M303

Further pure mathematics

Number theory

This publication forms part of an Open University module. Details of this and other Open University modules can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)845 300 6090; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

Note to reader
Mathematical/statistical content at the Open University is usually provided to students in printed books, with PDFs of the same online. This format ensures that mathematical notation is presented accurately and clearly. The PDF of this extract thus shows the content exactly as it would be seen by an Open University student. Please note that the PDF may contain references to other parts of the module and/or to software or audio-visual components of the module. Regrettably mathematical and statistical content in PDF files is unlikely to be accessible using a screenreader, and some OpenLearn units may have PDF files that are not searchable. You may need additional help to read these documents.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2014. Second edition 2016.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed in the United Kingdom by Halstan & Co. Ltd, Amersham, Bucks.

ISBN 978 1 4730 2036 8

2.1

Contents

1 What is number theory? 5

2 Mathematical induction 7
2.1 Notation 7
2.2 Mathematical induction 8
2.3 More general induction 13
2.4 Integer division 19
2.5 Basic properties 24
2.6 The Fundamental Theorem of Arithmetic 26

Solutions and comments on exercises 31

Index 39

1 What is number theory?

> The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and ten times more entertaining as the same amount of 'calculus for engineers'.
>
> G.H. Hardy, *Bulletin of the AMS* (1929)

There is an irresistible fascination in searching for numbers with specified properties. Nearly every century, as far back as the history of mathematics can be traced, has witnessed new and exciting discoveries concerning properties of numbers. Many of the greatest mathematicians, despite having their major interests elsewhere, have at some time in their careers been drawn into problems of number theory and have contributed to the body of knowledge. So what is the appeal of this subject both for professional mathematicians and for thousands of amateurs?

Consider the following problems.

1. Find all the factors of 4 294 967 297.
2. A right-angled triangle has the property that all three of its sides have length equal to a whole number of units. If one of the sides is 24, find seven pairs of values for the other two sides.
3. Show that

   $$1 \times 2 \times 3 \times 4 \times \cdots \times (n-1) + 1$$

   is always divisible by n if n is prime, but is never divisible by n if n is composite.
4. Can every even integer from 4 onwards be expressed as the sum of two primes?
5. For which integers n is $2^n - 1$ a prime?

All these problems will confront us at some stage in this part of the module. Each one illustrates the most attractive feature of number theory: the problems can be understood by beginners of the subject. Perhaps you are not completely familiar with some of the terms (which will be explained later) such as prime, composite and factor, but you should have a feeling for what is involved in these problems. Indeed, you could well take pencil and paper and start exploring some of them; there is no substantial body of knowledge needed as a prerequisite to becoming involved in number theory.

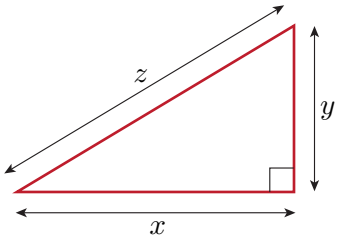


Figure 1.1 An illustration of the Pythagorean equation $x^2 + y^2 = z^2$

Yet while there is no difficulty posing these problems in a readily intelligible form, the varying degrees of difficulty involved in solving them highlights the most intriguing feature of number theory.

Because of the size of the number involved, Problem 1 is quite tricky. However, any reader who is familiar with computers might quickly solve this problem. As it happens, the smallest positive factor of the given number is 641 – a fact which, in the seventeenth century, eluded one of the all-time great mathematicians, Fermat (1601–1665), who had a particular interest in this very problem.

Problem 2 asks for solutions in whole numbers of the famous equation of Pythagoras relating the edge lengths of a right-angled triangle, $x^2 + y^2 = z^2$ (illustrated in Figure 1.1). This is an example of a Diophantine equation, named after the Greek mathematician Diophantus of the early Christian era. We will meet other instances of Diophantine equations in this module, which we will show how to solve. Many books have been written about Diophantine equations. What emerges is a lack of a general theory for solving them; each Diophantine equation appears to be a problem in its own right, requiring its own method of solution. In the meantime, if you are familiar with the 'smallest' solution in integers of the Pythagorean equation, namely $3^2 + 4^2 = 5^2$, then you may have spotted two of the solutions required by Problem 2 by scaling, namely $18^2 + 24^2 = 30^2$ and $24^2 + 32^2 = 40^2$. But what about the other five solutions? You might discover them by patient trial and error – but is there a more systematic approach? We will explore this further at the start of Book C, Chapter 12.

Problems 3, 4 and 5 are classics of number theory. Because the values involved in Problem 3 get very large, very quickly, it is not an easy problem to explore in depth by looking at special cases. But it turns out to be true, and we can give (and will do so in Chapter 4) a general proof of this result. Problem 4 is easier to explore and, on finding it very straightforward to write each even integer up to 200 (say) as a sum of two primes, you would probably be tempted to conclude that it also is a true result. But, perhaps surprisingly, nobody has ever managed to prove it; to this day it remains an unsolved problem of mathematics, despite assault by many great mathematicians. Problem 5 has its origin at the heart of another famous problem, which you will meet in Book C, Chapter 9. By the year 1951, only 12 numbers n were known for which $2^n - 1$ is prime; then computers were brought to bear on the problem, with the result that by the year 2014 forty-eight such numbers were known. The largest one, $n = 57\,885\,161$, led to the number $2^{57\,885\,161} - 1$ being the largest known prime at that time. And yet, despite the scarcity of solutions to Problem 5, most mathematicians still believe that there are infinitely many solutions to this problem – though proof of this seems, at the moment, hopelessly beyond reach.

Number theory is a subject that has developed over a long period of time and, as the previous paragraph suggests, remains very active today. We have already mentioned a few of the great mathematicians who contributed to the development of the subject; there are many, many more. In the *History Reader* for this topic, we give a flavour of the history of the subject. The *History Reader* is not an assessed part of the module and by no means gives a systematic account of the history of number theory. Its inclusion will, we hope, enliven the theoretical side of the material and should also reveal the stumbling way in which progress has been made.

The nature of number theory has changed dramatically in recent years, due to the advent of the computer. Computations that were nigh impossible just a few years ago can now be managed with ease. Consequently, exploration of alleged results and searches for numbers with prescribed properties are readily attacked with the assistance of a machine. Although the material of this module presents many challenges for those with access to (and enthusiasm for) a computer, we have written the module in such a way as to avoid the heavy computational side of the subject. We will be attacking problems in the way that they have been tackled historically, using pencil and paper. There are, however, many problems in the module involving 'arithmetic' that could be simplified with the help of a calculator, and although it is not essential, it is advisable that you have one.

Number theory is all about problem-solving. Nobody becomes competent at calculus by reading about it; it is essential to practise differentiation and integration on a large number of examples. The same is true of number theory; you cannot get to grips with the subject without solving lots of problems yourself. To this end we have included a good stock of problems in all the chapters, and while studying you should always have pencil and paper at hand. The Worked Exercises in the chapters are for you to read, but the Exercises are for you to *do*. Do not spend forever on an exercise that looks like defeating you. If you get stuck, you should refer to the solution – but do not give in too easily!

2 Mathematical induction

Although you may have encountered mathematical induction before now, you may not be familiar with the more formal approach taken to it in this section.

2.1 Notation

Before progressing further we introduce some standard notation to be used throughout this module. In number theory we are primarily interested in the positive integers, also called the *natural numbers*.

A collection of distinct objects (such as numbers) is known as a **set**. The set of all **integers**, positive, negative or zero, is denoted by $\mathbb{Z}$:

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

and the set of **natural numbers** is denoted by $\mathbb{N}$:

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

We have described each of these sets by (partially) listing its elements within 'curly brackets', which are known more formally as **braces**. We often describe a set by giving a property that characterises its elements. For example, the set of all integers that are multiples of 3, and which is denoted by $3\mathbb{Z}$, can be described either by

$$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

or by

$$3\mathbb{Z} = \{3n : n \in \mathbb{Z}\}.$$

We will also have occasion to refer to the set $\mathbb{Q}$ of **rational numbers** and the set $\mathbb{R}$ of **real numbers**. The rational numbers are the numbers $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, and the real numbers can be thought of as values representing all the points along an infinite number line.

Finally, we will make extensive use of the **modulus** or *absolute value* function, which is defined for any element n of $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$) by

$$|n| = \begin{cases} n, & \text{if } n \geq 0, \\ -n, & \text{if } n < 0. \end{cases}$$

Exercise 2.1

(a) Which set of numbers is described by each of the following?

(i) $\{n \in \mathbb{Z} : |n| > 20\}$

(ii) $\{n : n = 2m^2, \text{ for some } m \in \mathbb{N}\}$

(b) Describe each of the following sets in the notation used in part (a).

(i) The set of all odd natural numbers.

(ii) The set of all integers lying between -100 and 100 inclusive.

2.2 Mathematical induction

One property of $\mathbb{N}$ that is not shared by some other number sets such as $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$ is worth recording. It may seem a rather obvious property, but its presence is crucial to establishing less apparent properties that we are going to need.

