruence into two solutions modulo 8, since the solution is really just the congruence class $[3]_4$. Thus we reduce to solving the simultaneous congruences

$$\begin{aligned} x &\equiv 2 \bmod 7 \\ x &\equiv 0 \bmod 9 \\ x &\equiv 3 \bmod 4. \end{aligned}$$

Since $(7, 9) = 1 = (7, 4) = (9, 4)$ we will be able to apply 1.5.2. Take (say) the first two congruences to solve together. We have

$$7 \cdot (-5) + 9 \cdot 4 = 1,$$

so a solution to the first two is:

$$0 \cdot 7(-5) + 2 \cdot 9 \cdot 4 = 72 \bmod 7 \cdot 9.$$

This simplifies to 9 mod 63. So now the problem has been reduced to solving

$$\begin{aligned} x &\equiv 9 \bmod 63 \\ x &\equiv 3 \bmod 4. \end{aligned}$$

We have

$$16 \cdot 4 - 1 \cdot 63 = 1.$$

This gives

$$9 \cdot 16 \cdot 4 - 3 \cdot 1 \cdot 63 \bmod 63 \cdot 4$$

as the solution. This simplifies to 135 mod 252.

Finally, in this section, we briefly consider solving non-linear congruences. There are many deep and difficult problems here and to give a reasonable account would take us very far afield. So we content ourselves with merely indicating a few points (below, and in the exercises).

Example Consider the quadratic equation

$$x^2 + 1 \equiv 0 \bmod n.$$

The existence of solutions, as well as the number of solutions, depends on n. For example, when n is 3, we can substitute the three congruence classes $[0]_3$, $[1]_3$ and $[2]_3$ into the equation to see that $x^2 + 1$ is never $[0]_3$. When n is 5, it can be seen that $[2]_5$ and $[3]_5$ are solutions. If n is 65, it can be checked that $[8]_{65}$, $[-8]_{65}$, $[18]_{65}$ and $[-18]_{65}$ are all solutions, and this leads to the (different) factorisations

$$\begin{aligned} x^2 + 1 &\equiv (x + 8)(x - 8) \bmod 65 \\ &\equiv (x + 18)(x - 18) \bmod 65. \end{aligned}$$

When n is a prime, however, to the extent that a polynomial can be factorised, the factorisation is unique.

Example Consider the polynomial $x^3 - x^2 + x + 1$: does it have any integer roots? Suppose that it had an integer root k: then we would have $k^3 - k^2 + k + 1 = 0$. Let n be any integer greater than 1, and reduce this equation modulo n to obtain

$$[k]_n^3 - [k]_n^2 + [k]_n + [1]_n = [0]_n.$$

So we would have that the polynomial $X^3 - X^2 + X + [1]_n$ with coefficients from $\mathbb{Z}_n$ has a root in $\mathbb{Z}_n$. This would be true for *every* n.

Let us take $n = 2$: so reducing $x^3 - x^2 + x + 1 = 0$ modulo 2 gives $X^3 - X^2 + X + [1]_2$. It is straightforward to check whether or not this equation has a solution in $\mathbb{Z}_2$: all we have to do is to substitute $[0]_2$ and $[1]_2$ in turn. Doing this, we find that $[1]_2$ is a root. This tells us nothing about whether or not the original polynomial has a root.

So we try taking $n = 3$: reduced modulo 3, the polynomial becomes $X^3 - X^2 + X + [1]_3$. Let us see whether this has a root in $\mathbb{Z}_3$. Substituting in turn $[0]_3$, $[1]_3$ and $[2]_3$ for X we get the values $[1]_3$, $[2]_3$ and $[1]_3$ for the polynomial. In particular none of these is zero, so the polynomial has no root modulo 3. Therefore the original polynomial has no integer root (for by the argument above, if it did, then it would also have to have a root modulo 3). In Chapter 6 we look again at polynomials with coefficients which are congruence classes.

Exercises 1.5

1. Find all the solutions (when there are any) of the following linear congruences:

   (i) $3x \equiv 1 \bmod 12$;

   (ii) $3x \equiv 1 \bmod 11$;

   (iii) $64x \equiv 32 \bmod 84$;

(iv) $15x \equiv 5 \bmod 17$;
(v) $15x \equiv 5 \bmod 18$;
(vi) $15x \equiv 5 \bmod 100$;
(vii) $23x \equiv 16 \bmod 107$.

2. Solve the following sets of simultaneous linear congruences:
   (i) $x \equiv 4 \bmod 24$ and $x = 7 \bmod 11$;
   (ii) $3x \equiv 1 \bmod 5$ and $2x \equiv 6 \bmod 8$;
   (iii) $x \equiv 3 \bmod 5$, $2x \equiv 1 \bmod 7$ and $x \equiv 3 \bmod 8$.
3. Find the smallest positive integer whose remainder when divided by 11 is 8, which has last digit 4 and is divisible by 27.
4. (i) Show that the polynomial $x^4 + x^2 + 1$ has no integer roots, but that it has a root modulo 3, and factorise it over $\mathbb{Z}_3$.
   (ii) Show that the equation $7x^3 - 6x^2 + 2x - 1 = 0$ has no integer solutions.
5. A hoard of gold pieces 'comes into the possession of' a band of 15 pirates. When they come to divide up the coins, they find that three are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns there remain only 7 pirates capable of making an effective claim on the hoard. When, however, the hoard is divided between these seven it is found that two pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the four pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces which could have been in the hoard?

1.6 Euler's Theorem and public key codes

Suppose that we are interested in the behaviour of integers modulo 20. Fix an integer a and then form the successive powers of its congruence class:

$$[a]_{20}, [a]_{20}^2, [a]_{20}^3, \ldots, [a]_{20}^n, \ldots$$

What can happen? Let us try some examples (write '[3]' for '$[3]_{20}$' etc.). Taking $a = 3$ we obtain

$$[3]^1 = [3],\ [3]^2 = [9],\ [3]^3 = [27] = [7],$$
$$[3]^4 = [3]^3[3] = [7][3] = [21] = [1],\ [3]^5 = [3]^4[3] = [1][3] = [3],$$
$$[3]^6 = [3]^2 = [9],\ [3]^7 = [3]^3 = [7],\ [3]^8 = [1],\ [3]^9 = [3], \ldots$$

Observe that the successive powers are different until we reach [1] and then the pattern starts to repeat.

If we take $a = 4$ then the pattern of powers is somewhat different, in that [1] is never reached:

$$[4]^1 = [4],\ [4]^2 = [16],\ [4]^3 = [64] = [4],\ [4]^4 = [16], \ldots$$

Taking $a = 10$ the sequence of powers of $[10]_{20}$ is:

$$[10],\ [100] = [0],\ [0],\ [0], \ldots$$

If we take $a = 11$ then the behaviour is similar to that when $a = 3$; we reach [1] and then the pattern repeats from the beginning:

$$[11],\ [1],\ [11],\ [1],\ [11], \ldots$$

Those congruence classes, like $[3]_{20}$ and $[11]_{20}$, which have some power equal to the class of 1 are of particular significance. In this section we will give a criterion for a congruence class to be of this form and we examine the behaviour of such classes.

