

An Introduction to

Mathematical Reasoning

An Introduction to **Mathematical Reasoning**

numbers, sets and functions

Peter J. Eccles
*Department of Mathematics
University of Manchester*



CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo,
Delhi, Dubai, Tokyo

Cambridge University Press
The Edinburgh Building, Cambridge, CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521597180

© Cambridge University Press 2007

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 1997
Thirteenth printing 2010

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record of this publication is available from the British Library

Library of Congress Cataloging in Publication data
Eccles, Peter J., 1945-

An introduction to mathematical reasoning: lectures on numbers, sets,
and functions / Peter J. Eccles.

p. cm.

Includes bibliographical references and index.

ISBN 0 521 59269 0 hardback – ISBN 0 521 59718 8 paperback

1. Proof theory. I. Title.

QA9.54.E23 1997

511.3—dc21 97-11977 CIP

ISBN 978-0-521-59269-7 hardback

ISBN 978-0-521-59718-0 paperback

Cambridge University Press has no responsibility for the persistence or accuracy
of URLs for external or third-party internet websites referred to in this publication,
and does not guarantee that any content on such websites is, or will remain,
accurate or appropriate. Information regarding prices, travel timetables and other
factual information given in this work are correct at the time of first printing but

Cambridge University Press does not guarantee the accuracy of such
information thereafter.

I too will something make
And joy in the making;
Altho' tomorrow it seem
Like the empty words of a dream
Remembered on waking.

Robert Bridges, *Shorter poems*.

In loving memory of

Elizabeth Baron and John Baron

(Auntie Lizzie and Uncle Jack)

and those Woodside Bank summers

Contents

<i>Preface</i>	<i>page</i>	ix
Part I: Mathematical statements and proofs		
1	The language of mathematics	3
2	Implications	10
3	Proofs	21
4	Proof by contradiction	30
5	The induction principle	39
	Problems I	53
Part II: Sets and functions		
6	The language of set theory	61
7	Quantifiers	74
8	Functions	89
9	Injections, surjections and bijections	101
	Problems II	115
Part III: Numbers and counting		
10	Counting	123
11	Properties of finite sets	133
12	Counting functions and subsets	144
13	Number systems	157
14	Counting infinite sets	170
	Problems III	182
Part IV: Arithmetic		
15	The division theorem	191
16	The Euclidean algorithm	199
17	Consequences of the Euclidean algorithm	207
18	Linear diophantine equations	216
	Problems IV	225

	Part V: Modular arithmetic	229
19	Congruence of integers	231
20	Linear congruences	240
21	Congruence classes and the arithmetic of remainders	250
22	Partitions and equivalence relations	262
	Problems V	271
	Part VI: Prime numbers	275
23	The sequence of prime numbers	277
24	Congruence modulo a prime	289
	Problems VI	295
	<i>Solutions to exercises</i>	299
	<i>Bibliography</i>	345
	<i>List of symbols</i>	346
	<i>Index</i>	347

Preface

This book is based on lectures given at the Victoria University of Manchester to first year Honours Mathematics students including those taking joint or combined degrees. In common with most other British mathematics departments, the Manchester mathematics department has thoroughly reviewed its curriculum in recent years in the attempt to meet more adequately the needs of students who have experienced the effects of the great changes in the teaching of mathematics in schools, as well as the increased numbers of ‘mature students’ and students from non-standard backgrounds.

It was clear to us at the University of Manchester that we should completely rethink and broaden our curriculum, including material which we had previously expected students to know on entry to the course but also including introductory material on combinatorics, computer skills and numerical mathematics, as well as encouraging the development of problem solving skills.

A key ingredient of this new University of Manchester curriculum is a module on Mathematical Reasoning whose purpose is to introduce the basic ideas of mathematical proof and to develop skills in writing mathematics, helping to bridge the gap between school and university mathematics. This book is based on this course module. The ability to write correct and clear mathematics is a skill which has to be acquired by observing experienced practitioners at work in lectures and tutorials, by learning to appreciate the details of mathematical exposition in books, and by a great deal of practice. It is a skill readily transferable to many other areas and its acquisition is likely to be one of the main benefits of a mathematics degree course for most students who may well make no further use of most of the specific mathematical content of the course!

There is no absolutely *correct* way of writing out a given proof. For

example, it is necessary to take into account who the intended reader is. But, whoever the reader is, the proof should be expressed as clearly as possible and to achieve this the writer needs to understand the logic of the proof. Writing a proof is not separate from discovering the proof in the way that writing up a scientific experiment is separate from carrying out the experiment or performing a piece of music is separate from composing it. Attempts to write out a proof are an important part of the discovery process. Alison Leonard has written in a totally different context:

Not only are human ideas conveyed by language, they are actually formed by the language available to us.[†]

So it is in mathematics, where we find a parallel development of mathematical ideas and mathematical language.

This is reflected in this book. The emphasis is on helping the reader to understand and construct proofs and to learn to write clear and concise mathematics. This can only be achieved by exploring some particular mathematical topics and the contexts chosen are set theory, combinatorics and number theory. These topics

- provide good examples to illustrate a range of basic methods of proof, in particular proof by induction and proof by contradiction,
- include some fundamental ideas which are part of the standard tool kit of any mathematician, such as functions and inverses, the binomial theorem, the Euclidean algorithm, the pigeonhole principle, the fundamental theorem of arithmetic, and congruence,
- build on ideas met in early schooling illustrating ways in which familiar ideas can be formulated rigorously, for example counting or the greatest common divisor,
- include some of the all time great classic proofs, for example the Euclidean proofs of the irrationality of root 2 and the infinity of primes, but also ideas from throughout mathematical history so that there is an opportunity to present mathematics as a continually developing subject.

Roughly speaking, the first three parts of the book are about the basic language of mathematics and the final three parts are about number theory, illustrating how the ideas of the earlier parts are applied to some significant mathematics. The reader may find that the later parts

[†] See Alison Leonard, *Telling our stories: wrestling with a fresh language for the spiritual journey*, Dorton, Longman and Todd, 1995.

contain some more straightforward material than the early parts simply because there is material on problem solving techniques which can then be practised on specific numerical examples. The topics selected for these later parts, the Euclidean algorithm, modular arithmetic and prime numbers, include material from the whole of mathematical history from classical Greek times to the present day.

I would encourage the reader in working through the first three parts not to expect to understand everything at first. Part I introduces various forms of mathematical statements and the standard methods of proof. Proof by contradiction and proof by induction are explained in detail and these methods are then used again and again throughout the remainder of the book: so many great theorems are proved by contradiction and some are included in this book. Part II covers the basic material on sets and functions which provides the language in which much mathematics is best expressed. It includes a leisurely discussion of universal and existential statements which are so important in university mathematics, particularly analysis or advanced calculus. This is not a book on mathematical logic but inevitably some ideas from the beginnings of that subject are included in these first two parts. The reader may find some of the material on counting in Part III to be more difficult than the rest of the book. It is best not to become discouraged by this but if necessary to move on to Part IV which is probably the easiest part but also includes some very striking and attractive results, returning to Part III when more familiarity with the language of sets and functions has been acquired. This material on counting provides good practice in using the language of sets and functions in a very familiar context and also illustrates how a familiar process may be made mathematically precise and how this then enables the process to be extended to a less familiar context, counting infinite sets.

The book is divided into twenty four chapters and grew out of a series of twenty four lectures. However, there is far more material in most chapters than could reasonably be covered in a single lecture. A lecture course based on this book would need to be selective covering either a subset of the chapters or, more likely, a subset of the material in most or all of the chapters as the author's lecture courses have done.

There is a great range of ability, experience and knowledge amongst students embarking on university mathematics courses and a real attempt has been made here to provide material meeting the needs of weaker or ill-prepared students whilst at the same time providing something which will interest and challenge the most able students. This is

achieved by including material and, in particular, problems of varying difficulty; many of the over 250 problems are routine and computational but others are quite demanding. In the later stages of the book some significant developments of the ideas in the book are approached in the problems.

Each chapter concludes with a number of exercises many of which are very closely related to material in the chapter and intended to be relatively straightforward and routine. Occasionally something a little harder is included. The reader is encouraged to work through all of these and full solutions for them are given at the back of the book. There are also six sets of problems, some similar to the exercises in order to consolidate the techniques involved but others more wide ranging and challenging. I hope that every reader will find some of the exercises and problems to be fun.