The Well-Ordering Principle for $\mathbb{N}$

Every non-empty subset of $\mathbb{N}$ has a least member. In other words, if S is a non-empty subset of $\mathbb{N}$ then there exists $b \in S$ such that $b \leq n$ for all $n \in S$.

In future we will refer to this just as the Well-Ordering Principle. It says that any collection of natural numbers we care to describe, as long as it has some elements in it, must have a least member. Notice that the set of positive real numbers does not have this property. For example, the set of positive real numbers itself has no least element since, if x is *any* positive real, then

$$0 < \tfrac{1}{2}x < x,$$

showing that $\frac{1}{2}x$ is a positive real number smaller than x. Hence x cannot be the smallest positive real number.

From the Well-Ordering Principle we can quickly deduce the result that is the backbone of the method of proof by *mathematical induction*.

Theorem 2.1 *Principle of Induction*

If S is a set of natural numbers with the following two properties:

(a) 1 is a member of S

(b) if $k \in S$, then the next integer $k + 1 \in S$

then $S = \mathbb{N}$.

Proof We give a proof by contradiction. We assume that the theorem is not true and that there is a set S of natural numbers satisfying (a) and (b) that is not the whole of $\mathbb{N}$. We show that this assumption leads to a contradiction and therefore the theorem must be true.

Let A be the set of all natural numbers that do not belong to S. By the assumption that S is not the whole of $\mathbb{N}$, we know that A is non-empty. Hence, by the Well-Ordering Principle, A must contain a least member. Let this least member of A be a.

By property (a) the integer 1 belongs to S, and so 1 is not in A. Therefore $a > 1$. Now consider the integer $a - 1$, which must be positive as $a > 1$. Furthermore, as $a - 1 < a$ and a is the least member of A, it follows that $a - 1$ does not belong to A. Therefore $a - 1$ is a member of S.

But property (b) now tells us that the integer following $a - 1$, namely a itself, belongs to S. This contradicts the fact that a belongs to A. This contradiction means that the one assumption we made, namely that A is non-empty, must be false. So A is empty and hence S is the set of all natural numbers. ■

Worked Exercise 2.2

Prove that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \quad \text{for all natural numbers } n.$$

Solution

With an eye on the Principle of Induction, let S be the set of natural numbers n for which the formula holds. Our goal is to show that $S = \mathbb{N}$.

Putting $n = 1$ in the formula, we observe that the left-hand side has only one term so that the formula reduces to $1 = 1^2$, which is true. So $1 \in S$.

It remains to prove property (b). To that end, suppose $k \in S$, where k is some natural number. Since $k \in S$ we have that

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

To deduce that $k + 1 \in S$ we must show that the given formula is true for the case $n = k + 1$. Working on the left-hand side of the formula for $n = k + 1$:

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) & \\ = k^2 + (2k + 1), & \quad \text{from the assumption that } k \in S, \\ = (k + 1)^2, & \quad \text{which is the required right-hand side.} \end{aligned}$$

This reasoning shows that if $k \in S$ then $k + 1 \in S$, which confirms property (b).

Hence $S = \mathbb{N}$, and the formula is true for all natural numbers.

We presented Worked Exercise 2.2 by applying the Principle of Induction to the set of natural numbers for which the proposition was true. In future we will present such arguments less formally and will refer to them as proof by **mathematical induction**. The propositions for which we attempt such proofs are ones that are given in terms of a general natural number n, and that we hope to be true for all $n \in \mathbb{N}$.

Let $P(n)$ be a proposition whose truth we wish to prove by mathematical induction. Such a proposition can take various forms. It might be a formula as in Worked Exercise 2.2, an inequality such as $2^n > n^3$, which we will discuss in Worked Exercise 2.4, or a statement such as 'n can be written as a sum of distinct powers of 2', which you will meet in Worked Exercise 2.6. To prove the truth of $P(n)$, let S be the set of natural numbers n for which $P(n)$ is true. If we know that $P(1)$ is true then $1 \in S$. Further, if we can show that whenever $P(k)$ is true it follows that $P(k + 1)$ is true, then $k \in S$ implies $k + 1 \in S$. Hence, by the Principle of Induction, $S = \mathbb{N}$, and $P(n)$ is true for all natural numbers.

We state this formally as follows.

Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on a natural number n. If:

(a) $P(1)$ is true

(b) for any integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true

then $P(n)$ is true for all $n \in \mathbb{N}$.

Step (a), showing that the proposition is true for the first value, is called the **basis for the induction**. Step (b) is called the **induction step**. The assumption made in this step, that $P(k)$ is true for some integer k, is called the **induction hypothesis**.

Worked Exercise 2.3

Prove the following formula for the sum of the first n triangular numbers.

$$1 + 3 + 6 + 10 + \cdots + \tfrac{1}{2}n(n+1) = \tfrac{1}{6}n(n+1)(n+2) \qquad P(n)$$

By 'prove' we mean 'prove for all integers $n \geq 1$'. The 'for all integers $n \geq 1$' is taken for granted.

Solution

We use mathematical induction to prove that $P(n)$ is true for all integers $n \geq 1$ by establishing (a) and (b) above.

First the basis for the induction. Putting $n = 1$ in $P(n)$ gives

$$1 = \tfrac{1}{6} \times 1(1+1)(1+2).$$

This is correct, showing that $P(1)$ is true.

Now the induction step. We assume that $P(k)$ is true for some natural number k. That is, we have the induction hypothesis

$$1 + 3 + 6 + 10 + \cdots + \tfrac{1}{2}k(k+1) = \tfrac{1}{6}k(k+1)(k+2).$$

We need to deduce the truth of $P(k+1)$ from this, that is

$$1 + 3 + 6 + 10 + \cdots + \tfrac{1}{2}k(k+1) + \tfrac{1}{2}(k+1)(k+2) = \tfrac{1}{6}(k+1)(k+2)(k+3).$$

The last term on the left-hand side is the $(k+1)$th triangular number.

Taking the left-hand side, we have

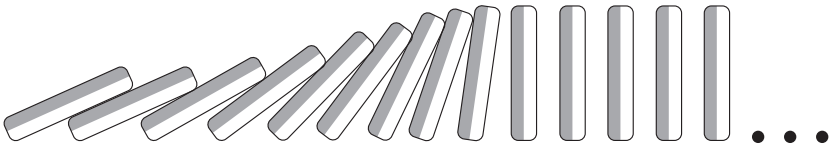
$$\begin{aligned} &1 + 3 + 6 + 10 + \cdots + \tfrac{1}{2}k(k+1) + \tfrac{1}{2}(k+1)(k+2) \\ &= \tfrac{1}{6}k(k+1)(k+2) + \tfrac{1}{2}(k+1)(k+2), \\ &\qquad\qquad \text{by the induction hypothesis,} \\ &= (k+1)(k+2)(\tfrac{1}{6}k + \tfrac{1}{2}) \\ &= \tfrac{1}{6}(k+1)(k+2)(k+3), \quad \text{which is the RHS of } P(k+1). \end{aligned}$$

RHS is short for right-hand side and LHS is short for left-hand side of an equation.

This establishes the truth of $P(k+1)$ and completes the induction step.

Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers.

Mathematical induction can be likened to a line of dominoes (Figure 2.1), arranged so that if any one falls over, it will knock over the next one along the line (the induction step). Then, if the first domino is knocked over (the basis for the induction), they all fall over.



The first domino is knocked over

If the kth domino is knocked over, so too is the $(k+1)$th

Figure 2.1 Illustrating mathematical induction

Of course, the induction step is at the heart of any induction proof. Quite often, as in both the preceding worked exercises, some algebraic manipulation is involved. This may be straightforward or quite complex. The next exercise provides you with an opportunity to practise proof by induction.

Exercise 2.2

(a) Use mathematical induction to prove that the formula

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \tfrac{1}{6}n(n+1)(2n+1)$$

is true for all natural numbers.

(b) A **geometric series** is the sum of a finite sequence of terms in which the ratio of successive terms is constant, r in the following example.

Use mathematical induction to prove the formula for the geometric series

$$a + ar + ar^2 + ar^3 + \cdots + ar^{n-1} = \frac{a(r^n - 1)}{r - 1}, \quad r \neq 1.$$

2.3 More general induction

The examples that we have seen using mathematical induction have all concerned propositions $P(n)$ that are true for all natural numbers. In this case $n = 1$, the smallest integer for which the proposition was true, provided the basis for the induction. In fact there is nothing special about the number 1 here. The Principle of Induction is readily adapted to provide proofs of results that are true for all integers greater than some integer n_0.

Principle of Mathematical Induction (generalised)

Let $P(n)$ be a proposition depending on an integer n. If:

(a) $P(n_0)$ is true

(b) for any integer $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true

then $P(n)$ is true for all integers $n \geq n_0$.

As before, step (a) of the generalised principle is called the basis for the induction, and step (b) is called the induction step.

In the next worked exercise we use this generalised form of induction to prove a result that is true for all integers from 10 onwards. In this example the induction step involves more reasoning than the simple algebraic manipulations we have met so far.

Worked Exercise 2.4

For which natural numbers n is it true that $2^n > n^3$?