Definition Let n be a positive integer greater than 1. The integer a is said to have **finite multiplicative order modulo** n if there is a positive integer k such that

$$[a]_n^k\ (= [a^k]_n) = [1]_n.$$

Thus $[3]_{20}$ and $[11]_{20}$ have finite multiplicative order, but $[4]_{20}$ and $[10]_{20}$ do not. Similarly if n is 6, then for all k

$$[3]_6^k = [3]_6$$

and so 3 does not have finite multiplicative order modulo 6.

Going beyond examples, we now give a general result which explains what can happen with finite multiplicative order.

Theorem 1.6.1 *The integer a has finite multiplicative order modulo n if, and only if, a is relatively prime to n.*

Proof Fix a and n and suppose that there is a positive integer k such that

$$[1]_n = [a^k]_n = [a^{k-1}]_n\,[a]_n.$$

It follows that $[a]_n$ has an inverse, namely $[a^{k-1}]_n$, and so, by Theorem 1.4.3, a is relatively prime to n.

Conversely, suppose that a and n are relatively prime so, by 1.4.3, $[a]_n$ has an inverse and hence, by 1.4.7 (and the comment after that), all its powers $[a]_n^k$

have inverses. Now consider the $n+1$ terms

$$[a], [a]^2, \ldots, [a]^{n+1}.$$

Since $\mathbb{Z}_n$ has only n distinct elements, at least two of these powers are equal as elements of $\mathbb{Z}_n$: say

$$[a]^k = [a]^t \text{ where } 1 \leq k < t \leq n+1$$

(so note that $1 \leq t - k$).

Take both terms to the same side and factorise to get

$$[a]^k([1] - [a]^{t-k}) = [0].$$

Multiplying both sides of the equation by $[a]^{-k}$ and simplifying, we obtain

$$[1] - [a]^{t-k} = [0].$$

This may be rewritten as

$$[a]^{t-k} = [1]$$

and so a does have finite multiplicative order modulo n. □

Definition If a has finite multiplicative order modulo n, then the **order** of a modulo n is the smallest positive integer k such that

$$[a]_n^k = [1]_n,$$

(or in terms of congruences $a^k = 1 \bmod n$.)

We also say, in this case, that the **order** of the congruence class $[a]_n$ is k.

Example 1 The discussion at the beginning of the section shows that the order of 3 modulo 20 is 4 and the order of 11 modulo 20 is 2.

Example 2 Since the first three powers of 2 are 2, 4 and 8, it follows that 2 has order 3 modulo 7. Similarly it can be seen that 3 has order 6 modulo 7.

Example 3 When n is 17, we see that

$$2^4 \equiv -1 \bmod 17$$

and so it follows that $[2]_{17}$ has order 8. (To see this, square each side to obtain $2^8 \equiv 1 \equiv 2^0 \bmod 17$. It then follows, by 1.6.2 below, that the order of $[2]_4$ is a divisor of 8. It cannot be 1, 2 or 4 because $2^4 \not\equiv 1 \bmod 17$, so must be 8.) Also, since

$$13^2 = 169 \equiv -1 \bmod 17,$$

so

$$13^4 \equiv (-1)^2 \equiv 1 \bmod 17,$$

we deduce that $[13]_{17}$ has order 4. Notice that this also implies that the inverse of 13 modulo 17 is 4 since

$$13^3 \equiv -1 \cdot 13 = -13 \equiv 4 \bmod 17,$$

and so

$$13 \cdot 4 \equiv 13 \cdot 13^3 \equiv 13^4 \equiv 1 \bmod 17.$$

The next theorem explains the periodic behaviour of the powers of 3 and 11 mod 20, seen at the beginning of this section.

Theorem 1.6.2 *Suppose that a has order k modulo n. Then*

$$a^r \equiv a^s \bmod n$$

if, and only if,

$$r \equiv s \bmod k.$$

Proof If

$$r \equiv s \bmod k$$

then r has the form $s + kt$ for some integer t, and so

$$\begin{aligned} a^r &= a^{s+kt} \\ &= a^s(a^{kt}) \\ &= a^s(a^k)^t \\ &\equiv a^s(1)^t \bmod n \\ &\equiv a^s \bmod n. \end{aligned}$$

Conversely, if

$$a^r \equiv a^s \bmod n,$$

then suppose, without loss of generality, that r is less than or equal to s. Since, by Theorem 1.6.1, a is relatively prime to n, it follows, by Theorems 1.4.3 and 1.4.7, that a^r has an inverse modulo n. Multiplying both sides of the above congruence by this inverse gives

$$1 \equiv a^{s-r} \bmod n.$$

Now write $s - r$ in the form

$$s - r = qk + u$$

where u is a natural number less than k. It then follows, as in the proof of the first part, that

$$a^{s-r} \equiv a^u \bmod n,$$

and so

$$a^u \equiv 1 \bmod n.$$

The minimality of k forces u to be 0.
Hence

$$r \equiv s \bmod k. \qquad \square$$

We now turn our attention to the possible orders of elements in $\mathbb{Z}_n$, considering first the case when n is prime. This result was announced by Pierre de Fermat in a letter of 1640 to Frénicle de Bessy, in which Fermat writes that he has a proof. Fermat states his result in the following words: 'Given any prime p, and any geometric progression 1, a, a^2, etc., p must divide some number $a^n - 1$ for which n divides $p - 1$: if then N is any multiple of the smallest n for which this is so, p divides also $a^N - 1$'. We use the language of congruence to restate this as follows.

Theorem 1.6.3 (Fermat's Theorem) *Let p be a prime and suppose that a is an integer not divisible by p. Then*

$$[a]_p^{p-1} = [1]_p.$$

That is,

$$a^{p-1} \equiv 1 \bmod p.$$

Therefore, for any integer a

$$a^p \equiv a \bmod p.$$

Proof Let G_p be the set of invertible elements of $\mathbb{Z}_p$, so by Corollary 1.4.6, G_p consists of the $p - 1$ elements

$$[1]_p, [2]_p, \ldots, [p-1]_p.$$

Denote by $[a]G_p$ the set of all multiples of elements of G_p by $[a]$:

$$\begin{aligned}[a]G_p &= \{[a][b] : [b] \text{ is in } G_p\}\\ &= \{[a][1], [a][2], \ldots, [a][p-1]\}.\end{aligned}$$

Since $[a]$ is in G_p it follows by Theorem 1.4.7 that every element in $[a]G_p$ is in G_p. No two elements $[a][b]$ and $[a][c]$ of $[a]G_p$ with $[b] \neq [c]$ are equal since, if

$$[a][b] = [a][c]$$

then, by Corollary 1.4.4,

$$[b] = [c].$$

It follows, since the sets $[a]G_p$ and G_p have the same finite number of elements, that the sets $[a]G_p$ and G_p are equal. Now, multiply all the elements of G_p together to obtain the element

$$[N] = [1][2]\cdots[p-1].$$

By Theorem 1.4.7, $[N]$ is in G_p. Since the set G_p is equal to the set $[a]G_p$ (though the elements might be written in a different order), multiplying all the elements of $[a]G_p$ together must give us the same result:

$$[1][2]\cdots[p-1] = [a][1] \times [a][2] \times \cdots [a][p-1].$$

Collecting together all the '$[a]$' terms shown on the right-hand side we deduce that

$$[N] = [a]^{p-1}[N].$$

Since $[N]$ is in G_p, it is invertible: so we may cancel, by Corollary 1.4.4, to obtain

$$[1] = [a]^{p-1},$$

as required.