Mathematicians are not good at encouraging students to read around the subject but the intention here is that material in this book not covered in a lecture course will provide additional reading particularly for stronger students and, through the references given, lead to wider study in some areas. I have tried to write the book which I would have welcomed for my own students.

Finally, I am only too conscious that anyone who writes a book about how to write mathematics well lays themselves open to ridicule when the proofs in the book are found to be confused or inadequate. If the reader does find failings in the proofs in this book then I hope that acquiring the ability to see these failings will be seen as a useful step in developing that self-criticism which is necessary for the writing of clear and beautiful mathematics.

Acknowledgements. The author is indebted to very many people who have knowingly or unknowingly influenced the material in this book or who have provided specific advice. I would in particular like to acknowledge the contributions of the following: Pyotr Akhmet'ev, Michael Barratt, Francis Coghlan, Mark Eccles, Michael Eccles, Pamela Eccles, Douglas Gregory, Brian Hartley, Martin Huxley, John King-Hele, E. Makin, Mick McCrudden, Jeff Paris, Mike Prest, Nigel Ray, John Reade, András Szűcs, Grant Walker, George Wilmers, J.R. Winn and Reg Wood. In addition I wish to thank the staff of Cambridge University Press for their careful editorial work and an anonymous referee whose report on a preliminary version was extremely helpful.

Peter J. Eccles, Manchester, June 1997.

Part I

Mathematical statements and proofs

1

The language of mathematics

Pure mathematics is concerned with the exploration of mathematical concepts arising initially from the study of space and number. In order to capture and communicate mathematical ideas we must make statements about mathematical objects and much mathematical activity can be described as the formulation of mathematical statements and then the determination of whether or not such statements are true or false. It is important to be clear about what constitutes a mathematical statement and this is considered in this first chapter. We begin with simple statements and then examine ways of building up more complicated statements.

1.1 Mathematical statements

It is quite difficult to give a precise formulation of what a mathematical statement is and this will not be attempted in this book. The aim here is to enable the reader to recognize simple mathematical statements. First of all let us consider the idea of a *proposition*. A good working criterion is that *a proposition is a sentence which is either true or false (but not both)*. For the moment we are not so concerned about whether or not propositions are in fact true. Consider the following list.

- (i) $1 + 1 = 2$.
- (ii) $\pi = 3$.
- (iii) 12 may be written as the sum of two prime numbers.
- (iv) Every even integer greater than 2 may be written as the sum of two prime numbers.
- (v) The square of every even integer is even.
- (vi) n is a prime number.

- (vii) $n^2 - 2n > 0$.
- (viii) $m < n$.
- (ix) $12 = 11$.
- (x) π is a special number.

Of these the first five are propositions. This says nothing about whether or not they are true. In fact (i) is true and (ii) is false. Proposition (iii) is true since $12 = 7 + 5$ and 5 and 7 are prime numbers.[†] Propositions (iv) and (v) are general statements which cannot be proved by this sort of simple arithmetic. In fact it is easy to give a general proof of (v) (see Exercise 3.3) showing that it is true. However, at the time of writing, it is unknown whether (iv) is true or false; this statement is called the Goldbach conjecture after Christian Goldbach who suggested that it might be true in a letter to Leonhard Euler written in 1742.

On the other hand the others on the above list are not propositions. The next two, (vi) and (vii), become propositions once a numerical *value* is assigned to n . For example if $n = 2$ then (vi) is true and (vii) is false, whereas if $n = 3$ then they are both true. The next, (viii), becomes a proposition when values are assigned to both m and n , for example it is true for $m = 2, n = 3$ and false for $m = 3, n = 2$. Sentences of this type are called *predicates*. The symbols which need to be given values in order to obtain a proposition are called *free variables*.

The word *statement* will be used to denote either a proposition or a predicate. So in the above list the first eight items are statements. We will use a single capital letter P or Q to indicate a statement, or sometimes an expression like $P(m, n)$ to indicate a predicate, with the free variables listed in brackets.

The last two entries in the above list are not statements: (ix) is not even a sentence and (x) doesn't mean anything until we know what 'special' means. Very often mathematicians do give technical meanings to everyday words (as in 'prime' number used in (iii) and (iv) above and 'even' number used in (v)) and so if 'special' had been given such a meaning as a possible property of a number then (x) would be a proposition and so a statement. Of course the fact that (i) to (viii) are statements relies on a number of assumptions about the meanings of the symbols and words which have been taken for granted.

[†] A positive integer is a *prime number* if it is greater than 1 and is divisible only by 1 and itself. Thus the first few prime numbers are 2, 3, 5, 7, 11, This definition is discussed in Chapter 23.

In particular it is quite complicated to give a precise definition of the number π in statement (ii). The number π was originally defined geometrically as the ratio between the length of the circumference of a circle and the length of the diameter of the circle. In order for this definition to be justified it is necessary to define the length of the circumference, a curved line, and having done that to prove that the ratio is independent of the size of the circle. This was achieved by the Greeks in classical times. A regular hexagon inscribed in a circle of unit diameter has circumference 3 and so it is clear that $\pi > 3$.† Archimedes showed by geometrical means in his book *On the measurement of the circle* that $3\frac{10}{71} < \pi < 3\frac{1}{7}$ and also provided a beautiful proof of the formula πr^2 for the area of a circle of radius r . The modern definition of π is usually as twice the least positive number for which the cosine function vanishes, and the details may be found in any text on analysis or advanced calculus.‡

1.2 Logical connectives

In mathematics we are often faced with deciding whether some given proposition is true or whether it is false. Many statements are really quite complicated and are built up out of simpler statements using various ‘logical connectives’. For the moment we restrict ourselves to the simplest of these: ‘or’, ‘and’ and ‘not’. The truth or falsehood of a complicated statement is determined by the truth or falsehood of its component statements. It is important to be clear how this is done.

The connective ‘or’

Suppose that we say

For integers a and b , $ab = 0$ if $a = 0$ or $b = 0$.

The statement ‘ $a = 0$ or $b = 0$ ’ is true if $a = 0$ (regardless of the value of b) and is also true if $b = 0$ (regardless of the value of a). Notice that the statement is true if both $a = 0$ and $b = 0$ are true. This is called

† Some fundamentalist Christians have claimed that 1 Kings vii 23, in which a round object of diameter 10 cubits is stated to have a circumference of 30 cubits, ‘proves’ that $\pi = 3$ but mathematical truth can never be a matter simply of faith (nor can religious truth either in the author’s experience) and in any case there is no suggestion in the biblical passage that the measurements were highly accurate!

‡ See for example R. Haggerty, *Fundamentals of mathematical analysis*, Addison-Wesley, Second edition 1993.

the ‘inclusive’ use of ‘or’. Its meaning is best made precise by means of a *truth table*. Any statement may be either true or false: we say that ‘true’ and ‘false’ are the two possible *truth values* for the statement. So given two statements P and Q each has two possible truth values giving four possible combinations in all. The truth table for ‘or’ which follows specifies the truth value for ‘ P or Q ’ corresponding to each possible combination of truth values for P and for Q , one line for each. In the table T indicates ‘true’ and F indicates ‘false’.

Table 1.2.1

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

In this table, the truth values in the second line for example indicate that if P is true and Q is false then the statement ‘ P or Q ’ is true.

‘ P or Q ’ is called the *disjunction* of the two statements P and Q .

In everyday speech ‘or’ is often used in the exclusive sense as in the first sentence of this section: ‘we are faced with deciding whether some given proposition is true or whether it is false’, in which it is implicitly understood (and emphasized by the uses of the word ‘whether’) that it is not possible for a proposition to be both true and false.

To give another everyday example of the ‘exclusive or’, when we say ‘everyone will travel there by bus or by train’ this would normally be taken to mean that everyone uses one or other form of transport but not both. If we wanted to allow for someone using both we would probably say ‘everyone will travel there by bus or by train or by both’. In practice the precise meaning of ‘or’ is made clear by the context or there is some ambiguity (but not both!). The meaning of mathematical statements must be precise and so we avoid these ambiguities by always using ‘or’ in the inclusive way determined by the above truth table.

The connective ‘or’ is sometimes hidden in other notation. For example when we write ‘ $a \leq b$ ’ where a and b are real numbers this is a shorthand for ‘ $a < b$ or $a = b$ ’. Thus both the statements ‘ $1 \leq 2$ ’ and ‘ $2 \leq 2$ ’ are true.