Solution

Exploration of the relative values of 2^n and n^3 for small values of n shows that 2^n is larger when $n = 1$, but then n^3 is larger for $n = 2, 3, 4, \ldots, 9$. For $n = 10$, 2^n becomes the larger value once again:

$$2^{10} = 1024 > 1000 = 10^3.$$

As n now increases it appears that 2^n grows more quickly than n^3, which leads us to conjecture:

$$2^n > n^3 \text{ for all integers } n \geq 10.$$

Preparing the way for induction, we let $P(n)$ be the statement that $2^n > n^3$.

Having seen that $P(10)$ is true, the basis for the induction is established (as $n_0 = 10$).

It remains to show that, for any integer $k \geq 10$, if $P(k)$ is true then $P(k+1)$ is true. So the induction hypothesis is

$$2^k > k^3, \quad \text{for some } k \geq 10,$$

and from this assumption we need to show that

$$2^{k+1} > (k+1)^3.$$

Now, $2^{k+1} = 2 \times 2^k$ and so the induction hypothesis gives

$$2^{k+1} > 2k^3.$$

Therefore it suffices to show that, for any $k \geq 10$,

$$2k^3 \geq (k+1)^3,$$

or, rearranging,

$$\left(1 + \tfrac{1}{k}\right)^3 \leq 2.$$

This is certainly true by the following argument. As $k > 1$, the largest value of $\left(1 + \frac{1}{k}\right)^3$ comes from the largest value of $1 + \frac{1}{k}$. This in turn comes from the smallest value of k, namely $k = 10$. However, $\left(1 + \frac{1}{10}\right)^3 = 1.331$, which is less than 2. This completes the induction step.

Hence, by the Generalised Principle of Mathematical Induction, the proposition is true for all integers $n \geq 10$.

Worked Exercise 2.4 has some points of interest. Investigation of the induction step led us to the inequality

$$\left(1 + \tfrac{1}{k}\right)^3 \leq 2.$$

In fact this inequality holds true for all integers $k \geq 4$ and so the induction step works for all integers $k \geq 4$ (although we were concerned only with integers $k \geq 10$). Drawing on the earlier analogy with dominoes, the situation in Worked Exercise 2.4 is as depicted in Figure 2.2. If any domino from the fourth onwards were to fall it would knock the next over, but the first one of these that *does* fall is the tenth.

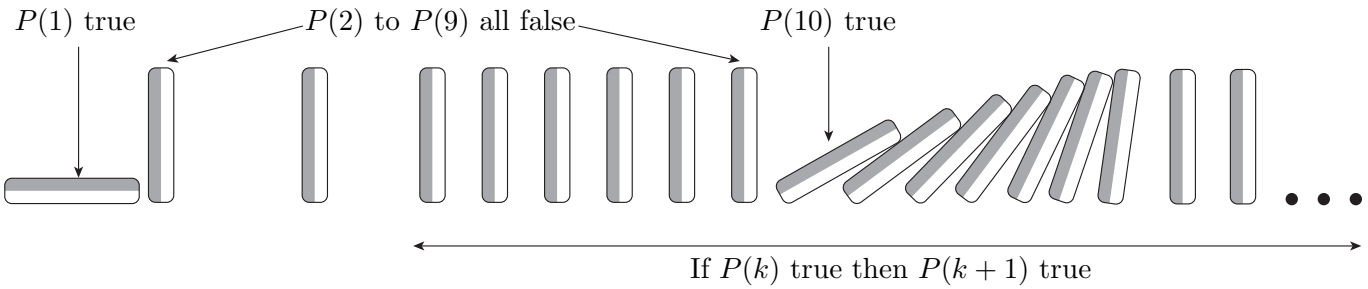


Figure 2.2 $P(n) : 2^n > n^3$ for $n \geq 10$

In the examples so far, when establishing the induction step, we assumed that the proposition under question was true for some integer $k \geq n_0$. On occasion it can be helpful to make a more general assumption. The *Second Principle of Mathematical Induction* employs a different induction step.

Second Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on an integer n. If:

(a) $P(n_0)$ is true

(b′) for any integer $k \geq n_0$, if $P(n_0)$, $P(n_0+1)$, …, $P(k)$ are all true, then $P(k+1)$ is true

then $P(n)$ is true for all integers $n \geq n_0$.

The Second Principle of Mathematical Induction seems logically sound if one thinks of the domino analogy, and can be established from the Well-Ordering Principle. We will not do so here but proof of this can be found in the solution to Exercise 2.4(d).

The next two worked exercises both make use of the Second Principle of Mathematical Induction.

Worked Exercise 2.5

A sequence of integers is defined as follows:

$$x_0 = 1; \quad x_n = x_0 + x_1 + \cdots + x_{n-1}, \quad \text{for all integers } n \geq 1.$$

Prove that $x_n = 2^{n-1}$, for all integers $n \geq 1$.

Solution

Denote the proposition $x_n = 2^{n-1}$ by $P(n)$.

Then $x_1 = x_0 = 1 = 2^0$, so $P(1)$ is true and we have the basis for the induction.

Heading towards the (new) induction step, suppose that $P(r)$ is true for all $1 \leq r \leq k$; that is,

$$x_r = 2^{r-1}, \quad \text{for } 1 \leq r \leq k.$$

Then

$$\begin{aligned} x_{k+1} &= x_0 + x_1 + \cdots + x_k \\ &= 1 + \left(1 + 2 + 4 + \cdots + 2^{k-1}\right), \text{ by the induction hypothesis,} \\ &= 1 + \frac{2^k - 1}{2 - 1}, \text{ by formula for geometric series, Exercise 2.2(b),} \\ &= 2^k. \end{aligned}$$

This establishes the truth of $P(k+1)$ and completes the induction step.

Hence the result follows by the Second Principle of Mathematical Induction.

Although there are other ways of proving the result in Worked Exercise 2.5, it is not easy to prove using mathematical induction without making use of the Second Principle. It is the fact that each number in the sequence is defined in terms of *all* the preceding numbers that makes the Second Principle relevant. In Worked Exercise 2.6 we employ the Second Principle of Mathematical Induction again, but this time it will be used differently.

Worked Exercise 2.6

Prove that every natural number n can be written as a sum of distinct (integer) powers of 2. For example, $13 = 2^0 + 2^2 + 2^3$ and $20 = 2^2 + 2^4$.

You might be familiar with the fact that each natural number is expressed *uniquely* in this way: we are essentially representing n in binary. However, we omit the proof of uniqueness here.

Solution

Let $P(n)$ be the proposition that n can be written as a sum of distinct powers of 2.

Then, since $1 = 2^0$, $P(1)$ is true and we have the basis for the induction.

To make use of the Second Principle we assume that, for some natural number k, $P(r)$ is true for each integer r in the range $1 \leq r \leq k$. That is, we assume that each r in this range can be expressed in the required way. To complete the induction proof we show that, under this assumption, $k+1$ can be expressed as a sum of distinct powers of 2, thereby establishing the truth of $P(k+1)$.

We consider two cases, depending on whether $k+1$ is even or odd.

Case $k+1$ even

Since $k+1$ is even we can write $k+1 = 2s$ for some natural number s. Now $s < k+1$ so, by the induction hypothesis, s can be written as a sum of distinct powers of 2, say

$$s = 2^a + 2^b + \cdots + 2^f, \quad a, b, \ldots, f \text{ distinct.}$$

Multiplying this sum by 2 gives

$$k+1 = 2s = 2^{a+1} + 2^{b+1} + \cdots + 2^{f+1}, \quad a+1, b+1, \ldots, f+1 \text{ distinct,}$$

as required.

Case $k+1$ odd

Since $k+1$ is odd we can write $k+1 = 2s+1$ for some natural number s. Now $2s < k+1$ so, by the induction hypothesis, $2s$ can be written as a sum of distinct powers of 2, say

$$2s = 2^a + 2^b + \cdots + 2^f, \quad a, b, \ldots, f \text{ distinct.}$$

Since $2s$ is even, and the exponents in this representation of $2s$ are distinct, no exponent can be 0 (because the only power of 2 giving an odd integer is $2^0 = 1$).

Hence

$$\begin{aligned} k+1 &= 2s+1 \\ &= 2^a + 2^b + \cdots + 2^f + 1, \quad a, b, \ldots, f \text{ distinct and non-zero,} \\ &= 2^a + 2^b + \cdots + 2^f + 2^0, \quad a, b, \ldots, f, 0 \text{ distinct,} \end{aligned}$$

as required.

This completes the induction step and the result follows by the Second Principle of Mathematical Induction.

Exercise 2.3

In the sequence

$$1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ \ldots,$$

each term, from the third onwards, is the sum of the previous two terms. That is, the sequence $\{L_n\}$ is defined by

$$L_1 = 1; \quad L_2 = 3; \quad L_n = L_{n-1} + L_{n-2}, \quad \text{for } n \geq 3.$$

Use the Second Principle of Mathematical Induction to prove that

$$L_n < \left(\tfrac{7}{4}\right)^n, \quad \text{for all } n \geq 1.$$

Mathematical induction provides a powerful method of proof, whose applications include proving the truth of formulas for all integers from some integer onwards. But while mathematical induction is a great help in proving formulas, it does not help us to find such formulas. Discovering the formulas in the first place is a different matter.