Finally, notice that for any integer a, either a is divisible by p, in which case a^p is also divisible by p, or a is not divisible by p, in which case, as we have just shown,

$$a^{p-1} \equiv 1 \bmod p.$$

Thus, in either case,

$$a^p \equiv a \bmod p. \qquad \square$$

Comment Run through the proof with particular (small) values for a and p to see, first, how multiplication by $[a]$ just rearranges the non-zero congruence classes and, second, how the cancellation argument involving $[N]$ works. For the purpose of understanding the proof it is better to leave $[N]$ as a product of terms rather than calculate its value. (It is, however, an interesting exercise to calculate the value of $[N]$: to explain what you find see Exercise 1.4.7.)

Corollary 1.6.4 *Let p be a prime number and let a be any integer not divisible by p. Then the order of a* mod p *divides* $p - 1$.

Proof This follows directly from the above theorem and 1.6.2. □

Warning The corollary above does *not* say that the order of a *equals* $p - 1$: certainly one has

$$a^{p-1} = 1 \bmod p,$$

but $p - 1$ need not be the lowest positive power of a which is congruent to 1 modulo p.

For example, consider the elements of G_7. The orders of its elements, $[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7$, are, respectively, 1, 3, 6, 3, 6, 2 (all, in accordance with Corollary 1.6.4, divisors of $6 = 7 - 1$).

Example 1 Let p be 17: so $p - 1$ is 16. It follows by Theorem 1.6.2 that 2^{100} is congruent to 2^4 modulo 17 since 100 ($= 6 \times 16 + 4$) is congruent to 4 modulo 16. That is,

$$\begin{aligned} 2^{100} &\equiv 2^4 \bmod 17 \\ &\equiv 16 \bmod 17. \end{aligned}$$

Example 2 When p is 101 we have, by the same sort of reasoning, that $15^{601} \equiv (15^{100})^6 \cdot 15 \equiv 1^6 \cdot 15 \equiv 15 \bmod 101$.

It is not known what Fermat's original proof of Theorem 1.6.3 was (it seems reasonable to suppose that he did in fact have a proof). The first published proof was due to Leibniz (1646–1716): it is very different from the proof we gave above, being based on the Binomial Theorem (see Exercise 1.6.4 for this alternative proof). In 1742 Euler found the same proof but, his interest in number theory having been aroused, he went on to discover (before 1750) a 'multiplicative proof' like that we gave above. In a sense, that proof is better since it deals only with the essential aspects of the situation and it generalises to give a proof of Euler's Theorem (below). Actually Euler's proof was closer to that we give for Lagrange's Theorem (Theorem 5.2.3).

By 1750 Euler had managed to generalise Fermat's Theorem to cover the case of any integer $n \geq 2$ in place of the prime p. The power $p - 1$ of Fermat's Theorem had to be interpreted correctly, since if n is an arbitrary integer then the order of an invertible element modulo n certainly need not divide $n - 1$. The point is that if p is prime then $p - 1$ is the number of invertible congruence classes modulo p: that is, the number of elements in G_p. The function which assigns to n the number of elements in G_n is referred to as **Euler's phi-function**. Euler introduced this function and described its elementary properties in his *Tractatus*.

Definition The number of elements in G_n is denoted by $\phi(n)$. Thus, by Theorem 1.4.3, $\phi(n)$ equals the number of integers between 1 and n inclusive which are relatively prime to n. The symbol ϕ used here is the Greek letter corresponding to the letter f in the Roman alphabet: in the Roman alphabet it is written 'phi' and pronounced accordingly. We will occasionally use other Greek letters in this book.

Theorem 1.6.5 *Suppose that p is a prime and let n be any positive integer. Then*

$$\phi(p^n) = p^n - p^{n-1}.$$

Proof The only integers beween 1 and p^n which have a factor in common with p^n are the integers which are divisible by p, namely

$$p, 2p, \ldots, p^2, \ldots, p^n = p^{n-1}p.$$

Thus there are p^{n-1} numbers in this range which are divisible by p and so there are $p^n - p^{n-1}$ numbers between 1 and p^n which are *not* divisible by p, i.e. which are relatively prime to p^n. □

Examples

$$\phi(5) = 4;$$
$$\phi(25) = \phi(5^2) = 5^2 - 5^1 = 20;$$
$$\phi(4) = \phi(2^2) = 2^2 - 2^1 = 2;$$
$$\phi(81) = \phi(3^4) = 3^4 - 3^3 = 54.$$

Theorem 1.6.6 *Let a and b be relatively prime integers. Then*

$$\phi(ab) = \phi(a)\,\phi\,(b).$$

Proof Let $[r]_a$ and $[s]_b$ be elements of G_a and G_b respectively. From $[r]_a$ and $[s]_b$ we will produce an element $[t]_{ab}$ which we will show lies in G_{ab}. By the Chinese Remainder Theorem (1.5.2) there is an integer t satisfying

$$t \equiv r \bmod a \text{ and}$$
$$t \equiv s \bmod b,$$

and t is uniquely determined up to congruence modulo ab. Now we show that the class $[t]_{ab}$ is invertible. Since we have $r = t + ka$ for some integer k, and since the gcd of r and a is 1, it follows by 1.1.4 that the gcd of t and a is 1. Similarly $(t, b) = 1$. Therefore, by Exercise 1.1.6 we may deduce that $(t, ab) = 1$. Hence $[t]_{ab}$ is in G_{ab}.

Next we show that every element $[t]_{ab}$ in G_{ab} comes from a pair consisting of an element $[r]_a$ in G_a and an element $[s]_b$ in G_b. So, given $[t]_{ab}$ in G_{ab}, let r be the standard representative for $[t]_a$. Since $(t, ab) = 1$, certainly $(t, a) = 1$. So, since t is of the form $r + ka$, we have (by 1.1.4) that $(r, a) = 1$, and hence $[r]_a$ is in G_a. Similarly if s is the standard representative for $[t]_b$, then $[s]_b$ is in G_b. It follows that each element $[t]_{ab}$ in G_{ab} determines (uniquely) a pair $([r]_a, [s]_b)$ where

$$t \equiv r \bmod a \text{ and}$$
$$t \equiv s \bmod b.$$

By the first paragraph (uniqueness of t up to congruence modulo ab), different elements of G_{ab} determine different pairs.

Now imagine writing down all the elements of G_{ab} in some order. Underneath each element $[t]_{ab}$ write the pair $([t]_a, [t]_b)$ $(([r]_a, [s]_b)$ in the notation used above). We have shown that the second row contains no repetitions, and also that it contains every possible pair of the form $([r]_a, [s]_a)$ with $[r]_a$ in G_a and $[s]_b$ in G_b (since every element of G_a can be paired with every element of G_b). Thus the numbers of elements in the two rows must be equal. The first row contains $\phi(ab)$ elements, and the second row contains $\phi(a)\,\phi\,(b)$ elements: thus $\phi(ab) = \phi(a)\,\phi\,(b)$, as required. □

Comment The reader may feel a little unsure about some points in the above proof. Within that proof we implicitly introduced two ideas which will be discussed at greater length in Chapter 2. The first of these is the idea of the Cartesian product, $X \times Y$, of sets X and Y. This is the set of all pairs of the form (x, y) with x in X and y in Y (and should not be confused with product in the arithmetic sense). The number of elements in $X \times Y$ is the product of the number of elements in X and the number of elements in Y. The second idea arises in the way in which we showed that the number of elements in the two sets G_{ab} and $G_a \times G_b$ are equal. The 'matching' obtained by writing the elements of the sets in two rows, one above the other, is an illustration of a bijective function, as we shall see in Section 2.3. This, rather than making a count of the elements, is the most common way in which pure mathematicians show that two sets have the same number of elements!