Similarly ‘ $a = \pm b$ ’ is a shorthand for ‘ $a = b$ or $a = -b$ ’. There is some possibility of confusion here for the true statement that $1 = \pm 1$ does not mean that 1 and ± 1 are interchangeable: ‘if $x^2 = 1$ then $x = \pm 1$ ’ is a

true statement whereas ‘if $x^2 = 1$ then $x = 1$ ’ is a false statement! It is necessary to be clear that $a = \pm b$ is not asserting that a single equality is true but is asserting that one (or both) of two equalities $a = b$, $a = -b$ is true. The following truth table illustrating this may help.

a	b	$a = b$	$a = -b$	$a = \pm b$
1	2	F	F	F
1	1	T	F	T
2	-2	F	T	T
0	0	T	T	T

Observe how the truth values in the final column may be read off from the truth values in the previous two columns using the truth table for ‘or’ (Table 1.2.1).

In fact the statement $a = \pm b$ can be written as a single equation, namely $|a| = |b|$ where $|a|$ denotes the *absolute value* of a (i.e. $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a \leq 0$).

The connective ‘and’

We use this when we wish to assert that two things are both true. Again this word can be hidden in other words or notation. Thus if we assert that

π lies between 3 and 4

or in symbols

$3 < \pi < 4$

then this means that

$\pi > 3$ and $\pi < 4$

which is called the *conjunction* of the two statements ‘ $\pi > 3$ ’ and ‘ $\pi < 4$ ’.

You should construct a truth table for ‘and’.

The connective ‘not’

Finally we have the idea of the *negation* of a statement. The negation of a statement is true when the original statement is false and it is false when the original statement is true. This is described by the following truth table.

Table 1.2.2

P	not P
T	F
F	T

The negation of a statement is usually obtained by including the word ‘not’ in the statement but does require a little care since this is often used very loosely in everyday speech.

Example 1.2.3 Consider the following statement about a polynomial $f(x)$ with real coefficients, such as $x^2 + 3$ or $x^3 - x^2 - x$.

- (i) For real numbers a , if $f(a) = 0$ then a is positive (i.e. $a > 0$).

What is the negation of this statement? The following possibilities spring to mind from the everyday use of ‘negation’.

- (ii) For real numbers a , if $f(a) = 0$ then a is negative.
- (iii) For real numbers a , if $f(a) = 0$ then a is non-positive.
- (iv) For real numbers a , if $f(a) \neq 0$ then a is positive.
- (v) For real numbers a , if a is positive then $f(a) = 0$.
- (vi) For real numbers a , if a is positive then $f(a) \neq 0$.
- (vii) For real numbers a , if a is non-positive then $f(a) \neq 0$.
- (viii) For some non-positive real number a , $f(a) = 0$.

If you think about it you will see that none but the last is the negation. For example, if $f(x) = x^3 - x = x(x+1)(x-1)$ then statement (i) is certainly false since, for the real number 0, $f(0) = 0$ but 0 is not positive. On the other hand so are all the other statements apart from (viii) which is true since 0 is a non-positive number such that $f(0) = 0$. We will consider the negation of statements of this form more formally in the next chapter.

Exercises

1.1 Construct a truth table for ‘and’ as follows.

P	Q	P and Q
T	T	
T	F	
F	T	
F	F	

1.2 Construct truth tables for the statements

- (i) not (P and Q);
- (ii) (not P) or (not Q);
- (iii) P and (not Q);
- (iv) (not P) or Q .

1.3 Using the truth table for ‘or’ complete the following truth table for the statement $a \leq b$.

a	b	$a < b$	$a = b$	$a \leq b$
1	1			
2	1			
1	2			
-2	1			

1.4 Consider the following statement.

- (i) All girls are good at mathematics.

Which of the following statements is the negation of the above statement?

- (ii) All girls are bad at mathematics.
- (iii) All girls are not good at mathematics.
- (iv) Some girl is bad at mathematics.
- (v) Some girl is not good at mathematics.
- (vi) All children who are good at mathematics are girls.
- (vii) All children who are not good at mathematics are boys.

Can you find any statements in this list which have the same meaning as the original statement (i)?

1.5 Prove that $|a|^2 = a^2$ for every real number a .

2

Implications

In the first chapter we were mainly interested in the meaning of mathematical statements. However, mathematics is primarily concerned with establishing the truth of statements. This is achieved by giving a proof of the statement. The key idea in most proofs is that of implication and this idea is discussed in this chapter.

2.1 Implications

A proof is essentially a sequence of statements starting from statements we know† to be true and finishing with the statement to be proved. Each statement is true because the earlier statements are true. The justification for such steps usually makes use of the idea of ‘implication’; an implication is the assertion that if one particular statement is true then another particular statement is true.

The symbol usually used to denote implication in pure mathematics‡ is \Rightarrow although there are a variety of forms of words which convey the same meaning. For the moment we can think of ' $P \Rightarrow Q$ ' as asserting that if statement P is true then so is statement Q , which is often read as ' P implies Q '. The meaning will be made precise by means of a truth table. Before doing this it is necessary to clarify what this meaning should be and to do this we consider an example concerning an integer n .

Suppose that $P(n)$ is the statement ' $n > 3$ ' and $Q(n)$ is the statement

† See the section on ‘mathematical truth’ at the end of this chapter.

‡ In mathematical logic the symbol \rightarrow is usually used instead of \Rightarrow . Other symbols used in mathematical logic are ' $P \vee Q$ ' for ' P or Q ', ' $P \wedge Q$ ' for ' P and Q ', and ' $\neg P$ ' or ' $\sim P$ ' for 'not P '.

' $n > 0$ ', where n is an integer. Then the statement $P(n) \Rightarrow Q(n)$, i.e.

$$n > 3 \Rightarrow n > 0,$$

is the assertion that if an integer n is greater than 3 then it is greater than 0, which is certainly a true statement. Notice that this statement is true for each integer n even though the statement ' $n > 3$ ' is true for some values of n and false for others as is the statement ' $n > 0$ '. Let us consider the possibilities.

	$P(n)$	$Q(n)$
$n < 0$	F	F
$n = 0$	F	F
$n = 1$	F	T
$n = 2$	F	T
$n = 3$	F	T
$n > 3$	T	T

This table demonstrates that if it is true that $n > 3$ then it is indeed true that $n > 0$. But if $n \not> 3$ (i.e. $P(n)$ is false) then we may have $n > 0$ (so $Q(n)$ is true) for example when $n = 2$, and we may have $n \not> 0$ (so $Q(n)$ is false) for example when $n = -2$. However, there is no value of n for which $P(n)$ is true and $Q(n)$ is false; and this is precisely what we mean when we say that if $P(n)$ is true then $Q(n)$ is true. We can summarize this in the following truth table.

Table 2.1.1

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

In an implication $P \Rightarrow Q$, the statement P is called the *hypothesis* or *antecedent* and the statement Q is called the *conclusion* or *consequent*.

Here is another illustration. The assertion

$$n = 1 \Rightarrow (n - 1)(n - 2) = 0 \quad (\text{for integers } n)$$

is certainly true, for if we substitute $n = 1$ into $(n - 1)(n - 2)$ we obtain $(1 - 1)(1 - 2) = 0 \times (-1) = 0$. If we write $P(n)$ for the statement ' $n = 1$ ' and $Q(n)$ for the statement ' $(n - 1)(n - 2) = 0$ ' we can consider the

truth or falsehood of these two statements for different values of n as follows.

	$P(n)$	$Q(n)$
$n = 1$	T	T
$n = 2$	F	T
$n \neq 1, 2$	F	F

Thus $n = 1$ illustrates line 1 of Table 2.1.1, $n = 2$ illustrates line 3, and $n \neq 1, 2$ illustrates line 4. Again there is no value of n for which $P(n)$ is true and $Q(n)$ is false.

It is important to realize that in mathematics we use the idea of implication in this particularly precise way (as defined by the truth table) extending everyday usage. Consider the following statements.