We finish this section with an exercise that sets several problems on proof by mathematical induction.

Exercise 2.4

(a) Use the Principle of Mathematical Induction to prove that the following formulas are true for all natural numbers n.

(i) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{1}{3}n(4n^2 - 1)$

(ii) $1 + 5 + 12 + 22 + \cdots + \frac{1}{2}n(3n-1) = \frac{1}{2}n^2(n+1)$

(b) The **factorial** of $k \in \mathbb{N}$ is $k! = 1 \times 2 \times \cdots \times k$.

Prove the following formula for all natural numbers n.

$$1 \times (1!) + 2 \times (2!) + 3 \times (3!) + \cdots + n \times (n!) = (n+1)! - 1$$

(c) For which natural numbers n is it true that $n! > 6n^2$? Prove your result using mathematical induction.

(d) Show how the Second Principle of Mathematical Induction can be derived from the Well-Ordering Principle, as follows.

Suppose that the conditions (a) and (b′) stated in the Second Principle of Mathematical Induction hold. Let S be the set of integers k, $k \geq n_0$, for which $P(k)$ does not hold, that is,

$$S = \{k \in \mathbb{Z} : k \geq n_0 \text{ and } P(k) \text{ is false}\}.$$

Suppose that S is non-empty and use this assumption to deduce that the set

$$T = \{s - n_0 : s \in S\}$$

is a non-empty set of natural numbers. Show how the existence of a least member of T leads to a contradiction.

2.4 Integer division

From an early age we learn how to divide one natural number by another, obtaining a quotient and a remainder. For example, we can divide 23 by 4 to obtain a quotient of 5 and a remainder of 3 or, rather more formally, $23 = 4 \times 5 + 3$. In fact, if we stipulate that when dividing by 4 the only permitted remainders are 0, 1, 2 and 3 then the quotient and remainder in any division by 4 turn out to be unique. That is, the only way that we can write $23 = 4 \times q + r$, where q and r are integers with $0 \leq r < 4$, is $q = 5$ and $r = 3$. Such uniqueness holds for division by any natural number. The familiar result exemplified here, known as the *Division Algorithm*, is of enormous theoretical importance. In what follows we will discuss certain consequences of it that are fundamental to our treatment of numbers.

Theorem 2.7 *The Division Algorithm*

For any two integers a and b, where $b > 0$, there exist unique integers q and r such that

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

Proof Consider the set of integers

$$S = \{a - bn \geq 0 : n \in \mathbb{Z}\}.$$

S is the set of non-negative integers in the set $\{\ldots, a-2b, a-b, a, a+b, \ldots\}$.

The set S is non-empty because, as b is positive, $a - bn$ will certainly be positive for large negative values of n. Either 0 is a member of S, and hence the least member of S, or S is a non-empty set of natural numbers and, by the Well-Ordering Principle, again has a least member. So in either case there exists an integer q such that $a - bq = r$ is the least member of S. Hence we have integers q and r such that

$$a = bq + r, \quad \text{where } 0 \leq r.$$

If $r \geq b$ then $r - b \geq 0$. In addition,

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

and so $r - b$ is a member of S. However, $r - b$ is smaller than r, which contradicts the minimality of r, and so $r < b$.

It remains to prove the uniqueness of q and r. Suppose, therefore, that

$$a = bq + r, \quad 0 \leq r < b,$$

and

$$a = bq' + r', \quad 0 \leq r' < b.$$

Subtracting gives

$$0 = b(q - q') + (r - r').$$

Now if $q = q'$ this equation gives $r = r'$ and so the expressions for a are the same.

On the other hand, if $q \neq q'$, we may assume that $q > q'$ and hence that $q - q' > 0$. It follows that $q - q' \geq 1$. Since $b > 0$ we have

$$\begin{aligned} r' - r &= b(q - q') \\ &\geq b \times 1 = b. \end{aligned}$$

Adding r to both sides gives

$$r' \geq b + r \geq b,$$

contradicting the definition of r'.

Therefore the values of q and r are unique. ■

Essentially the same argument is illustrated as follows. Imagine multiples of b stepped off along the number line, as shown in Figure 2.3. As the intervals marked off in this way cover the whole line, the number a lies in some interval

$$bq \leq a < b(q + 1).$$

This interval containing a will be unique. Notice that if a is a multiple of b then a coincides with one of the marks between the intervals. In this case, the interval to either side of a could be chosen to contain a. However, the inequalities decree that we choose the interval that has a at its left-hand end.

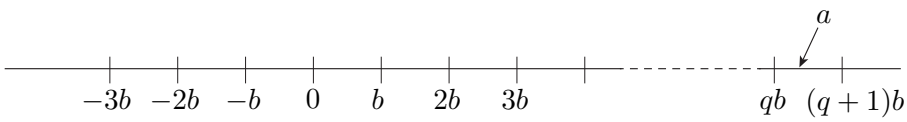


Figure 2.3 Illustrating the Division Algorithm

Subtracting bq through the above inequality shows us that there is a unique integer q such that $0 \leq a - bq < b$. Now putting $a - bq = r$ gives the claimed result.

The way of representing numbers suggested by the Division Algorithm will be important to us, so let us pause to look at some simple applications.

Worked Exercise 2.8

Show that when any square is divided by 4 the remainder is either 0 or 1.

Solution

The Division Algorithm, applied to division by 4, tells us that any integer can be written uniquely in one of the forms $4n$, $4n+1$, $4n+2$ or $4n+3$ for some integer n. So any square number is the square of an integer of one of these four forms. We write each square in its unique form $4q+r$ and hope to find that the only possible values for r are 0 and 1.

$$(4n)^2 = 16n^2 = 4(4n^2) + 0$$
$$(4n+1)^2 = 16n^2 + 8n + 1 = 4(4n^2 + 2n) + 1$$
$$(4n+2)^2 = 16n^2 + 16n + 4 = 4(4n^2 + 4n + 1) + 0$$
$$(4n+3)^2 = 16n^2 + 24n + 9 = 4(4n^2 + 6n + 2) + 1$$

In each case the remainder on division by 4 is either 0 or 1, as claimed.

In fact we could have made the calculations simpler by working with remainders on division by 2. Any number is either of form $2n$ or of form $2n+1$ and the respective squares are

$$(2n)^2 = 4n^2 + 0,$$
$$(2n+1)^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1,$$

showing that the remainder on division by 4 is either 0 or 1.

Exercise 2.5

The Division Algorithm tells us that any integer can be written in one of the forms $3n$, $3n+1$ or $3n+2$. Use this fact to deduce that when any cube is divided by 9 the remainder is one of 0, 1 or 8.

Before moving on, we would like to highlight two formulas with which you are likely to be familiar and which can readily be verified by expanding the brackets.

$$(an+b)^2 = a^2n^2 + 2abn + b^2$$
$$(an+b)^3 = a^3n^3 + 3a^2bn^2 + 3ab^2n + b^3$$

Knowledge of these formulas can be useful, as was the case in the solutions to Worked Exercise 2.8 and Exercise 2.5.

The Division Algorithm provides us with our definition of divisibility: one number is divisible by another when the unique remainder is 0.

Definition 2.9 *Factors and multiples*

An integer a is divisible by the natural number b (or, for brevity, b **divides** a) if there exists some integer q such that $a = bq$.

When b divides a we say that b is a **factor** of a or that a is a **multiple** of b.

We write $b \mid a$ as a shorthand for b divides a, and $b \nmid a$ for b does not divide a.

In other texts you may find the phrase 'b is a **divisor** of a' rather than 'b is a factor of a'.

Be careful not to confuse the statement $b \mid a$ with the fraction $\frac{b}{a}$. For example, $3 \mid 21$ since $21 = 3 \times 7$ and $6 \mid -24$ since $-24 = 6 \times (-4)$. On the other hand, $6 \nmid 16$ since $16 = 6 \times 2 + 4$.

Notice that we consider division only by positive integers. The definition could be adapted to permit division by negative numbers by declaring that a is divisible by b (positive or negative) when there exists an integer q such that $a = bq$. But if $a = bq$ it must be the case that $a = (-b)(-q)$ and so this definition would lead to b being a factor of a if, and only if, $-b$ is a factor of a. There is therefore nothing essentially complicated in dividing by negative numbers, but we will have no occasion to do so. Therefore, if we ask for the factors of an integer, we expect answers that are positive.

Notice also that 0 is excluded as a factor, as the only number for which 0 is a factor is 0 itself. Additionally, since $0 = n \times 0$, every natural number is a factor of 0; in fact 0 is unique in having an infinite number of factors, as will be shown in the proof of Theorem 2.10(b).

Exercise 2.6

(a) List all the factors of 18 and -24. Do these two numbers have any factors in common?

(b) Show that if n is not a multiple of 3 then $n^2 - 1$ is divisible by 3.

Exercise 2.6(a) highlights one property of divisibility, namely that any integer greater than 1 has at least two factors, namely itself and 1. This is just one of a number of simple properties that are direct consequences of the definition. Such properties are not particularly exciting in themselves but some of them will prove to be useful as tools for deriving further information. A selection of the more important properties have been grouped together in the following theorem.