Examples

$$\phi(100) = \phi(25)\phi(4) = 20 \cdot 2 = 40;$$
$$\phi(14) = \phi(2)\phi(7) = 6;$$
$$\phi(41) = 40.$$

Now we come to Euler's generalisation of Fermat's Theorem.

Theorem 1.6.7 (Euler's Theorem) *Let n be greater than or equal to* 2 *and let a be relatively prime to n. Then*

$$[a]_n^{\phi(n)} = [1]_n$$

that is

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Proof The proof is a natural generalisation of that given for Fermat's Theorem. We have arranged matters so that we can repeat that proof almost unchanged.

Let G_n be the set of invertible elements of $\mathbb{Z}_n$. Denote by $[a]G_n$ the set of all multiples of elements of G_n by $[a]$:

$$[a]G_n = \{[a][b] : [b] \text{ is in } G_n\}.$$

Since $[a]$ is in G_n it follows by Theorem 1.4.7 that every element in $[a]G_n$ is in G_n. No two elements $[a][b]$ and $[a][c]$ of $[a]G_n$ with $[b] \neq [c]$ are equal, since if

$$[a][b] = [a][c]$$

then, by Corollary 1.4.4,

$$[b] = [c].$$

It follows that the sets $[a]G_n$ and G_n are equal.

Now multiply together all the elements of G_n to obtain an element $[N]$, say, and note that $[N]$ is in G_n by Theorem 1.4.7. Multiplying the elements of $[a]G_n$ together gives $[a]^{\phi(n)}[N]$ so, since the set G_n is equal to the set $[a]G_n$, we deduce that

$$[a]^{\phi(n)}[N] = [N].$$

Since $[N]$ is in G_n it is invertible and so, by Corollary 1.4.4, we may cancel to obtain

$$[a]^{\phi(n)} = [1],$$

as required. □

Corollary 1.6.8 *Suppose that n is a positive integer and let a be an integer relatively prime to n. Then the order of a* mod *n divides* $\phi(n)$.

Proof This follows directly from the theorem and 1.6.2. □

Example 1 Since $14 = 2 \cdot 7$, so $\phi(14) = \phi(2)\phi(7) = 6$, the value of 3^{19} modulo 14 is determined by the congruence class of 19 modulo 6 and so 3^{19} is congruent to 3^1, that is, to 3, modulo 14. More explicitly, $3^{19} \equiv (3^6)^3 \cdot 3^1 \equiv (1^3) \cdot 3^1 = 3 \bmod 14$ since $3^6 \equiv 1 \bmod 14$.

Example 2 Since the last two digits of a positive integer are determined by its congruence class modulo 100 and since $\phi(100) = \phi(2^2)\phi(5^2)$ is 40, we have that the last two digits of 3^{125} are 43, since

$$3^{125} \equiv (3^{40})^3 \times 3^5 \equiv (1)^3 \times 243 \equiv 43 \bmod 100.$$

Warning If the integers a and n are not relatively prime then, by 1.6.1 no power of a can be congruent to $1 \bmod n$, although it might happen that $a^{\phi(n)+1} \equiv a \bmod n$.

For instance, take $n = 100$ (so $\phi(n) = 40$) and $a = 5$: then it is easily seen (and proved by induction) that every power of a beyond the first is congruent to 25 mod 100 and so, in particular, $5^{\phi(n)+1}$ is not congruent to 5.

On the other hand, if one takes n to be 50 (so $\phi(n) = 20$) and a to be 2 then it does turn out that $2^{\phi(n)+1} \equiv 2 \bmod 50$ (in Exercise 1.6.8 you are asked to explain this).

To conclude this chapter, we discuss the idea of public key codes and how such codes may be constructed.

The traditional way to transmit and receive sensitive information is to have both sender and receiver equipped with a ‘code book’ which enables the sender to encode information and the receiver to decode the resulting message. It is a general feature of such codes that if one knows how to *en*code a message then one can in practice *de*code an intercepted message. Thus, if one wishes to receive sensitive information from a number of different sources, one is confronted with obvious problems of security.

The idea of a public key code is somewhat different. Suppose that the ‘receiver’ R wishes to receive information from a number of different sources $S_1, S_2, \ldots$ (R could be a company or bank headquarters, a computer database containing medical records, an espionage headquarters,... with the S_i being correspondingly branches, hospitals, field operatives,...) Rather than equipping each S_i with a ‘code book’, R provides, in a fairly public way, certain information which allows the S_i to encode messages. These messages may then be sent over public channels. The code is designed so that if some third party T intercepts a message then T will find it impossible in practice to decode the message *even if T has access to the information that tells the S_i how to encode messages*.

That is, decoding a message is somehow inherently more difficult than encoding a message, even if one has access to the ‘code book’.

Various ways of realising such a code in practice have been suggested (the idea of public key codes was put forward by Diffie and Hellman in 1976). One method is the ‘knapsack method’ (see [Salomaa, Section 7.3] for a description of this method). It seemed for a while that this provided a method for producing public key codes: it was however discovered by Shamir in 1982 that the method did not give an inherently ‘safe’ code, although it has since been modified to give what appears to be a safe code.

The mathematics of the method which we describe here is based on Euler’s Theorem. It is generally believed to be ‘inherently safe’, but there is no proof of that, and so it is not impossible that it will have to be fundamentally modified or replaced. The method is referred to as the RSA system, after its inventors: Rivest, Shamir and Adleman (1978). It also transpired that a group at GCHQ in the UK had come up with the same idea somewhat earlier but, for security reasons, it was kept secret (see www.cesg.gov.uk/publications/media/nsecret/ellis.pdf for details). The (assumed) efficacy of this type of code depends on the inherent difficulty of factorising a (very large!) integer into a product of primes. It has been shown by Rabin that deciphering (a variant of) this system is as difficult as factorising integers.

Construction of the code First one finds two very large primes (say about 100 decimal digits each). With the aid of a reasonably powerful computer it is very quickly checked whether a given number is prime or not, so what one could do in practice is to generate randomly a sequence of 100-digit numbers, check each in turn for primality, and stop when two primes have been found. Let us denote the chosen primes by p and q.

Set n equal to the product pq: this is one of the numbers, the **base**, which will be made public.

By Theorem 1.6.5 and Theorem 1.6.6, $\phi(n)$ is equal to $(p-1)(q-1)$. Now choose a number a, the **exponent**, which is relatively prime to $\phi(n)$. To do this, simply generate a large number randomly and test whether this number is relatively prime to $\phi(n)$ (using 1.1.5): if it is, then take it for a; if it is not, then try another number... (the chance of having to try out many numbers is very small). Using the methods of Section 1.1, find a linear combination of $\phi(n)$ and a which is 1:

$$ax + \phi(n)y = 1. \qquad (*)$$

Note that x is, in particular, the inverse of a modulo $\phi(n)$.

Now one may publish the pair of numbers (n, a).

To encode a message If the required message is not already in digital form then assign an integer to each letter of the alphabet and to each punctation mark according to some standard agreement, with all such letter–number equivalents having the same length (perhaps a = 01, b = 02 and so on). Break the digitised message into blocks of length less than the number of digits in either p or q (so if p and q are of 100 digits each then break the message into blocks each with length less than 100 digits).