- (i) $(\pi < 4) \Rightarrow (1 + 1 = 2)$
- (ii) $(\pi < 4) \Rightarrow (1 + 1 = 3)$
- (iii) $(\pi < 3) \Rightarrow (1 + 1 = 2)$
- (iv) $(\pi < 3) \Rightarrow (1 + 1 = 3)$

From the truth table it is easily seen that the second of these statements is false whereas the other three are true (since $3 < \pi < 4$). However, these statements all seem a little odd from an everyday point of view since the size of the number π really has nothing to do with the effect of adding the number 1 to itself. In everyday speech when we say that P implies Q this suggests that the statement P causes the statement Q to be true. The idea of causation is difficult to make precise and so it is eliminated from the mathematical use of the word ‘implies’. This difference from everyday usage is clarified in mathematical logic where a statement of the form $P \Rightarrow Q$ is referred to as a *conditional statement* rather than an implication. In this book we have adopted the language used by most mathematicians.

Another way of motivating our use of implication is to consider its negative, the statement that P does not imply Q , usually written $P \not\Rightarrow Q$. This will be true precisely when $P \Rightarrow Q$ is false and from the truth table this is when P is true and Q is false. If you think about it these are precisely the circumstances when we would wish to say that P does not imply Q . Notice that this means that the statements ' $P \not\Rightarrow Q$ ' and ' P and (not Q)' are logically equivalent, i.e. have the same meaning (cf. the truth table for ' P and (not Q)' in the solution to Exercise 1.2).

Using the fact that '(not P) or Q ' is the negation of ' P and (not Q)' we can say this in a different way: the statements ' $P \Rightarrow Q$ ' and '(not

P) or Q' are logically equivalent (again see Exercise 1.2). This logical equivalence does arise in everyday speech. For example, when we say ‘Read the lecture notes or you won’t understand the lecture’ this has the same meaning as ‘If you don’t read the lecture notes then you won’t understand the lecture.’ Here P is the statement ‘you don’t read the lecture notes’ and Q is the statement ‘you won’t understand the lecture’.

Universal implications

Strictly speaking the statements ‘ $n > 3 \Rightarrow n > 0$ ’ and ‘ $n = 1 \Rightarrow (n - 1)(n - 2) = 0$ ’ are predicates and give different propositions for each value of n . However, we often use statements of this form in the way we have been doing to mean that the predicate leads to a true proposition whatever value is assigned to the free variable n – this is called a *universal* statement. The possible range of values for the free variables may be explained in the text by a phrase like ‘for integers n ’ or ‘where n is an integer’, or it may be intended to be clear from the context; it is usually good practice to make the range of values explicit.

A statement of this type is false if it is not a universal statement, in other words there is at least one possible value for the variable for which it fails. Consider the statement ‘ $x > 0 \Rightarrow x \geq 1$ ’ for real numbers x . We can construct a truth table as follows.

Table 2.1.2

	$x > 0$	$x \geq 1$	$x > 0 \Rightarrow x \geq 1$
$x \leq 0$	F	F	T
$0 < x < 1$	T	F	F
$x \geq 1$	T	T	T

Here the entries in the last column are determined by the entries in the previous two columns using the truth table for implication, Table 2.1.1. We see from this that there are values of x for which $x > 0$ and $x \not\geq 1$, for example $x = 1/2$, so that $x > 0 \Rightarrow x \geq 1$ is not universally true. This means that, for real numbers x , $x > 0$ does not imply that $x \geq 1$, which may be written

$$x > 0 \not\Rightarrow x \geq 1.$$

This is an *existence* statement: it claims that there is a value of x for which the hypothesis is true and the conclusion false.

There will be a fuller discussion of universal statements and existence statements in Chapter 7.

Notice that in these examples we have adopted the common practice of using letters in the middle of the alphabet (such as n) to denote integers and letters at the end of the alphabet (such as x) to denote real numbers.

If we now reconsider Example 1.2.3 we see that statement (i) there is the universal implication

$$f(a) = 0 \Rightarrow a > 0 \quad (\text{for real numbers } a).$$

The negation of this is the assertion that the implication is false for some real number a , in other words $f(a) = 0$ and $a \not> 0$ for some real number a . This is precisely the statement (viii) which we identified as the negation.

Reading implications

There are many different ways of reading the statement $P \Rightarrow Q$, which may also be written $Q \Leftarrow P$, and some of the most common are listed below.

- (i) If P then Q .
- (ii) P implies Q .
- (iii) Q if P .
- (iv) P only if Q .
- (v) Q whenever P .
- (vi) P is sufficient for Q .
- (vii) Q is necessary for P .

Take care with the third and fourth of these and also with the last two for it is important to appreciate the difference between $P \Rightarrow Q$ and $Q \Rightarrow P$. It is quite possible for one of these to hold without the other. For example, let us return to the examples already considered. We have seen that, for integers n , $n > 3 \Rightarrow n > 0$; but $n > 0 \not\Rightarrow n > 3$ since, for example, when $n = 1$, the hypothesis $n > 0$ is true whereas the conclusion $n > 3$ is false. Similarly, $n = 1 \Rightarrow (n - 1)(n - 2) = 0$ but $(n - 1)(n - 2) = 0 \not\Rightarrow n = 1$ since, when $n = 2$, $(n - 1)(n - 2) = 0$ but $n \neq 1$.

The statement $Q \Rightarrow P$ is called the *converse* of the statement $P \Rightarrow Q$. As an illustration, in Example 1.2.3, statement (v) is the converse of (i) (and in addition (iv) and (vi) are converse to each other).

When both implications do hold we write $P \Leftrightarrow Q$. Thus we define

$$P \Leftrightarrow Q \text{ means } (P \Rightarrow Q) \text{ and } (Q \Rightarrow P).$$

From the truth tables we see that this means that either P and Q are both true or they are both false (see Exercise 2.3).

We read $P \Leftrightarrow Q$ as follows.

- (i) P is equivalent to Q .
- (ii) P is necessary and sufficient for Q .
- (iii) P if and only if Q (sometimes written P iff Q).
- (iv) P precisely when Q .

2.2 Arithmetic

The basic principles of mathematical reasoning apply throughout mathematics but in this book we are going to explore them mainly in the context of number theory or arithmetic since the basic ideas here are familiar from early schooldays. For the moment it is assumed that the reader is familiar with the *integers*, both positive and negative, i.e. the numbers $\dots, -2, -1, 0, 1, 2, 3, \dots$, and their basic arithmetic properties (under addition and multiplication) and order properties. We will also make use of the *rational numbers* (or fractions) and the *real numbers* (or infinite decimals) and these will be discussed in more detail in Chapter 13.

As we do mathematics new vocabulary may be introduced by means of a *definition*. Quite often this gives a precise meaning to an everyday word. Then when we wish to understand the meaning of a statement involving that word it is necessary to invoke the definition. Humpty Dumpty's principle could well stand at the head of any piece of mathematical writing.

'When I use a word,' Humpty Dumpty said, in rather a scornful tone, 'it means what I choose it to mean – neither more nor less.'

Lewis Carroll, *Through the looking glass and what Alice found there*.

This reminds us that when we meet a new word, or a familiar word in a new setting, we need to discover what the writer means by it, not to decide how *we* might have defined it!

Here is a familiar idea to illustrate this.

Odd and even integers

Definition 2.2.1 Given two integers a and b , we say that b divides a or a is a multiple of b to mean that there is an integer q such that $a = bq$.

Thus for example 3 divides 6 since $6 = 3 \times 2$, -14 divides 28 since $28 = (-14) \times (-2)$, and b divides 0 whatever the value of the integer b since $0 = b \times 0$.

Definition 2.2.2 Given an integer a we say that a is even to mean that 2 divides a .

Definition 2.2.3 Given an integer a we say that a is odd to mean that it is not even.

Notice how the third definition makes use of the second and the second definition makes use of the first. It is very common to get chains of definitions; you have to work back through the chain to make use of them.

Now consider the following statement.

Proposition 2.2.4 101 is an odd integer.

Of course, you know that this is true. But what we are interested in here is how we might prove it from the arithmetic and order properties of the integers and our definition of the word ‘odd’. If we cannot prove it from the definition then our definition isn’t much use.

Incidentally, the word ‘Proposition’ used in this way indicates that I am claiming that this result is true. It is really a synonym for ‘Theorem’ but that word is usually restricted to results of greater significance than this one.

Proof From Definition 2.2.3, ‘101 is odd’ means the same as ‘101 is not even’ which from Definition 2.2.2 means that 2 does not divide 101. By Definition 2.2.1, this means that there is no integer q such that $2q = 101$. Now we clearly cannot prove this by exhausting all the possibilities one at a time. However, for an integer q , either $q \leq 50$ or $q \geq 51$. Hence either $2q \leq 100$ or $2q \geq 102$, so that $2q \neq 101$. Hence 101 is not even and so is odd as required. \square

The symbol \square at the end of this proof is there simply to mark the completion of the proof. I recommend that proofs are concluded by stating what has been proved as occurs here.