Theorem 2.10 *Properties of division*

Let a and b be natural numbers and c and d be any integers.

(a) If $a \mid c$ then $a \mid (c + na)$ for any integer n.

(b) If $c \neq 0$ and $a \mid c$ then $a \leq |c|$.

(c) If $a \mid b$ and $b \mid a$ then $a = b$.

(d) If $a \mid b$ and $b \mid c$ then $a \mid c$.

(e) If $a \mid c$ and $a \mid d$ then $a \mid (mc + nd)$ for any integers m and n.

Proof

(a) As $a \mid c$ there is an integer q such that $c = aq$. But then

$$c + na = aq + na = a(q + n) = ax,$$

and as $x = q + n$ is an integer, this confirms that a divides $c + na$.

(b) As $c = aq$ as in (a), $|c| = |aq| = a|q|$, and the result follows since $|q| \geq 1$, q being a non-zero integer.

Notice that this result shows that the non-zero integer c can have only a finite number of factors, since they must all be less than or equal to $|c|$.

(c) If $a \mid b$ and $b \mid a$ then, from (b), $a \leq b$ and $b \leq a$. The required equality follows.

(d) If $a \mid b$ and $b \mid c$ then there are integers s and t such that $b = as$ and $c = bt$. Substituting for b gives $c = ast = a(st)$, and as st is an integer this shows that $a \mid c$.

(e) If $a \mid c$ and $a \mid d$ then there are integers p and q such that $c = ap$ and $d = aq$. But then, for any integers m and n,

$$mc + nd = map + naq = a(mp + nq) = ax,$$

where $x = mp + nq$ is an integer. So $a \mid (mc + nd)$. ■

2.5 Basic properties

We begin with the key definition.

Definition 2.11 *Prime numbers*

An integer n, where $n \geq 2$, is said to be **prime** if it has no positive factor other than itself and 1. Otherwise n is said to be **composite**.

Notice that we have excluded consideration of 0 and the negative integers from these definitions; we will not be concerned with the primality or otherwise of non-positive integers. Notice also that the integer 1 is classified neither as prime nor as composite. As the composite integers are essentially those that can be broken down into products of at least two non-trivial (that is, not itself and 1) positive factors, it is natural to exclude 1 from the composite integers. On the other hand, we do not want to list 1 amongst the primes for a variety of reasons. For example, if 1 were to be considered as a prime,

$$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3$$

would be three (of infinitely many) different ways of expressing 6 as a product of primes. Excluding 1 from the list of primes enables us to express any integer greater than or equal to 2 as a *unique* product of primes. This result, which we will prove shortly, is of great importance in the study of number theory.

By a product we mean any number of integers multiplied together, including the possibility of a single integer on its own, such as 2.

Is there an efficient way of determining whether a given integer is prime? For example, is 211 prime or is it composite? If we can spot an integer in the range 2 to 210 that divides 211 then we can conclude immediately that 211 is composite. On the other hand, to show that 211 is prime there are a lot of potential factors to be eliminated. Do we have to test division by all the numbers in the range 2 to 210? Fortunately we do not. The following two results show that the list of potential factors can be drastically reduced. The first of these results appeared in Book VII of Euclid's *Elements*.

Proposition 2.12

Each integer $n \geq 2$ is divisible by some prime number.

If n is prime then n is a prime factor of itself.

Proof Preparing for a proof by mathematical induction (using the Second Principle), let $P(n)$ be the statement that the integer $n \geq 2$ is divisible by some prime number.

The statement $P(2)$ is certainly true, since 2 divides 2 and 2 is prime, and this provides the basis for the induction.

For the induction step suppose that for some integer $k \geq 2$, each of $P(2)$, $P(3)$, ..., $P(k)$ is true; that is, suppose that each of the integers 2, 3, ..., k is divisible by some prime. Now consider the next integer, $k+1$. Either $k+1$ is prime or it is composite. If it is a prime, it is divisible by the prime $k+1$ itself. If it is composite, then $k+1 = rs$, where r and s are integers with $2 \leq r \leq k$, whereupon the induction hypothesis tells us that there is some prime p that divides r. But then p divides r and r divides $k+1$ and so p divides $k+1$. In either case we conclude that $k+1$ is divisible by some prime, confirming the truth of $P(k+1)$.

The result follows by mathematical induction. ■

The next result determines a limit to the number of divisions one has to make in order to decide whether a given integer $n \geq 2$ is prime or not.

Proposition 2.13

If the integer $n \geq 2$ is composite, then it is divisible by some prime $p \leq \sqrt{n}$.

Proof As n is composite we can write $n = ab$, where a and b are integers with $2 \leq a \leq b$. Now we cannot have $a > \sqrt{n}$, for that would imply $b > \sqrt{n}$ and the product ab would exceed n. So $a \leq \sqrt{n}$. At this point we can invoke Proposition 2.12, which guarantees the existence of a prime p dividing a (and therefore dividing n). As $p \leq a \leq \sqrt{n}$, p suffices as the required prime. ■

This proposition can be applied to the question of whether 211 is composite. The prime numbers that are less than $\sqrt{211}$ are 2, 3, 5, 7, 11 and 13, and so if 211 is composite it must be divisible by one of these primes. However, straightforward division shows that this is not the case: 211 has remainder 1 when divided by each of 2, 3, 5 and 7, remainder 2 on division by 11 and remainder 3 on division by 13. Hence 211 is prime.

Exercise 2.7

(a) Which, if any, of the integers 111, 113, 115 and 117 is prime?

(b) To test whether or not 499 is a prime, for which numbers is it sufficient to check divisibility?

2.6 The Fundamental Theorem of Arithmetic

Any composite integer can be expressed, possibly in many ways, as a product of factors. For instance, observing that 11 divides 660, we may express the latter as 11×60. Now the factor 60 is composite, so it may be broken down further into, for example, 4×15, so that $660 = 11 \times 4 \times 15$. The factors 4 and 15 are each composite, so they can be broken down further. Indeed, by continuing to break down any composite factor in this way, we can eventually express the original number as a product of primes. Figure 2.4 shows three ways in which 660 can be broken down to its prime factors.

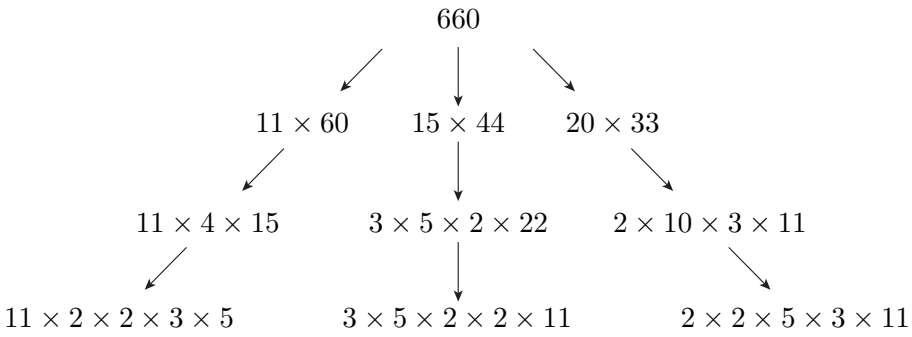


Figure 2.4 Expressing 660 as a product of primes

What is noticeable is that in all these ways of breaking down 660, we end up with the same product of primes; the order in which they are written varies, but in all cases $660 = 2 \times 2 \times 3 \times 5 \times 11$. Our next goal is to show that every integer greater than 1 is expressible as a product of primes in a unique way (except for the order in which the primes are written) – but on the way we will need some divisibility properties involving primes.

First we record one simple property, which will come up frequently, concerning highest common factors. Suppose that p is prime and n is any integer. What can we say about $\text{hcf}(n, p)$? As the only factors of prime p are p itself and 1, $\text{hcf}(n, p)$ has just the two possible values, namely p and 1. Now $\text{hcf}(n, p)$ takes value p precisely when p divides n. Hence we have the following property.

The value of $\text{hcf}(n, p)$

If p is a prime and n is any integer, then

$$\text{hcf}(n, p) = \begin{cases} p, & \text{if } p \text{ divides } n, \\ 1, & \text{otherwise.} \end{cases}$$

If a prime p divides a product of numbers then it must divide one of those numbers.

Theorem 2.14 *Euclid's Lemma for prime factors*

If p is prime and p divides the product $a_1a_2\cdots a_n$ then p divides a_i, for some integer i, where $1 \leq i \leq n$.

Proof We prove the result by mathematical induction on the number of terms in the product. With that goal in mind let $P(n)$ be the statement of the theorem.

We have the basis for induction since $P(1)$ is trivially true, for it states that if p divides a_1, then p divides a_1.

Heading for the induction step, suppose that $P(k)$ is true for some integer $k \geq 1$, that is, if p divides the product of any k integers then p divides one of them. Now consider any product of $k+1$ integers that is divisible by p, say

$$p \mid a_1a_2\cdots a_ka_{k+1}.$$

Either p divides a_{k+1} or it does not. If p divides a_{k+1} we are finished. If p does not divide a_{k+1} then $\text{hcf}(p, a_{k+1}) = 1$. Since p divides the product $(a_1a_2\cdots a_k)a_{k+1}$ and $\text{hcf}(p, a_{k+1}) = 1$ we conclude that p divides $a_1a_2\cdots a_k$. But then, by the induction hypothesis, p divides a_i for some i, where $1 \leq i \leq k$.