Now encode each block β by calculating the standard representative m for β^a modulo n. Now send the sequence of encoded blocks with the beginning of each block clearly defined or marked in some way.

To decode The constructor of the code now receives the message and breaks it up into its blocks. To decode a block m, simply calculate the standard representative of

$$m^x \bmod n,$$

where x is as in $(*)$. The result is the original block β of the message. To see that this is so, we recall that m was equal to $\beta^a \bmod n$. Therefore

$$m^x \equiv (\beta^a)^x = \beta^{ax} = \beta^{1-\phi(n)y} = \beta \cdot \left(\beta^{\phi(n)}\right)^{-y} \equiv \beta \cdot 1^{-y} = \beta \bmod n.$$

Here we are using Euler's Theorem (1.6.7) to give us that

$$\beta^{\phi(n)} \equiv 1 \bmod n.$$

This, of course, is only justified if β is relatively prime to n: but that is ensured by our choosing β to have fewer digits than either of the prime factors of n (actually the chance of an arbitrary integer β not being relatively prime to n is extremely small).

At first sight it might seem that this is not an effective code, for surely anyone who intercepts the message may perform the calculation above, and so decode the message. But notice that the number x is not made public. Very well you may say: an interceptor may simply calculate x. But how does one calculate x? One computes 1 as a linear combination of a and $\phi(n)$. And here is the point: although a and n are made public, $\phi(n)$ is not and, so far as is known, there is no way in which one may easily calculate $\phi(n)$ for such a large number n. Of course, one way to calculate $\phi(n)$ from n is to factorise n as the product of the two primes p and q, but factorisation of such large numbers seems to be an inherently difficult task. Certainly, at the moment, factorisation of such a number (of about 200 decimal digits) seems to be well beyond the range of any existing computer (unless one is prepared to hang around, waiting for an answer, for a few million years). See www.rsasecurity.com/rsalabs/challenges/factoring/index.html for up-to-date information.

It should be said that, in order to obtain a code which cannot easily be broken, there are a few more (easily met) conditions to impose on p, q and a: see [Salomaa] or the RSA Labs website www.rsasecurity.com/rsalabs/ for this, as well as for a more detailed discussion of these codes. For up-to-date information about this code and its uses see the RSA Labs website.

We give an example: we will of course choose small numbers for the purpose of illustrating the method, so our code would be very easy to break.

Example Take 3 and 41 to be our two primes p, q. So $n = 123$ and $\phi(n) = (3-1)(41-1) = 80$.

We choose an integer a relatively prime to 80: say $a = 27$. Express 1 as a linear combination of 80 and 27:

$$3 \cdot 27 - 1 \cdot 80 = 1$$

so 'x' is 3. We publish $(n, a) = (123, 27)$.

To encode a block β, the sender calculates $\beta^{27} \bmod 123$, and to decode a received block m, we calculate $m^3 \bmod 123$.

Thus, for example, to encode the message $\beta = 05$, the sender computes

$$5^{27} \bmod 123\,(= (125)^9 \equiv 2^9 \equiv 4 \cdot 128 \equiv 4 \cdot 5 \equiv 20 \bmod 123)$$

and so sends $m = 20$. On receipt of this message, anyone who knows 'x' (the inverse of 27 mod 80) computes 20^3 mod 123 which, you should check, is equal to the original message 05.

If now we use the number-to-letter equivalents:

$$\mathrm{G} = 1, \mathrm{R} = 2, \mathrm{A} = 3, \mathrm{D} = 4, \mathrm{U} = 5, \mathrm{O} = 6, \mathrm{S} = 7, \mathrm{I} = 8, \mathrm{T} = 9, \mathrm{Y} = 0,$$

and the received message is $10/04$, the original message is decoded by calculating

$$\begin{aligned} 10^3 &= 1000 \\ &= 8 \cdot 123 + 16 \\ &\equiv 16 \bmod 123 \end{aligned}$$

and

$$4^3 = 64 \bmod 123.$$

Juxtaposing these blocks gives 1664, and so the message was the word G O O D.

(In this example we used small primes for purposes of illustration but, in doing so, violated the requirement that the number of digits in any block should be less than the number of digits in either of the primes chosen. Exercise 1.6.9 below asks you to discover what effect this has.)

Pierre Fermat was born in 1601 near Toulouse. In 1631 he became a magistrate in the 'Parlement' of Toulouse, and so became 'Pierre de Fermat'. He held this office until his death in 1665. Fermat's professional life was divided between Toulouse, where he had his main residence, and Castres, which was the seat of the 'Chambre' of the Parlement which dealt with relations between the Catholic and Protestant communities within the province.

Fermat's contact with other mathematicians was almost entirely by letter: his correspondence with Mersenne and others in Paris starts in 1636. In 1640 he was put in contact with one of his main correspondents, Frénicle de Bessy, by Mersenne. In fact, Fermat seems never to have ventured far from home, in contrast to most of his scientific contemporaries.

Fermat's name is perhaps best known in connection with what was, for many centuries, one of the most celebrated unsolved problems in mathematics. The equation

$$x^n + y^n = z^n$$

can be seen to have integer solutions when n is 1 or 2 (for example when n is 2, $x = 3$, $y = 4$ and $z = 5$ is an integer solution). Fermat claimed, in the margin of his copy of Diophantus' *Arithmetica*, that he could show that this equation never has a solution in positive integers when n is greater than 2. Fermat appended his note to Proposition 8 of Book II of the *Arithmetica*: 'To divide a given square number into two squares'. Fermat's note translates as

> On the other hand it is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or generally any power except a square into two powers with the same exponent. I have discovered a truly marvellous proof of this, which however the margin is not large enough to contain.

However, until very recently, no-one had been able to supply a proof of 'Fermat's Last Theorem', and one may reasonably doubt whether Fermat did in fact have a correct proof.

Many attempts were made over the centuries to prove this result and various special cases were dealt with. In 1983 Faltings proved a general result which put strong limits on the number of solutions but the conjecture, that there are no solutions for $n \geq 3$, remained open. Then, in 1993, Andrew Wiles announced, in a lecture at the Isaac Newton Institute in Cambridge, that he had proved 'Fermat's Last Theorem'. As it turned out, however, there was a gap in the proof. It took over a year for Wiles, and a collaborator, Richard Taylor, to correct the proof. But, it was corrected and so, finally, after more than 400 years, Fermat's assertion has been proved to be correct.

Number theory, as opposed to many other parts of mathematics, had not enjoyed a renaissance before Fermat's time. For instance, the first Latin translation, by 'Xylander', of Diophantus' *Arithmetica* had only appeared in 1575, and the first edition to contain the full Greek text, with many of the corrupt passages corrected, was published by Bachet in 1621. It was in a copy of this edition that Fermat made marginal notes, including the (in?)famous one above.

Fermat had hoped to see a revival of interest in number theory, but towards the end of his life he despaired of the area being treated with the seriousness he felt it deserved. In fact, Fermat's work in number theory remained relatively unappreciated for almost a century, until Euler, having been referred to Fermat's works by Goldbach, found his interest aroused.

Exercises 1.6

1. Find the orders of
   (i) 2 modulo 31,
   (ii) 10 modulo 91,

(iii) 7 modulo 51, and
(iv) 2 modulo 41.