Notice that the key step in the proof is provided by the two universal implications

$$q \leq 50 \Rightarrow 2q \leq 100 \quad (\text{for integers } q)$$

and

$$q \geq 51 \Rightarrow 2q \geq 102 \quad (\text{for integers } q).$$

This proof might seem over-elaborate, but if you think about it you will see that it is simply spelling out a simple reason why 101 is an odd number. You might like to try to find a better proof based simply on the above definitions.[†]

2.3 Mathematical truth

It is reasonable to ask how we can get started in establishing the truth of mathematical statements if the only method of doing this is to prove them starting from other mathematical statements known to be true.

When the deductive method was first used, for example in the *Elements* of Euclid written about 300 B.C., proofs began from certain ‘axioms’ or ‘postulates’ which were viewed as self-evident truths. For example, Euclid’s Postulate 1 may be reformulated as ‘Given two distinct points, there is a unique straight line passing through them’ which most people would consider to be obvious. This approach sees mathematics as a body of facts about real objects: points, lines, numbers. These facts are determined by using certain accepted self-evident rules of deduction from certain accepted obvious facts, the axioms. There are a number of philosophical difficulties about this point of view. For one thing mathematical objects appear to be ideal abstract representations of objects in the real world: for example you can’t see a point and can only see a blob having some size. For another it has been discovered that different sets of axioms are possible and give rise to different theories which appear to be equally valid mathematically. This was first realized in geometry when in the early nineteenth century ‘non-Euclidean’ geometries were discovered. We can then ask what is the ‘true’ geometry of the universe.

[†] You may feel that the most obvious argument is simply to state that $101/2 = 50\frac{1}{2}$ which is not an integer. This is of course a valid argument but assumes the properties of the rational numbers. For the present purpose of illustrating the use of definitions it is appropriate to seek an argument based simply on the integers.

This is not a mathematical question but is one for physicists and astronomers. However, the awareness that there is more than one possible geometry was enormously liberating and has given rise to much interesting mathematics as well as physics. Without it the geometry which provides the language used in general relativity theory would not have been discovered.

Most mathematicians do appear to take the view that mathematics deals with real objects. However, in the modern axiomatic approach axioms are seen not necessarily as ‘self-evident truths’ but simply as statements which we are assuming to be true. We do mathematics by exploring what follows from the truth of these axioms using certain accepted rules of deduction. When we come to apply the mathematics we must confirm that these axioms are ‘true’ in an appropriate sense in the area of application or acknowledge that this is an assumption that we are making. The reader will meet good examples of this axiomatic method in the study of algebra.

Since this book is primarily concerned with introducing the reader to mathematical reasoning and exposition it seems best to keep the mathematical context very familiar and so we will mainly restrict ourselves to arithmetic. Most mathematicians probably would consider the basic properties of numbers to be ‘self-evident truths’. It would be cumbersome to develop these properties formally from a list of axioms although this can be done.†. We will simply assume that the reader is familiar with the basic algebraic properties of numbers (dealing with addition, subtraction, multiplication and division) and take these for granted. These can be summarized as follows.

Properties 2.3.1 *Given two real numbers a and b they have a sum $a + b$ and a product ab (sometimes denoted by $a \cdot b$ or $a \times b$) which are also real numbers. The operations of sum (or addition) and product (or multiplication) of real numbers have the following properties.*

- (i) Commutativity. $a + b = b + a$ and $ab = ba$. (This means that the

† Formally the real numbers and the rational numbers have the algebraic structure of a *field* and the integers have the algebraic structure of an *integral domain*. In a precise sense the integers are characterized by the statement that they form an ordered integral domain in which the positive elements satisfy the induction property (see Axiom 5.1.1). For details of such an axiomatic approach see for example G. Birkhoff and S. Mac Lane *A survey of modern algebra*, Macmillan, Fourth edition 1977. The positive integers can be characterized by a particularly simple set of axioms, Peano’s axioms, and these will be described in Chapter 9 (see Axioms 9.4.2).

order in which we write numbers to be added or multiplied doesn't matter.)

- (ii) **Associativity.** $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$. (*This means that we can write $a+b+c$ and abc without brackets without ambiguity.*)
- (iii) **Distributivity.** $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. (*This tells us how to remove brackets.*)
- (iv) **Zero.** $a + 0 = a = 0 + a$.
- (v) **Unity.** $a \times 1 = a = 1 \times a$.
- (vi) **Subtraction.** *The equation $a + x = 0$ has the unique solution $x = -a$ and so $a + x = b \Leftrightarrow x = b + (-a) = b - a$. (This means that we can cancel: $a + x_1 = a + x_2 \Rightarrow x_1 = x_2$.)*
- (vii) **Division.** *If $a \neq 0$, then equation $ax = b$ has the unique solution $x = b/a = ba^{-1}$. (This means that we can cancel: $ax_1 = ax_2 \Rightarrow x_1 = x_2$ so long as $a \neq 0$.)*

All the usual algebraic properties of numbers can be deduced from the above statements. In particular it follows that $a \times 0 = 0 = 0 \times a$ and we can also deduce the rule of signs $(-a)b = -(ab) = a(-b)$ and $(-a)(-b) = ab$ (see Problems I, Question 6).

If a and b are rational numbers (fractions) then so are $a + b$, ab , $b - a$ and (for $a \neq 0$) b/a . The distinction between rational numbers and real numbers will be considered in Chapter 13. If a and b are integers then so are $a + b$, ab and $b - a$, but b/a is an integer only if a divides b . Most of this book will be concerned with the integers.

We will also make use of the order properties of the real numbers (and have already made use of these in the proof of Proposition 2.2.4); these may be less familiar and so a formal set of axioms about order (inequalities) will be given and discussed in the next chapter.

Exercises

2.1 Which of the following universal statements are true and which are false for integers n ?

- (i) $n = 2$ only if $n^2 - n - 2 = 0$.
- (ii) $n = 2$ if $n^2 - n - 2 = 0$.
- (iii) $n = 2$ is sufficient for $n^2 - n - 2 = 0$.
- (iv) $n = 2$ is necessary for $n^2 - n - 2 = 0$.
- (v) $n^2 - n - 2 = 0 \Rightarrow (n = 2 \text{ and } n = -1)$.
- (vi) $n^2 - n - 2 = 0 \Rightarrow (n = 2 \text{ or } n = -1)$.

- (vii) $n^2 - n - 2 = 0 \Leftrightarrow (n = 2 \text{ or } n = -1)$.
- (viii) $n^2 - n - 2 = 0 \Leftrightarrow (n = 2 \text{ and } n = -1)$.
- (ix) $(n^2 - n - 2 = 0 \Rightarrow n = 2) \text{ or } (n^2 - n - 2 = 0 \Rightarrow n = -1)$.
- (x) $(n^2 - n - 2 = 0 \Leftarrow n = 2) \text{ or } (n^2 - n - 2 = 0 \Leftarrow n = -1)$.
- (xi) $(n^2 - n - 2 = 0 \Leftarrow n = 2) \text{ and } (n^2 - n - 2 = 0 \Leftarrow n = -1)$.

2.2 By constructing a truth table exhausting the possibilities of n and using the truth table for ‘implies’, prove that $n > 0 \Rightarrow n \geq 1$ for integers n .

2.3 Complete the following truth table for $P \Leftrightarrow Q$ using the tables for ‘ \Rightarrow ’ and ‘and’.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T			
T	F			
F	T			
F	F			

2.4 By using truth tables prove that, for all statements P and Q , the following statements are true.

- (i) $P \Rightarrow (P \text{ or } Q)$.
- (ii) $(P \text{ and } Q) \Rightarrow P$.

2.5 By using truth tables prove that, for all statements P and Q ,

- (i) the statements ‘ $P \Rightarrow Q$ ’ and ‘(not Q) \Rightarrow (not P)’ are equivalent,
- (ii) the statements ‘ P or Q ’ and ‘(not P) \Rightarrow Q ’ are equivalent.