Putting the two possibilities together, either p divides a_{k+1} or p divides a_i for some i, where $1 \leq i \leq k$, which verifies that $P(k+1)$ is true. Hence, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers. ■

One consequence of Theorem 2.14 merits recording, as follows.

Corollary 2.15 *to Euclid's Lemma for prime factors*

If p, p_1, p_2, …, p_n are primes such that

$$p \mid p_1p_2\cdots p_n,$$

then $p = p_i$ for some i, where $1 \leq i \leq n$.

Proof Theorem 2.14 tells us that p divides p_i for some i, where $1 \leq i \leq n$. But the only factors of p_i are 1 and p_i, and as 1 is not a prime, it follows that $p = p_i$. ■

The following worked exercise makes use of these results.

Worked Exercise 2.16

Let p be prime and a and b be integers. Show that:

(a) if p divides a^n, then p^n divides a^n

(b) if $\text{hcf}(a, b) = p$, then $\text{hcf}\,(a^n, b^n) = p^n$.

Solution

(a) Using Theorem 2.14 with $a_1 = a_2 = \cdots = a_n = a$, we deduce immediately that if p divides a^n then p divides a. Hence $a = pr$, for some integer r. Raising both sides of this equation to the power n gives $a^n = p^n r^n$, which tells us that p^n divides a^n.

(b) If $\text{hcf}(a, b) = p$, there exist integers r and s such that $a = pr$ and $b = ps$, with $\text{hcf}(r, s) = 1$. But then

$$\begin{aligned}\text{hcf}\,(a^n, b^n) &= \text{hcf}\,(p^n r^n, p^n s^n)\\ &= p^n \text{hcf}\,(r^n, s^n)\,.\end{aligned}$$

It remains to show that $\text{hcf}\,(r^n, s^n) = 1$.

Suppose q is a prime that divides $\text{hcf}\,(r^n, s^n)$. Then q divides r^n and q divides s^n. As we saw in part (a), this implies that q divides r and q divides s, so that q divides $\text{hcf}(r, s)$. But $\text{hcf}(r, s) = 1$, contradicting the existence of such a prime q.

Hence $\text{hcf}\,(r^n, s^n) = 1$, which completes the proof.

We are just about ready for our main result of this section, but first a word about notation. Earlier we saw several ways of expressing 660 as a product of primes, the only difference between the expressions being the order in which the primes were written. Conventionally, when writing a number down as a product of its prime factors, we arrange the primes in ascending order with like primes collected together as a power. For instance, we write 660 as

$$660 = 2^2 \times 3 \times 5 \times 11.$$

This convention removes the ambiguity of ordering and, as we are about to see, renders a unique representation of the integer as a product of its prime factors. We refer to this as the **prime decomposition** of the integer.

Exercise 2.8

Give the prime decompositions of each of the integers 168, 226 and 36 000.

Theorem 2.17 *The Fundamental Theorem of Arithmetic*

Any integer $n \geq 2$ can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where p_i, $i = 1, \ldots, r$, are primes with $p_1 < p_2 < \cdots < p_r$ and each k_i, $i = 1, \ldots, r$, is a natural number.

As its name suggests, this theorem is central to many investigations in number theory.

Proof We prove the theorem in two parts. First, we show the *existence* of such a decomposition, that is, we show that n can be expressed as such a product of primes. Second, we show that the prime decomposition obtained is *unique*.

Existence

With proof by mathematical induction in mind, let $P(n)$ be the proposition that n can be expressed as a product of primes. We need to show that $P(n)$ is true for all $n \geq 2$.

Now $P(2)$ is certainly true, since 2 is a prime, and so we have the basis for the induction.

Suppose that, for some integer $k \geq 2$, $P(2)$, $P(3)$, ..., $P(k)$ are all true. That is, each of 2, 3, ..., k can be written as a product of primes. Now consider the integer $k+1$. By Proposition 2.12, $k+1$ is divisible by some prime p and so we may write $k+1 = pr$, for some integer r. If $r = 1$, $k+1$ is a prime and we are done. If $r > 1$ then, as $r < k+1$, the induction hypothesis tells us that r is a product of primes, whereupon $k+1 = pr$ is also a product of primes. It follows therefore that $P(k+1)$ is true.

Hence, by the Second Principle of Mathematical Induction, $P(n)$ is true for all integers $n \geq 2$.

Uniqueness

Suppose that some integer $n \geq 2$ has two representations as a product of primes, say,

$$\begin{aligned} n &= p_1 p_2 \cdots p_r, \quad \text{where } p_1 \leq p_2 \leq \cdots \leq p_r, \\ &= q_1 q_2 \cdots q_s, \quad \text{where } q_1 \leq q_2 \leq \cdots \leq q_s. \end{aligned}$$

Note that in these expressions for n we have kept the primes separate rather than collecting them in powers.

Now p_1 divides n and so p_1 divides the product $q_1 q_2 \cdots q_s$. By the Corollary to Euclid's Lemma for prime factors, this gives $p_1 = q_j$ for some $1 \leq j \leq s$. As $q_1 \leq q_j$ we conclude that $q_1 \leq p_1$. But there is symmetry between the ps and qs. So similarly we argue that since q_1 divides n, we have $q_1 = p_i$ for some $1 \leq i \leq r$, which leads to $p_1 \leq q_1$. Combining the two inequalities gives $p_1 = q_1$.

Since p_1 divides n we have $n = p_1 n_1$ for some integer n_1. Hence

$$n_1 = p_2 \cdots p_r = q_2 \cdots q_s,$$

and a repetition of the argument gives $p_2 = q_2$. Then, putting $n = p_1 p_2 n_2$, we get

$$n_2 = p_3 \cdots p_r = q_3 \cdots q_s,$$

giving $p_3 = q_3$.

We can continue in this way, cancelling equal primes from the left of the two products.

If $r < s$ then we obtain $p_i = q_i$ for $1 \leq i \leq r$ and we are left with

$$1 = q_{r+1} \cdots q_s.$$

This is a contradiction, since the q_i are primes. The assumption that $r > s$ leads to a similar contradiction. Hence $r = s$ and the proof of the uniqueness of the prime decomposition is complete. ■

Exercise 2.9

(a) Show that the integer $n > 1$ with prime decomposition $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is a square if, and only if, each of the exponents k_i is even.

(b) Use the identity $n^3 - 1 = (n-1)\left(n^2 + n + 1\right)$ to prove that the only prime of the form $n^3 - 1$ is 7.

Exercise 2.10

(a) Find the prime decomposition of 20!

(b) Given that p and q are distinct primes such that their product pq divides a^n, prove that $(pq)^n$ divides a^n.

(c) Prove that the only prime p for which $3p + 1$ is a square is $p = 5$.

(d) Show that for any prime p, $8p - 1$ and $8p + 1$ cannot both be prime.

Hint: use the fact that p must be either equal to 3 or of one of the forms $3k + 1$ or $3k + 2$.

(e) Let $p \geq 5$ be prime. Show that the remainder on dividing p by 12 must be one of 1, 5, 7 or 11. Hence prove that if $p \geq q \geq 5$ are primes then $24 | \left(p^2 - q^2\right)$.

(f) Prove (as Cataldi did in 1588) that if a is a natural number and $n \geq 2$ such that $a^n - 1$ is prime then $a = 2$ and n is prime.

Hint: consider the factorisation $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$.

Solutions and comments on exercises

Solution to Exercise 2.1

(a) (i) The set $\{n \in \mathbb{Z} : |n| > 20\}$ consists of all the integers except those from -20 to 20 inclusive. That is,

$$\{\ldots, -23, -22, -21, 21, 22, 23, \ldots\}.$$

(ii) The set $\{n : n = 2m^2, \text{ for some } m \in \mathbb{N}\}$ is the set consisting of those integers that are equal to twice the square of a positive integer, namely

$$\{2, 8, 18, 32, \ldots\}.$$

(b) (i) The set is $\{n : n = 2m - 1, \text{ for some } m \in \mathbb{N}\}$.

We could equally well write this set as $\{n : n = 2m + 1, \text{ for some } m \in \mathbb{Z} \text{ with } m \geq 0\}$.

(ii) The set is $\{n \in \mathbb{Z} : |n| \leq 100\}$.

Solution to Exercise 2.2

(a) Let $P(n)$ be the proposition that the formula is true for the natural number n.

Then $P(1)$ is true since

$$1^2 = \tfrac{1}{6} \times 1(1+1)(2+1).$$

Hence we have the basis for the induction.

For the induction step, assume that $P(k)$ is true, that is,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \tfrac{1}{6}k(k+1)(2k+1).$$

Then

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2, &\quad \text{the LHS of } P(k+1),\\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2, \quad \text{by the induction hypothesis,}\\
&= \tfrac{1}{6}(k+1)\left(2k^2 + k + 6(k+1)\right)\\
&= \tfrac{1}{6}(k+1)\left(2k^2 + 7k + 6\right)\\
&= \tfrac{1}{6}(k+1)(k+2)(2k+3)\\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1), \quad \text{the RHS of } P(k+1).
\end{aligned}$$

This shows that $P(k+1)$ is true and completes the induction step.