2. Find
   (i) 5^{20} mod 7,
   (ii) 2^{16} mod 8,
   (iii) 7^{1001} mod 11, and
   (iv) 6^{76} mod 13.
3. Prove that for every positive integer a, written in the base 10, a^5 and a have the same last digit.
4. This exercise indicates the 'additive proof' (see above) of Fermat's Theorem. Let p be a prime. Consider the expansion of $(x + y)^p$ using the Binomial Theorem. Replace each of x and y in this expansion by 1, and reduce modulo p to deduce that $2^p \equiv 2 \bmod p$, that is, Fermat's Theorem for the case $a = 2$.

   (This proof may be generalised to cover the case of an arbitrary a by writing a as a sum of a '1s', using the Multinomial Theorem expansion of $(x_1 + x_2 + \ldots + x_a)^p$ and deducing that p divides all the coefficients in the expanded expression except the first and the last. For the Multinomial Theorem, see [Biggs, p. 99] for example.)
5. Calculate $\phi(32)$, $\phi(21)$, $\phi(120)$ and $\phi(384)$.
6. Find
   (i) 2^{25} mod 21,
   (ii) 7^{66} mod 120 and
   (iii) the last two digits of $1 + 7^{162} + 5^{121} \cdot 3^{312}$.
7. Show that, for every integer n, $n^{13} - n$ is divisible by 2, 3, 5, 7 and 13.
8. Show that, if $n \geq 2$ and if p is a prime which divides n but is such that p^2 is not a factor of n, then $p^{\phi(n)+1} \equiv p \bmod n$. Can you find and prove a generalisation of this?

   [Hint for first part: n may be written as pm, and $(p, m) = 1$; consider powers of p modulo m.

   Hint for second part: for example, you may check that, although $2^{\phi(100)+1}$ is not congruent to 2^1 mod 100, one does have $2^{\phi(100)+2}$ congruent to 2^2 mod 100; also $6^{20+1} \equiv 6 \bmod 66$.]
9. In the example at the end of this section we used small primes for purposes of illustration, and in doing so violated the requirement that the number of digits in any block should be less than the number of digits in either of the primes chosen. This means that certain blocks, such as 18, 39,... which we might wish to send, will not be relatively prime to 123. What happens if we attempt to encode and then decode such blocks?

[Hint: the previous exercise is relevant. You should assume that x in $(*)$ on p. 71 is positive. The argument is quite subtle.]

10. Recall that the Mersenne primes are those numbers of the form $M(n) = 2^n - 1$ that are prime. In Exercise 1.3.6 you were asked to show that if $M(n)$ is prime then n itself must be prime. The converse is false: there are primes p such that $M(p)$ is not prime. One such value is $p = 37$. A factorisation for $M(37) = 2^{37} - 1$ was found by Fermat: he used what is a special case of Fermat's Theorem, indeed it seems that this is what led him to discover the general case of 1.6.3. In this exercise we follow Fermat in finding a non-trivial proper factor of $2^{37} - 1$, which equals 137 438 953 471.
    (i) Show that if p is a prime and if $q(\neq 2)$ is a prime divisor of $2^p - 1$ then q is congruent to 1 mod p.
    [Hint: since q divides $2^p - 1$ we have $2^p \equiv 1 \bmod q$; apply Fermat's Theorem to deduce that p divides $q - 1$.]
    (ii) Apply part (i) with $p = 37$ to deduce that any prime divisor of $2^{37} - 1$ must have the form $37k + 1$ for some k. Indeed, since clearly 2 does not divide $2^{37} - 1$, any such prime divisor must have the form $74k + 1$ (why?). Hence find a proper factorisation of $2^{37} - 1$ and so deduce that $2^{37} - 1$ is not prime.
    [We have cut down the possibilities for a prime divisor to: 75 (which may be excluded since it is not prime), 149, 213, ... The arithmetic in this part may be a little daunting, but you will not have to search too far for a divisor (there is a factor below 500), provided your arithmetic is accurate! It would be a good idea to use 'casting out nines' (Exercise 1.4.9) to check your divisions.]

11. Use a method similar to that in the exercise just above to find a prime factor of $F(5) = 2^{32} + 1$ (see notes to Section 1.3).
    [Hint: as before, start with a prime divisor $q(\neq 2)$ of $2^{32} + 1$ and work modulo 32. You should be able to deduce that q has the form $64k + 1$. Eliminate non-primes such as 65 and 129. As before, be very careful in your arithmetic. There is a factor below 1000.]

12. A word has been broken into blocks of two letters and converted to two-digit numbers using the correspondence

    a = 0, b = 1, c = 2, d = 3, o = 4, k = 5, f = 6, h = 7, l = 8, j = 9.

    The blocks are then encoded using the public key code with base 87 and exponent 19. The coded message is 04/10. Find the word which was coded.

13. A public key code has base 143 and exponent 103. It uses the following letter-to-number equivalents:

    $$\mathrm{J} = 1, \mathrm{N} = 2, \mathrm{R} = 3, \mathrm{H} = 4, \mathrm{D} = 5, \mathrm{A} = 6, \mathrm{S} = 7, \mathrm{Y} = 8,$$
    $$\mathrm{T} = 9, \mathrm{O} = 0.$$

    A message has been converted to numbers and broken into blocks. When coded using the above base and exponent the message sent is 10/03. Decode the message.

Summary of Chapter 1

We have investigated the divisibility relation on the set of integers. We defined the greatest common divisor of any two non-zero integers and showed that this is an integral linear combination of them. The notion of integers being relatively prime was introduced and was seen to play an important role in the investigation of congruence classes. We saw the prime numbers as being the 'building blocks' of integers under divisibility, in particular, we proved that every positive integer is, in an essentially unique way, a product of primes.

The additive structure on integers was used to define the set of congruence classes modulo n. It was shown that the set of congruence classes modulo n carries a natural arithmetic structure and a criterion for existence of inverses was established. We learned how to determine whether (sets of) congruences are solvable and, when they are, how to find the solutions.

Investigating the multiplicative structure of invertible congruence classes, we proved Fermat's Theorem and its generalisation, Euler's Theorem. The Euler phi-function was defined and we learned how to compute it. This was used to design public key codes.

We have also seen a variety of techniques of proof used. In particular, definition and proof by induction were introduced, as well as proof by contradiction.

2 Sets, functions and relations

In this chapter we set out some of the foundations of the mathematics described in the rest of the book. We begin by examining sets and the basic operations on them. This material will, at least in part, be familiar to many readers but if you do not feel entirely comfortable with set-theoretic notation and terminology you should work through the first section carefully. The second section discusses functions: a rigorous definition of ‘function’ is included and we present various elementary properties of functions that we will need. Relations are the topic of the third section. These include functions, but also encompass the important notions of partial order and equivalence relation.

The fourth section is a brief introduction to finite state machines.

2.1 Elementary set theory

The aim of this section is to familiarise readers with set-theoretic notation and terminology and also to point out that the set of all subsets of any given set forms a kind of algebraic structure under the usual set-theoretic operations.

A **set** is a collection of objects, known as its **members** or **elements**. The notation $x \in X$ will be used to mean that x is an element of the set X, and $x \notin X$ means that x is not an element of X. We will tend to use upper case letters as names for sets and lower case letters for their elements.