2.6 Use the method of proof of Proposition 2.2.4 to prove that 7 does not divide 100.

3

Proofs

A proof of a mathematical statement is a logical argument which establishes the truth of the statement. The steps of the logical argument are provided by implications. One of the main aims of this book is to describe a variety of methods of proof so that you can follow these when you meet them and also construct proofs for yourself.

No doubt anyone reading this book will have been seeing and understanding proofs for years. At university you are expected to be able to construct your own proofs and, as importantly, to write them out carefully so that other people can understand them – or even so that you can understand them yourself when you come to look back at your work some months later. One real difficulty is that we do not normally discover proofs in the polished form in which they are presented. It is important to realize that you will usually spend time constructing a proof before you then write out a formal proof. You can think of this as erecting a sort of scaffolding for the purpose of constructing the proof. When the proof has been constructed the scaffolding is removed so that the proof can be admired in all its economical beautiful simplicity! However, one difficulty for the person encountering the proof for the first time is that it can be hard to make sense of. To read and understand the proof we may have to reconstruct the scaffolding for ourselves from the formal proof. This can be difficult – but not usually as difficult as thinking of the proof in the first place unless the proof is very badly written. This is a problem not just for beginning undergraduates but also for professional mathematicians when they read mathematics.

You may ask why then the scaffolding is not retained. The difficulty is that if every detail is given then mathematical arguments become enormously long and cluttered. The aim is to pitch your writing at the level of the expected reader so that there is just enough information

to enable the reconstruction of the scaffolding if necessary but not so much that it would mask the essence of the argument. Too much detail can make a proof based possibly on one simple idea appear enormously complicated. To avoid detail it is quite common to use statements like ‘it is easy to show that [some statement] is true’ or ‘it now readily follows that [some statement] is true’ and then the reader has to confirm that this is indeed the case. It is, however, important not to use such phrases as a lazy way of avoiding thinking about the details.

It is also the case that excessive pedantic precision can sometimes make mathematics hard to read. Writing mathematics is not like writing a computer program; what is written will be read by a human being who has much common experience with the writer and so is able to anticipate to some extent what the writer intends. As Gila Hanna has written,

The student of mathematics has to develop a tolerance for ambiguity. Pedantry can be the enemy of insight.†

Putting this into practice is a matter of fine judgement: ambiguous statements are only acceptable in contexts which resolve the ambiguity almost immediately. While learning to write good mathematics it is probably better to err on the side of pedantry.

In this book arguments will often be presented first with lots of scaffolding (as ‘constructing a proof’) and then with the scaffolding removed (as ‘(formal) proofs’). You should ensure that in each case you do understand why the ‘proof’ does prove the result as claimed. When you read most mathematics books you need to work with pencil in hand reconstructing the detail behind the proofs provided. You cannot normally read a mathematics book like a conventional novel.

3.1 Direct proofs

Let us begin by thinking about one of the simplest forms of mathematical result. Very many theorems are of the form $P \Rightarrow Q$. How do we set about proving such a statement? Since the statement is necessarily true if P is false (remember Table 2.1.1) we only need consider the case when P is true. Then from the truth table we see that $P \Rightarrow Q$ is true so long as Q is also true.

So to prove that $P \Rightarrow Q$ is true, it is sufficient to assume that P is true and deduce Q . This is the direct form of proof. Here is an example.

† In David Tall (editor), *Advanced mathematical thinking*, Kluwer, 1991.

Proposition 3.1.1 For positive real numbers a and b , $a < b \Rightarrow a^2 < b^2$.

Constructing a proof. We can summarize what is needed in the following way using a given-goal diagram.†

Given	Goal
a, b positive real numbers	$a < b \Rightarrow a^2 < b^2$

The direct method of proof of an implication is to add the hypothesis to the given statements and to set a new goal of proving the conclusion. This leads to the following new given-goal diagram.

Given	Goal
a, b positive real numbers $a < b$	$a^2 < b^2$

We now start to think how we can obtain something like the goal from the given statements. We see that we want a^2 and b^2 in the goal and this suggests multiplying the given inequality through by a and by b . Thus

$$a < b \Rightarrow a^2 < ab \tag{3.1}$$

and

$$a < b \Rightarrow ab < b^2 \tag{3.2}$$

using the fact that a and b are both positive. Hence, if we suppose that $a < b$, it follows that $a^2 < ab$ and $ab < b^2$. But now we recognize that the two inequalities we have obtained both involve ab and that

$$[(a^2 < ab) \text{ and } (ab < b^2)] \Rightarrow a^2 < b^2 \tag{3.3}$$

so that if $a < b$ then $a^2 < b^2$ as required.

The reader might well ask where the three numbered implications have come from; why are these true? The answer is that these statements follow immediately from fundamental properties of the real numbers which can be encapsulated in the inequality (or order) axioms. We have already commented that it would be unwieldy to work from a complete axiom system in this book and readers are unlikely to have difficulties

† The idea of using these ‘given–goal diagrams’ comes from the book by Daniel J. Velleman, *How to prove it, a structured approach*, Cambridge University Press, 1994. It extends usefully the approach taught to the author at school of starting by stating clearly what we are ‘required to prove’ or ‘required to find’. Velleman provides many illustrative examples of different methods of proof some of which are also used in this book.

with the algebraic properties assumed. However, inequalities are less familiar and so it seems useful to list the basic properties to be assumed.

Axioms 3.1.2

- (i) Trichotomy law. *For each pair of real numbers a and b , one and only one of the three possibilities $a < b$, $a = b$, $a > b$ is true.*
- (ii) Addition law. *For real numbers a , b and c ,*

$$a < b \Leftrightarrow a + c < b + c.$$

- (iii) Multiplication law. *For real numbers a , b and c ,*

$$\begin{aligned} a < b &\Leftrightarrow ac < bc && \text{if } c > 0, \\ a < b &\Leftrightarrow ac > bc && \text{if } c < 0. \end{aligned}$$

- (iv) Transitive law. *For real numbers a , b and c ,*

$$a < b \text{ and } b < c \Rightarrow a < c.$$

Now statements (3.1) and (3.2) follow from the multiplication law and statement (3.3) from the transitive law.

We can now write out a formal proof of Proposition 3.1.1 as follows.

Proof Given positive real numbers a and b suppose that $a < b$. Then $a^2 < ab$ (multiplying through by $a > 0$) and $ab < b^2$ (multiplying through by $b > 0$). Hence $a^2 < b^2$. It follows that $a < b \Rightarrow a^2 < b^2$. \square

Notice that this proof is written as a sequence of sentences with words like ‘then’, ‘hence’ and ‘it follows’ indicating how the sentences are related. Of course some symbols are used but it is a good practice when writing mathematics to read it out aloud to check that when the symbols are converted into words (‘ a is less than b ’ in the first sentence of the above proof for example) what you have written is a sensible piece of prose. We do sometimes use more symbols so that the above proof might have been written out as follows.

Proof For positive integers a and b , $a < b \Rightarrow (a^2 < ab \text{ and } ab < b^2) \Rightarrow a^2 < b^2$. Hence $a < b \Rightarrow a^2 < b^2$. \square

This presentation highlights the fact that in constructing a proof as a chain of implications we repeatedly use

$$[(P \Rightarrow Q) \text{ and } (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$$

which is readily checked by using a truth table.[†]

However, I would encourage the reader to beware of using too many symbols in writing out proofs at this stage as it makes it much harder to be clear that what you are writing is conveying what you intend.

Notice how the ‘and’ statement was handled in this proof. An implication of the form ‘ $P \Rightarrow (Q \text{ and } R)$ ’ is logically equivalent to ‘ $(P \Rightarrow Q) \text{ and } (P \Rightarrow R)$ ’. Thus ‘ $a < b \Rightarrow (a^2 < ab \text{ and } ab < b^2)$ ’ is proved by proving (3.1) and (3.2).

One problem in writing out proofs is to decide how much detail to give and what can be assumed. There is no simple answer to this. Although the above proof did start from the inequality axioms this was not explicitly referred to in the formal proof. You always do have to start somewhere. But it is cumbersome to reduce everything to a set of axioms and there is usually a wide body of results which it is reasonable to assume. For example the result of Proposition 2.2.4 that 101 is an odd number is something which normally would simply be taken for granted. It was explored in Chapter 2 simply to illustrate the role of definitions. One very useful piece of advice is always to be sceptical, for if your proof doesn’t convince you, then it is unlikely to convince anyone else. Notice that the above proof did refer to the facts that $a > 0$ and $b > 0$ at the points where they were needed (in applying the multiplication law of inequalities). It is good style to indicate where the hypotheses in the result being proved are used in the proof. Also if some steps in the argument are only valid under certain conditions then you should verify that these conditions are indeed satisfied.