Hence, by mathematical induction, the formula is true for all natural numbers n.

(b) Let $P(n)$ be the proposition that the formula is true for n.

Then $P(1)$ is true since

$$a = \frac{a(r-1)}{r-1}.$$

So we have the basis for the induction.

Now for the induction step. Assume that $P(k)$ is true; that is,

$$a + ar + ar^2 + ar^3 + \cdots + ar^{k-1} = \frac{a(r^k - 1)}{r - 1}.$$

Then

$$\begin{aligned} a + ar + ar^2 + ar^3 + \cdots + ar^{k-1} + ar^k \\ &= \frac{a(r^k - 1)}{r - 1} + ar^k, \quad \text{by the induction hypothesis,} \\ &= \frac{a(r^k - 1) + ar^k(r - 1)}{r - 1} \\ &= \frac{a(r^{k+1} - 1)}{r - 1}, \end{aligned}$$

which is $P(k + 1)$, completing the induction step.

Hence, by mathematical induction, the formula is true for all natural numbers n.

Solution to Exercise 2.3

Let $P(n)$ be the proposition that $L_n < \left(\frac{7}{4}\right)^n$.

We note that $P(1)$ and $P(2)$ are true since

$$L_1 = 1 < \tfrac{7}{4} \quad \text{and} \quad L_2 = 3 < \left(\tfrac{7}{4}\right)^2 = \tfrac{49}{16}.$$

So we have the basis for the induction.

For the induction step (using the Second Principle) suppose that $P(1)$, $P(2)$, …, $P(k)$ are all true and consider $P(k + 1)$ for $k \geq 2$.

$$\begin{aligned} L_{k+1} &= L_k + L_{k-1} \\ &< \left(\tfrac{7}{4}\right)^k + \left(\tfrac{7}{4}\right)^{k-1}, \quad \text{by the induction hypothesis,} \\ &= \left(\tfrac{7}{4}\right)^{k-1} \left(\tfrac{7}{4} + 1\right) \\ &= \left(\tfrac{7}{4}\right)^{k-1} \left(\tfrac{11}{4}\right) \\ &< \left(\tfrac{7}{4}\right)^{k-1} \left(\tfrac{7}{4}\right)^2, \quad \text{since } \tfrac{11}{4} < \tfrac{49}{16}, \\ &= \left(\tfrac{7}{4}\right)^{k+1}, \end{aligned}$$

which shows that $P(k + 1)$ is true.

Hence, by the Second Principle of Mathematical Induction, the proposition is true.

Note that, since the proof of the induction step uses the formula $L_{k+1} = L_k + L_{k-1}$, which holds only for $k \geq 2$, our induction step first deduces the truth of $P(3)$ from that of $P(1)$ and $P(2)$, and then goes on to deduce the truth of $P(4)$, $P(5)$, etc. It does not deduce the truth of $P(2)$ from $P(1)$. Hence we have to show the truth of $P(2)$ separately, which we have done by including it in the basis for the induction.

Solution to Exercise 2.4

(a) (i) Let $P(n)$ be the proposition that the formula is true for n.

$P(1)$ is true, since

$$1^2 = \tfrac{1}{3} \times 1 \times (4 \times 1^2 - 1).$$

This gives the basis for the induction.

Assume that $P(k)$ is true for some natural number k; that is,

$$1^2 + 3^2 + 5^2 + \cdots + (2k-1)^2 = \tfrac{1}{3}k(4k^2 - 1).$$

Then

$$\begin{aligned}
1^2 + 3^2 + 5^2 + \cdots + (2k-1)^2 + (2k+1)^2, &\quad \text{the LHS of } P(k+1),\\
&= \tfrac{1}{3}k(4k^2 - 1) + (2k+1)^2, \quad \text{by the induction hypothesis,}\\
&= \tfrac{1}{3}k(2k-1)(2k+1) + (2k+1)^2\\
&= \tfrac{1}{3}(2k+1)[k(2k-1) + 3(2k+1)]\\
&= \tfrac{1}{3}(2k+1)(2k^2 + 5k + 3)\\
&= \tfrac{1}{3}(2k+1)(2k+3)(k+1)\\
&= \tfrac{1}{3}(k+1)(4k^2 + 8k + 3)\\
&= \tfrac{1}{3}(k+1)(4(k+1)^2 - 1), \quad \text{the RHS of } P(k+1),
\end{aligned}$$

which establishes the truth of $P(k+1)$, and completes the induction step.

Hence, by the Principle of Mathematical Induction, the formula is true for all natural numbers.

(ii) Let $P(n)$ be the proposition that the formula is true for n.

Then $P(1)$ is true since

$$1 = \tfrac{1}{2} \times 1^2 \times (1+1).$$

Assume that $P(k)$ is true; that is,

$$1 + 5 + 12 + 22 + \cdots + \tfrac{1}{2}k(3k-1) = \tfrac{1}{2}k^2(k+1).$$

Then

$$\begin{aligned}
1 + 5 + 12 + 22 + \cdots + \tfrac{1}{2}k(3k-1) + \tfrac{1}{2}(k+1)(3k+2)&\\
= \tfrac{1}{2}k^2(k+1) + \tfrac{1}{2}(k+1)(3k+2)&\\
= \tfrac{1}{2}(k+1)(k^2 + 3k + 2)&\\
= \tfrac{1}{2}(k+1)^2(k+2),&
\end{aligned}$$

confirming that $P(k+1)$ is true and completing the induction step.

The truth of $P(n)$ for all $n \geq 1$ follows by mathematical induction.

(b) Let $P(n)$ be the proposition that the formula is true for n.

$P(1)$ is certainly true since

$$1 \times (1!) = 2! - 1,$$

both sides being equal to 1.

For the induction step, suppose that $P(k)$ is true for some $k \geq 1$. That is,

$$1 \times (1!) + 2 \times (2!) + \cdots + k \times (k!) = (k+1)! - 1.$$

Then

$$\begin{aligned} 1 \times (1!) + 2 \times (2!) + \cdots + k \times (k!) + (k+1) \times ((k+1)!) \\ &= (k+1)! - 1 + (k+1)((k+1)!) \\ &= (k+1)!(1 + k + 1) - 1 \\ &= (k+2)! - 1, \end{aligned}$$

which confirms the truth of $P(k+1)$ and completes the induction step.

The truth of $P(n)$ for all $n \geq 1$ follows by mathematical induction.

(c) We observe that $n!$ increases more rapidly than $6n^2$ and $n!$ exceeds $6n^2$ for the first time when $n = 6$. So we make the conjecture that $n! > 6n^2$ for all $n \geq 6$, and prove it by mathematical induction.

Let $P(n)$ be the proposition that $n! > 6n^2$. Now

$$6! = 720 > 6 \times 6^2 = 216,$$

so $P(6)$ is true, giving us the basis for induction.

Suppose that $P(k)$ is true for some integer $k \geq 6$, that is,

$$k! > 6k^2.$$

On multiplying through by $k+1$, we get

$$(k+1)! > 6k^2(k+1).$$

If we can show that $k^2 \geq k+1$ it will follow that $(k+1)! > 6(k+1)^2$, completing the induction step. But this is easily seen since, for $k \geq 6$,

$$k^2 \geq 6k > 2k = k + k > k + 1,$$

which completes the induction step.

So by the Generalised Principle of Mathematical Induction, $P(n)$ is true for all $n \geq 6$.

(d) Suppose that

$$S = \{k \in \mathbb{Z} : k \geq n_0 \text{ and } P(k) \text{ is false}\}$$

is non-empty. We cannot apply the Well-Ordering Principle directly to this set, as it may not be a subset of $\mathbb{N}$.

Now consider the set T defined by

$$T = \{s - n_0 : s \in S\}.$$

Certainly T is a non-empty set of integers, each of whose elements is greater than or equal to zero. Now, by condition (a), $P(n_0)$ is true so n_0 is not an element of S. Hence zero is not an element of T, and T is a non-empty subset of $\mathbb{N}$.

By the Well-Ordering Principle, T has a least element. We may take this least element of T to be $m - n_0$ for some integer m in S and, by the definition of T, it follows that m is the least element of S.

Furthermore, since $n_0 \notin S$ we know that $m > n_0$, which ensures that the list $P(n_0)$, $P(n_0 + 1)$, ..., $P(m - 1)$ contains at least one element. By the definition of S it follows that $P(n_0), P(n_0 + 1)$, ..., $P(m - 1)$ must all be true. But then condition (b′) gives that $P(m)$ is true, which contradicts the fact that $m \in S$.

Hence the only assumption made, namely that S is non-empty, must be false. Hence S is empty and so the proposition $P(k)$ is true for all $k \geq n_0$.