A set may be defined either by listing its elements or by giving some ‘membership criterion’ for an element to belong to the set. In listing the elements of a set, each element is listed only once and the order in which the elements are listed is unimportant. For example, the set

$$X = \{2, 3, 5, 7, 11, 13\} = \{3, 5, 7, 11, 13, 2\}$$

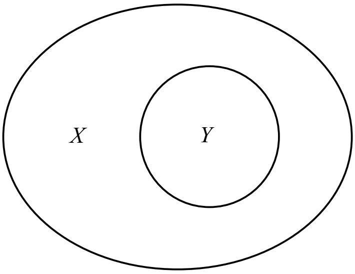


Fig. 2.1 $Y \subseteq X$

has just been defined by listing its elements, but it could also be specified as the set of positive integers that are prime and less than 15:

$$X = \{p \in \mathbb{P}\colon p \text{ is prime and } p < 15\}.$$

The colon in this formula is read as ‘such that’ and so the symbols are read as ‘X is the set of positive integers p such that p is prime and is less than 15’. If the context makes our intended meaning clear, then we can define an infinite set by indicating the list of its members: for example

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\},$$

where the sequence of three dots means ‘and so on, in the same way’. The notation Ø is used for the **empty set**: the set with no elements.

Two sets X,Y are said to be **equal** if they contain precisely the same elements. If every member of Y is also a member of X, then we say that Y is a **subset** of X and write $Y \subseteq X$ (or $X \supseteq Y$). Note that if $X = Y$ then $Y \subseteq X$. If we wish to emphasise that Y is a subset of X but not equal to X then we write $Y \subset X$ and say that Y is a **proper subset** of X. Observe that $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

Every set X has at least the subsets X and Ø; and these will be distinct unless X is itself the empty set.

We may illustrate relationships between sets by use of **Venn diagrams** (certain pictorial representations of such relationships). For instance, the Venn diagram in Fig. 2.1 illustrates the relationship ‘$Y \subseteq X$’: all members of Y are to be thought of as inside the boundary shown for Y so, in the diagram, all members of Y are inside (the boundary corresponding to) X. The diagram is intended to leave open the possibility that there is nothing between X and Y (a region need not contain any elements), so it represents $Y \subseteq X$ rather than $Y \subset X$.

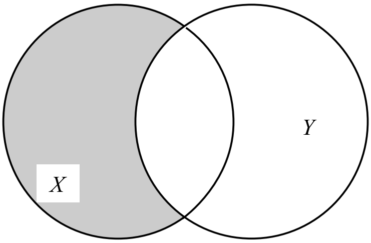


Fig. 2.2 $X\backslash Y$

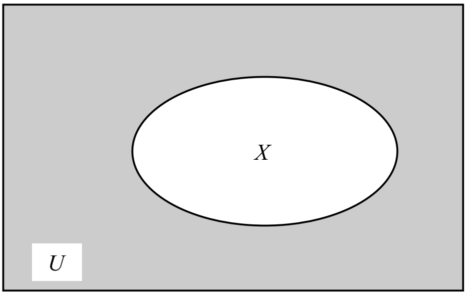


Fig. 2.3 X^{c} is the shaded area.

Venn, extending earlier systems of Euler and Leibniz, introduced these diagrams to represent logical relationships between defined sets in 1880. Dodgson, better known as Lewis Carroll, described a rather different system in 1896.

Given sets X and Y, we define the **relative complement** of Y in X to be the set of elements of X which do not lie in Y: we write

$$X\backslash Y = \{z\colon z \in X \text{ and } z \notin Y\}.$$

This set is represented by the shaded area in Fig. 2.2.

It is often the case that all sets that we are considering are subsets of some fixed set, which may be termed the **universal** set and is commonly denoted by U (note that the interpretation of U depends on the context). In this case the **complement** X^{c} of a set X is defined to be the set of all elements of U which are not in X: that is, $X^{\mathrm{c}} = U\backslash X$ (see Fig. 2.3).

If X, Y are sets then the **intersection** of X and Y is defined to be the set of elements which lie in both X and Y:

$$X \cap Y = \{z\colon z \in X \text{ and } z \in Y\}$$

(see Fig. 2.4).

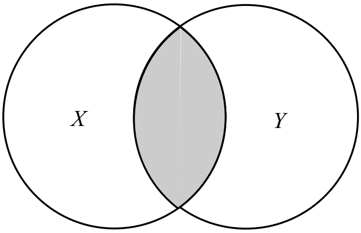


Fig. 2.4 $X \cap Y$

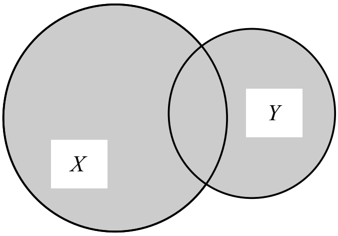


Fig. 2.5 $X \cup Y$

The sets X and Y are said to be **disjoint** if $X \cap Y = \emptyset$, that is, if no element lies in both X and Y.

Also we define the **union** of the sets X and Y to be the set of elements which lie in at least one of X and Y:

$$X \cup Y = \{z\colon z \in X \text{ or } z \in Y\}$$

(see Fig. 2.5).

There are various relationships between these operations which hold whatever the sets involved may be. For example, for any sets X, Y one has

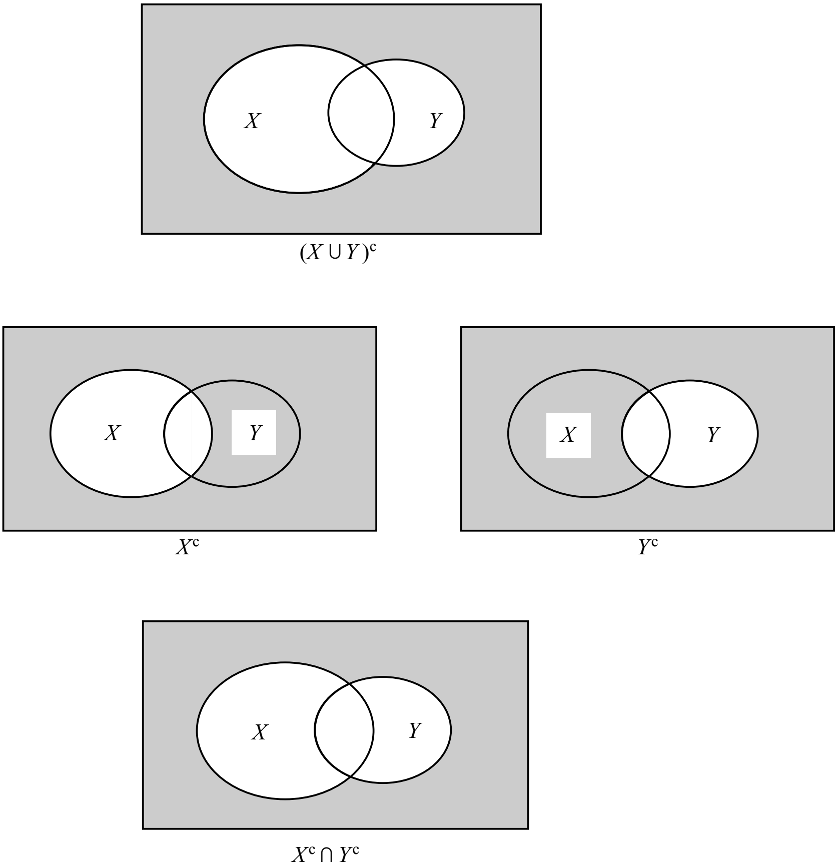
$$(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}.$$

How does one establish such a general relationship? We noted above that two sets are equal if each is contained in the other. So to show that $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ it will be enough to show that every element of $(X \cup Y)^{\mathrm{c}}$ is in $X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ and, conversely, that every element of $X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ is in $(X \cup Y)^{\mathrm{c}}$.