Proof by cases

When proving universal implications it is often very difficult to consider together all the objects satisfying the hypothesis. Here is a very simple example.

Example 3.1.3 *If $a = 1$ or $a = 2$ then $a^2 - 3a + 2 = 0$.*

Proof If $a = 1$ then $a^2 - 3a + 2 = 1 - 3 + 2 = 0$. If $a = 2$ then $a^2 - 3a + 2 = 4 - 6 + 2 = 0$. Hence, if $a = 1$ or $a = 2$ then $a^2 - 3a + 2 = 0$. \square

Notice how the ‘or’ statement was handled in constructing this simple proof. An implication of the form ‘ $(P \text{ or } Q) \Rightarrow R$ ’ is logically equivalent

[†] This step is known in formal logic as a ‘syllogism’: P is the ‘minor term’, Q the ‘middle term’ and R the ‘major term’; $P \Rightarrow Q$ is the ‘minor premise’ and $Q \Rightarrow R$ the ‘major premise’.

to the statement ' $(P \Rightarrow R)$ and $(Q \Rightarrow R)$ ' (this is common usage but can be checked by a truth table argument) and so is proved by proving the two implications in this 'and' statement.

In this example the 'cases' were simply the two numbers satisfying the hypothesis. It can be viewed as 'proof by enumeration' working through the possibilities one by one. This is not always possible. Recall the proof of Proposition 2.2.4 on page 16. The aim was to prove the universal implication 'if q is an integer then $2q \neq 101$ '. It is impossible to work through the integers one by one. The proof was achieved by considering two cases: integers q such that $q \leq 50$ and integers q such that $q \geq 51$. This argument works because these two cases are *exhaustive*: for every integer q either $q \leq 50$ or $q \geq 51$.

Here is another example deriving a familiar property of the integers from the inequality axioms.

Proposition 3.1.4 *For non-zero real numbers a , $a^2 > 0$.*

Constructing a proof. Summarizing what is needed gives the following.

Given	Goal
a a real number	
$a \neq 0$	$a^2 > 0$

The trichotomy law is the only inequality axiom which refers to the equality of real numbers. If we apply this to the real numbers a and 0 it can be rewritten

$$a \neq 0 \Rightarrow a > 0 \text{ or } a < 0. \quad (3.4)$$

However, from the multiplication law,

$$a > 0 \Rightarrow a^2 > 0 \quad (3.5)$$

and

$$a < 0 \Rightarrow a^2 > 0. \quad (3.6)$$

Hence

$$a > 0 \text{ or } a < 0 \Rightarrow a^2 > 0. \quad (3.7)$$

Finally, putting together statements (3.4) and (3.7) we obtain

$$a \neq 0 \Rightarrow a^2 > 0$$

as required.

We can now write out the formal proof as follows.

Proof Suppose that a is a non-zero real number. Then (by the trichotomy law) either $a > 0$ or $a < 0$. In either case, from the multiplication law, $a^2 > 0$. Hence, if $a \neq 0$ then $a^2 > 0$ as required. \square

Again notice how the ‘or’ statement was handled in constructing this proof. To prove statement (3.7) we must prove both statement (3.5) and statement (3.6).†

3.2 Constructing proofs backwards

The grand thing is to be able to reason backwards.

Arthur Conan Doyle, *A study in scarlet*.

The process of mathematical investigation is extremely complex. Even when you know what you are trying to prove it is quite unusual in practice to be able construct proofs in the direct way which has been illustrated so far. One analogy which may be helpful is that of creating or discovering a route up a mountain. You may succeed by simply heading off towards the top. But often there will be a number of false starts and it may be helpful to stand back and take an overview of what is possible. You may find that for certain routes your technique is inadequate and you need to refine this on less ambitious projects. One possible approach is to develop your route by mentally working back from the summit, in other words by planning the route backwards. This is frequently a sensible approach to constructing mathematical proofs.

It may be worth remarking that this analogy seems useful when we ponder the nature of mathematical invention: is mathematics discovered or created? A new route up a mountain is both discovered and created; it is to some extent rediscovered and recreated every time someone subsequently uses it – it may even be slightly different each time. But the route appears to have an objective existence independent of those who use it. The same is true of mathematical ideas.

Here is an example requiring a little more thought than the results considered so far.

Proposition 3.2.1 *For real numbers a and b , $a < b \Rightarrow 4ab < (a + b)^2$.*

† It is necessary to be careful about the way the words ‘and’ and ‘or’ are used in normal speech. For example statement (3.7) might be formulated using the word ‘and’ as ‘ $a > 0$ and $a < 0$ (both) imply that $a^2 > 0$ ’. This is really a shorthand for ‘ $a > 0$ implies that $a^2 > 0$ and $a < 0$ implies that $a^2 > 0$ ’.

Constructing a proof. We can summarize what is needed for a direct proof as follows.

Given	Goal
a, b real numbers $a < b$	$4ab < (a + b)^2$

It is difficult to see how to proceed. One difficulty is that the goal is more complicated than the given statement and it is not immediately clear how to reach this more complicated statement. In such a situation it is often best to start with the more complicated statement and to simplify it. In this case simplifying the goal leads to the construction of a proof backwards.

$$\begin{aligned}
 4ab < (a + b)^2 &\Leftarrow 4ab < a^2 + 2ab + b^2 \\
 &\Leftarrow 0 < a^2 - 2ab + b^2 \\
 &\Leftarrow 0 < (a - b)^2 \\
 &\Leftarrow a - b \neq 0 \text{ by Proposition 3.1.4} \\
 &\Leftarrow a \neq b \\
 &\Leftarrow a < b.
 \end{aligned}$$

Hence $a < b \Rightarrow 4ab < (a + b)^2$.

It is essential for the proof that these implications go in the direction shown. Of course, apart from the last step, in this case they do in fact go in both directions, and it would be usual to write ' \Leftrightarrow ' instead of ' \Leftarrow ' in those cases. But the fact that the implications ' \Rightarrow ' are true is quite irrelevant for the proof. The above sequence of implications is perfectly satisfactory as a formal proof for it makes it clear that the truth of the goal is *implied* by what is given. If preferred the proof can be presented as a direct proof as follows.

Proof $a < b \Rightarrow a \neq b \Rightarrow a - b \neq 0 \Rightarrow 0 < (a - b)^2 \Rightarrow 0 < a^2 - 2ab + b^2 \Rightarrow 4ab < a^2 + 2ab + b^2 \Rightarrow 4ab < (a + b)^2$. Hence $a < b \Rightarrow 4ab < (a + b)^2$.

□

However, presenting the proof in this way disguises where it has come from. Whilst readers of the proof may accept each of the steps and so be forced to accept the proof they would probably find the earlier backwards presentation more satisfying because it demonstrates how the proof was found.

Exercises

3.1 Prove that for all real numbers a , b and c ,

- (i) $(a + b - c)^2 = (a + b)^2 + (a - c)^2 + (b - c)^2 - a^2 - b^2 - c^2$,
- (ii) $bc + ac + ab \leq a^2 + b^2 + c^2$.

3.2 Prove that for all integers a , b and c ,

$$(a \text{ divides } b) \text{ and } (b \text{ divides } c) \Rightarrow a \text{ divides } c.$$

3.3 Prove that the square of an even integer is even.

3.4 Prove that 0 divides an integer a if and only if $a = 0$.

3.5 Prove, from the inequality axioms, that if a , b and c are real numbers with $a > 0$, then $b \geq c \Rightarrow ab \geq ac$.

3.6 Prove that for negative real numbers a and b , $a < b \Rightarrow a^2 > b^2$.

3.7 Proposition 3.2.1 states that $a < b$ is a sufficient condition for $4ab < (a + b)^2$. Is this condition also necessary? If so, prove it. If not, find a necessary and sufficient condition.

3.8 Prove that for all real numbers a and b ,

- (i) $0 \leq a < b \Rightarrow a^2 < b^2$,
- (ii) $|a| < |b| \Rightarrow a^2 < b^2$,
- (iii) $|a| = |b| \Rightarrow a^2 = b^2$,
- (iv) $|a| \leq |b| \Rightarrow a^2 \leq b^2$.