Solution to Exercise 2.5

Cubing each of the three given forms that the number can take, and then writing each cube in the form $9n + r$, where $0 \leq r < 9$, gives

$$(3n)^3 = 27n^3 = 9(3n^3) + 0,$$
$$(3n + 1)^3 = 27n^3 + 27n^2 + 9n + 1 = 9(3n^3 + 3n^2 + n) + 1,$$
$$(3n + 2)^3 = 27n^3 + 54n^2 + 36n + 8 = 9(3n^3 + 6n^2 + 4n) + 8.$$

Hence the only possible remainders are 0, 1 and 8.

Solution to Exercise 2.6

(a) The factors of 18 are 1, 2, 3, 6, 9 and 18. The factors of -24 are 1, 2, 3, 4, 6, 8, 12 and 24. (These are the same as the factors of 24.)

The common factors of 18 and -24 are 1, 2, 3 and 6.

(b) The Division Algorithm tells us that n takes one of the three forms $3k$, $3k + 1$ or $3k + 2$. But n is not a multiple of 3 and so the first of these forms cannot occur.

For $n = 3k + 1$ we get

$$(3k + 1)^2 - 1 = 9k^2 + 6k + 1 - 1 = 3(3k^2 + 2k).$$

For $n = 3k + 2$ we get

$$(3k + 2)^2 - 1 = 9k^2 + 12k + 4 - 1 = 3(3k^2 + 4k + 1).$$

In each case $n^2 - 1$ has remainder zero on dividing by 3.

Solution to Exercise 2.7

(a) As $11^2 > 117$ we need to test each of the given numbers for divisibility only by 2, 3, 5 and 7.
111 is divisible by 3, and so is composite.
113 is not divisible by 2, 3, 5 or 7 and so is prime.
115 is divisible by 5 and so is composite.
117 is divisible by 3 and so is composite.

(b) Since $22 < \sqrt{499} < 23$, it suffices to check divisibility by the primes not exceeding 22, that is, by 2, 3, 5, 7, 11, 13, 17 and 19.

Solution to Exercise 2.8

$168 = 2^3 \times 3 \times 7$

$226 = 2 \times 113$

$36000 = 2^5 \times 3^2 \times 5^3$

Solution to Exercise 2.9

(a) On the one hand if each exponent is even, say $k_i = 2l_i$, then

$$n = p_1^{2l_1} p_2^{2l_2} \cdots p_r^{2l_r} = \left(p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}\right)^2$$

is a square.

On the other hand if n is a square, say $n = a^2$, then writing $a = q_1^{m_1} q_2^{m_2} \cdots q_t^{m_t}$ in its prime decomposition and squaring gives

$$n = q_1^{2m_1} q_2^{2m_2} \cdots q_t^{2m_t}.$$

As the q_i are distinct primes and each m_i is positive, this is the unique prime decomposition of n, revealing that each exponent is even.

Note that a simple modification of this argument generalises the result to any power; an integer is an nth power if, and only if, each of its prime exponents is a multiple of n.

(b) If $n^3 - 1$ is prime then the given identity expresses a prime as a product of two factors. The uniqueness of prime decomposition tells us that this cannot happen unless one of these factors is 1. Now $n > 1$ (since $n^3 - 1$ is prime) and so $n^2 + n + 1 > 3$. The only possibility is that $n - 1 = 1$, giving $n = 2$ and $n^3 - 1 = 7$.

Solution to Exercise 2.10

(a) As

$$20! = 1 \times 2 \times 3 \times 4 \times \cdots \times 19 \times 20$$

it is divisible by each of the primes from 2 to 19 inclusive, and by no others.

Looking at the terms on the right-hand side, the primes from 11 to 19 occur just once. The prime 7 occurs twice, in the terms 7 and 14. The prime 5 occurs in terms 5, 10, 15 and 20. The prime 3 occurs once in each term 3, 6, 12 and 15 but twice in terms 9 and 18, making eight occurrences in all. Finally, the prime 2 occurs once in terms 2, 6, 10, 14 and 18, twice in terms 4, 12 and 20, three times in term 8 and four times in term 16, making a total of eighteen occurrences. Hence

$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19.$$

(b) Since pq divides a^n, we know that p divides a^n and Euclid's Lemma for prime factors gives p divides a. Similarly, q divides a^n and so q divides a. Now as p and q are distinct primes, $\text{hcf}(p, q) = 1$ and so pq divides a; say $(pq)r = a$. But then, raising to the nth power, $(pq)^n r^n = a^n$, which confirms that $(pq)^n$ divides a^n.

(c) Suppose that $3p + 1$ is a square, say $3p + 1 = n^2$. Then

$$3p = n^2 - 1 = (n - 1)(n + 1).$$

Now $n > 2$, since $p \geq 2$, and so the right-hand side of this equation is a product of two factors each exceeding 1. The left-hand side is the product of two primes. By uniqueness of prime decomposition we must have either $3 = n - 1$ and $p = n + 1$, or alternatively $3 = n + 1$ and $p = n - 1$. The former case leads to $n = 4$ and $p = 5$, which is one solution. The latter case leads to $n = 2$ and $p = 1$, which is invalid.

(d) Thinking in terms of remainders on division by 3, there are three possibilities for the prime p: it is 3, of form $3k + 1$, or of form $3k + 2$.

If $p = 3$ then $8p + 1 = 25$ is composite.
If $p = 3k + 1$ then $8p + 1 = 24k + 9 = 3(8k + 3)$ is composite.
If $p = 3k + 2$ then $8p - 1 = 24k + 15 = 3(8k + 5)$ is composite.

(e) The prime p must take one of the twelve forms $12k + r$, where $0 \leq r \leq 11$. However, when r is even $12k + r$ is divisible by 2, and similarly $12k + r$ is divisible by 3 when $r = 3$ or 9. The only remaining possibilities are $12k + 1$, $12k + 5$, $12k + 7$ and $12k + 11$, and any prime $p \geq 5$ must take one of these forms.

We are told that $p \geq 5$ and so $p = 2$ and $p = 3$ are not possibilities.

Now

$$(12k + 1)^2 = 24\left(6k^2 + k\right) + 1,$$
$$(12k + 5)^2 = 24\left(6k^2 + 5k + 1\right) + 1,$$
$$(12k + 7)^2 = 24\left(6k^2 + 7k + 2\right) + 1,$$
$$\text{and } (12k + 11)^2 = 24\left(6k^2 + 11k + 5\right) + 1.$$

So whichever of the four forms p takes, p^2 is of the form $24m + 1$.

If q is another such prime, say $q^2 = 24n + 1$, then

$$p^2 - q^2 = (24m + 1) - (24n + 1) = 24(m - n)$$

which is divisible by 24.

(f) Consider the given factorisation

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

For $a^n - 1$ to be prime, one of the two factors on the right-hand side of this equation will have to be equal to 1. The only way this can happen is when $a - 1 = 1$, so that $a = 2$.

Next, suppose that n is composite, say $n = rs$, where $r > 1$ and $s > 1$. Then $2^n - 1 = (2^r)^s - 1$, and so replacing a by 2^r and replacing n by s in the above factorisation:

$$(2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + 2^{r(s-3)} + \cdots + 2^r + 1).$$

Once again this expresses $2^n - 1$ as a product of two factors and, this time, since $2^r > 2$ neither factor is equal to 1. This contradicts the primality of $2^n - 1$. The only assumption we have made is that $n = rs$ is composite. Hence we conclude that n must be prime.

Index

$3\mathbb{Z}$, 16
$|n|$, 17
$b \mid a$, 31
$b \nmid a$, 31

arithmetic progression, 8
arithmetic series, 8

basis for the induction, 19
braces, 16

coprime, 34

Diophantine equation, 45
divides, 31
divisibility, 31
Division Algorithm, 28
divisor, 31

Euclid's Lemma, 36
Euclidean Algorithm, 42

factor, 31
factorial, 27

$\gcd(a, b)$, 33
geometric series, 21
greatest common divisor, 33

$\mathrm{hcf}(a, b)$, 33
heptagonal numbers, 12
heptagonal-based pyramidal numbers, 14
hexagonal numbers, 11
highest common factor, 33

induction hypothesis, 19
induction step, 19
integer, 16
integer combination, 33

$k!$, 27

$\mathrm{lcm}(a, b)$, 39
least common multiple, 39
linear Diophantine equation, 45

mathematical induction, 19
modulus, 17
multiple, 31

$\mathbb{N}$, the natural numbers, 16
non-negative integers, 45

octagonal numbers, 12

$P(k, n)$, the nth k-gonal number, 13
pentagonal numbers, 11
polygonal numbers, 12
Principle of Induction, 18
Principle of Mathematical Induction, 19
Principle of Mathematical Induction (generalised), 22
pyramidal numbers, 13

$Q(k, n)$, the nth k-gonal pyramidal number, 15
$\mathbb{Q}$, the rational numbers, 16

$\mathbb{R}$, the real numbers, 16
rational numbers, 16
relatively prime, 34

Second Principle of Mathematical Induction, 24
set, 16
square number, 9
square-based pyramidal numbers, 14

T_n, the nth triangular number, 8
triangle-based pyramidal numbers, 13
triangular numbers, 8

Well-Ordering Principle, 17

$\mathbb{Z}$, the integers, 16