Suppose then that x is an element of $(X \cup Y)^{\mathrm{c}}$: so x is not in $X \cup Y$. That is, x is not in X nor is it in Y. Said otherwise: x is in X^{c} and also in Y^{c}. Thus x is in $X^{\mathrm{c}} \cap Y^{\mathrm{c}}$. So we have established $(X \cup Y)^{\mathrm{c}} \subseteq X^{\mathrm{c}} \cap Y^{\mathrm{c}}$.

Suppose, conversely, that x is in $X^{\mathrm{c}} \cap Y^{\mathrm{c}}$. Thus x is in X^{c} and x is in Y^{c}. That is, x is not in X and also not in Y: in other words, x is not in $X \cup Y$, so x is in $(X \cup Y)^{\mathrm{c}}$. Hence $X^{\mathrm{c}} \cap Y^{\mathrm{c}} \subseteq (X \cup Y)^{\mathrm{c}}$.

Thus we have shown that $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$.



$(X \cup Y)^{\mathrm{c}}$

X^{c}

Y^{c}

$X^{\mathrm{c}} \cap Y^{\mathrm{c}}$

Fig. 2.6

You may have observed how, in this proof, we used basic properties of the words ‘or’, ‘and’ and ‘not’. Indeed, we replaced the set-theoretic operations union, intersection and complementation by use of these words and then applied elementary logic. For an explanation of this (general) feature, see Section 3.1 below.

One may picture the relationship expressed by the equation $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ by using Venn diagrams (Fig. 2.6).

This sequence of pictures probably makes it more obvious why the equation $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ is true. But do not mistake the sequence of pictures for a rigorous proof. For there may be hidden assumptions introduced by the way in which the pictures have been drawn. For example, does the sequence of pictures deal with the possibility that X is a subset of Y? (Pictures may be helpful in finding relationships in the first place or in understanding why they are true.)

The algebra of sets Let X be a set: we denote by $P(X)$ the set of all subsets of X. Thus, if X is the set with two elements x and y, $P(X)$ consists of the empty set, $\emptyset$, together with the sets $\{x\}$, $\{y\}$ and $X = \{x, y\}$ itself.

We will think of $P(X)$ as being equipped with the operations of intersection, union and complementation. Just as the integers with addition and multiplication obey certain laws (such as $x + y = y + x$) from which the other algebraic laws may be deduced, so $P(X)$ with these operations obeys certain laws (or 'axioms'). Some of these are listed in the next result. They are all easily established by the method that was used above to show $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$.

Theorem 2.1.1 *For any sets, X, Y and Z (contained in some 'universal set' U) we have*

$$\begin{array}{ll}
X \cap X = X \textit{ and} & \\
X \cup X = X & \textit{idempotence;} \\
X \cap X^{\mathrm{c}} = \emptyset \textit{ and} & \\
X \cup X^{\mathrm{c}} = U & \textit{complementation;} \\
X \cap Y = Y \cap X \textit{ and} & \\
X \cup Y = Y \cup X & \textit{commutativity;} \\
X \cap (Y \cap Z) = (X \cap Y) \cap Z \textit{ and} & \\
X \cup (Y \cup Z) = (X \cup Y) \cup Z & \textit{associativity;} \\
(X \cap Y)^{\mathrm{c}} = X^{\mathrm{c}} \cup Y^{\mathrm{c}} \textit{ and} & \\
(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}} & \textit{De Morgan laws;} \\
X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \textit{ and} & \\
X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) & \textit{distributivity;} \\
(X^{\mathrm{c}})^{\mathrm{c}} = X & \textit{double complement;} \\
X \cap \emptyset = \emptyset \textit{ and} & \\
X \cup \emptyset = X & \textit{properties of empty set;} \\
X \cap U = X \textit{ and} & \\
X \cup U = U & \textit{properties of universal set;} \\
X \cap (X \cup Y) = X \textit{ and} & \\
X \cup (X \cap Y) = X & \textit{absorption laws.}
\end{array}$$

One may list a similar set of basic properties of the integers. In that case one would include rules such as the distributive law $a \times (b + c) = a \times b + a \times c$

and the law for identity $a \times 1 = a$. One could also include the law $a \times (b + (a + 1)) = a \times b + (a \times a + a)$. However, it is not necessary to do so because it already follows from two applications of the distributive law and one application of the law for identity:

$$\begin{aligned} a \times (b + (a + 1)) &= a \times b + a \times (a + 1) \text{ (\textit{by distributivity})} \\ &= a \times b + (a \times a + a \times 1) \text{ (\textit{by distributivity})} \\ &= a \times b + (a \times a + a) \text{ (\textit{by identity})}. \end{aligned}$$

Thus the inclusion of the above law would be redundant. Similarly, the list of laws in Theorem 2.1.1 has some redundancy.

For example, by properties of complement, $X \cup U$ is equal to $X \cup (X \cup X^{\mathrm{c}})$ which, by associativity, is equal to $(X \cup X) \cup X^{\mathrm{c}}$ which, by idempotence, is equal to $X \cup X^{\mathrm{c}}$; then, by another appeal to the properties of complement, this is equal to U. Thus the equality $X \cup U = U$ follows from some of the others.

You should work out proofs for the laws above: either verifications as with $(X \cup Y)^{\mathrm{c}} = X^{\mathrm{c}} \cap Y^{\mathrm{c}}$ or, in appropriate cases, derivations from laws which you have already established (but avoid circular argument in such derivations).

So we are thinking of the set $P(X)$ of all subsets of X, equipped with the operations of '$\cap$', '$\cup$' and '$^{\mathrm{c}}$', as being some kind of 'algebraic structure'. In fact it is an example of what is termed a 'Boolean algebra'. We say more about these in Section 4.4. Let us say that a **Boolean algebra of sets** is a subset B of the set $P(X)$ of all subsets of a set X, which contains at least the empty set $\emptyset$ and X, and also B must be closed under the 'Boolean' operations, $\cap$, $\cup$ and $^{\mathrm{c}}$, in the sense that if Y and Z are in B then so are $Y \cap Z$, $Y \cup Z$ and Y^{c}.

Example Let X be the set $\{0, 1, 2, 3\}$. Then $P(X)$ has $2^4 = 16$ elements. Take B to be the set $\{\emptyset, \{0, 2\}, \{1, 3\}, X\}$. You should check that B is closed under the operations and hence forms a Boolean algebra of sets.

The operations '$\cap$', '$\cup$' and '$^{\mathrm{c}}$' produce new sets from existing ones. Here is a rather different way of producing new sets from old.

Definition The (**Cartesian**, named after Descartes) **product** of two sets X, Y is defined to be the set of all ordered pairs whose first entry comes from X and whose second entry comes from Y:

$$X \times Y = \{(x, y) \colon x \in X \text{ and } y \in Y\}.$$

Recall that ordered pairs have the property that $(x, y) = (x', y')$ exactly if $x = x'$ and $y = y'$. The product of a set X with itself is often denoted X^2.