4

Proof by contradiction

In the previous chapter we considered how to construct some simple direct proofs. However, the direct method can be inconvenient and does not always work. In this chapter we consider a logically more elaborate but very common and powerful method of proof: proof by contradiction.

4.1 Proving negative statements by contradiction

The direct method of proof is often hard to use when we are proving negative statements. Consider the following example.

Proposition 4.1.1 *There do not exist integers m and n such that*

$$14m + 20n = 101.$$

This is a simple example of a *non-existence result* and results of this type are very common in more advanced mathematics.

It is difficult to see how to prove Proposition 4.1.1 directly for we clearly cannot consider all the possibilities for m and n one at a time. The method of proof by contradiction is to demonstrate that if what we are trying to prove were false then this would lead to a statement which is known not to be true, a contradiction. A *contradiction* is a statement of the form ' P and (not P)'. For example, if a is an integer, the statement ' a is even and a is odd' is a contradiction since 'odd' is defined to mean 'not even'. Having obtained a contradiction we know that our initial assumption must have been wrong and so the result we are trying to prove must be true.

This may sound confusing and so before we consider in general how this method can be justified let us illustrate it by considering the proof of Proposition 4.1.1.

Constructing a proof. The proposition states that whatever integers m and n we choose these will not satisfy the equation, i.e. $14m + 20n \neq 101$. We can sum this up as follows.

Given	Goal
m, n integers	$14m + 20n \neq 101$

A proof by contradiction is given by showing that if the goal were false then this would lead to something which we know not to be true, a contradiction. Then since this shows that the negative of the goal is impossible it means that the goal must be true in accordance with the following precept of Sherlock Holmes'.

When you have eliminated the impossible, whatever remains, *however improbable*, must be the truth.

Arthur Conan Doyle, *The sign of four*.

The method is carried out by adding the negative of the goal to the givens and making the finding of a contradiction the new goal. In this case this gives the following strategy.

Given	Goal
m, n integers $14m + 20n = 101$	contradiction

Here we can get a contradiction by using the idea of even and odd numbers. Notice that both $14 = 2 \times 7$ and $20 = 2 \times 10$ are even numbers and so any number of the form $14m + 20n$, where m and n are integers, is also even since $14m + 20n = 2(7m + 10n)$. Thus if $14m + 20n = 101$ this means that 101 is an even number. But 101 is an odd number (see Proposition 2.2.4 for a formal proof but we would usually assert this without proof) and so we have two contradictory statements about 101 giving a contradiction as required.

The proof is quite short when written out in final form. Notice that we include the phrase ‘for contradiction’ in the first sentence in order to indicate the method we are using.

Proof Suppose for contradiction that m and n are integers such that $14m + 20n = 101$. Then, since 14 is even and 20 is even, $101 = 14m + 20n = 2(7m + 10n)$ is even. But this is not true since 101 is odd. Hence such integers m and n cannot exist, as required. □

We can justify this method using a truth table. Suppose that we are trying to prove statement P . The method of contradiction is to prove

the statement $(\text{not } P) \Rightarrow Q$ where Q is a false statement. Now look at the following truth table.

P	$\text{not } P$	Q	$(\text{not } P) \Rightarrow Q$
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	F

If we know that $(\text{not } P) \Rightarrow Q$ is true and Q is false, then the only possibility in the above table is the second line. But this shows that P is true.

A template for proofs by contradiction

It may be useful to present a template for writing out these proofs. Suppose that we are writing out a formal proof of the statement P using the contradiction method. We would set out the proof as follows.

Proof Suppose, for contradiction, that the statement P is false.
 Then [present some argument which leads to a contradiction of some sort].
 Hence our assumption that P is false must be false.
 Thus P is true as required. □

A common failing in writing out proofs by contradiction is for it to be unclear precisely what the contradiction is. Take care to make this clear.

As a second example here is an alternative proof of Proposition 2.2.4 using this method.

Proposition 2.2.4 101 is an odd integer.

Constructing a proof. This appears to be a positive statement but since the word ‘odd’ means ‘not even’ it too is a non-existence result since it asserts that 101 is not a multiple of 2. We can describe this as follows.

Given	Goal
q an integer	$2q \neq 101$

In Chapter 2 the goal was achieved by considering all the possibilities for q . Although it is not possible to consider these one at a time we could take account of all the possibilities by observing that for any integer q either $q \leq 50$ or $q \geq 51$. It was observed in Chapter 3 that this is an example of a proof by cases.

As an alternative we can apply the method of proof by contradiction which leads to the following strategy.

Given	Goal
q an integer	
$2q = 101$	contradiction

We get a contradiction if we remember how we did division in our early school-days. Then we would have divided 2 into 101 giving 50 with remainder 1. This suggests

$$101 = 2q \Rightarrow 1 = 101 - 100 = 2q - 2 \times 50 = 2(q - 50) \geq 2 \Rightarrow 1 \geq 2$$

and we have a contradiction since it is certainly true that $1 < 2$.

Proof Suppose for contradiction that 101 is even so that $101 = 2q$ for some integer q . Then $1 = 2(q - 50)$ where $q - 50$ must be a positive integer. But $2(q - 50) \geq 2$ so that $1 \geq 2$ contradicting the fact that $1 < 2$. Hence 101 is not even and so must be odd. \square

4.2 Proving implications by contradiction

We sometimes find that the direct method of proof of statements of the form $P \Rightarrow Q$ does not work. Consider the following result.

Proposition 4.2.1 *If a, b, c are integers such that $a > b$, then*

$$ac \leq bc \Rightarrow c \leq 0.$$

Constructing a proof. It is difficult to know how to make use of the multiplicative law of inequalities (see Axioms 3.1.2) in a direct proof since this depends on the sign of c which is what we are trying to determine.

The easiest thing to do in this case is again a proof by contradiction. Notice from the truth table for ‘implies’ (Table 2.1.1) that if $P \Rightarrow Q$ is false then we must have P true and Q false. So we can prove that $P \Rightarrow Q$ is true by showing that P true and Q false together imply a contradiction.

What we are asked for in Proposition 4.2.1 may be summarized as follows.

Given	Goal
$a, b, c \text{ integers}$ $a > b$	$ac \leq bc \Rightarrow c \leq 0$

An attempt at a direct proof of the proposition leads to the following strategy.

Given	Goal
$a, b, c \text{ integers}$ $a > b$ $ac \leq bc$	$c \leq 0$

The method of proof by contradiction is to add the negative of the desired conclusion to the ‘givens’ and to seek a contradiction. This gives the following strategy.

Given	Goal
$a, b, c \text{ integers}$ $a > b$ $ac \leq bc$ $c > 0$	contradiction

It is easy to obtain a contradiction. For by the multiplicative law of inequalities (Axioms 3.1.2)

$$a > b \text{ and } c > 0 \Rightarrow ac > bc.$$

Hence, since our given statements include the statement $ac \leq bc$, they imply that $ac > bc$ and $ac \leq bc$ which is a contradiction.

The proof is quite short when written out in final form as follows.

Proof For integers a, b and c , with $a > b$, suppose that $ac \leq bc$ but, for contradiction, that $c > 0$. Then the given statement $a > b$ implies that $ac > bc$, contradicting the statement that $ac \leq bc$. Hence our assumption that $c > 0$ must be false, i.e. $c \leq 0$. Thus $ac \leq bc \Rightarrow c \leq 0$.

□

4.3 Proof by contrapositive

In the proof of Proposition 4.2.1 the contradiction we obtained involved the hypothesis in the proposition. This is a particular form of proof by

contradiction. It essentially uses the fact that, given any statements P and Q , the statements ' $P \Rightarrow Q$ ' and its *contrapositive* '(not Q) \Rightarrow (not P)' are equivalent, as can be seen by examining their truth tables (see Exercise 2.5). Thus if one is true then so is the other. Now Proposition 4.2.1 is a statement about integers a , b and c such that $a > b$, of the form $P \Rightarrow Q$ where

P is the statement $ac \leq bc$,
 Q is the statement $c \leq 0$.

To write down the contrapositive notice that

(not P) is the statement $ac > bc$,
(not Q) is the statement $c > 0$,

and so the statement (not Q) \Rightarrow (not P) reads

$$c > 0 \Rightarrow ac > bc,$$

where a , b and c are integers such that $a > b$. But this is just the multiplicative law of inequalities included in Axioms 3.1.2. Hence we could have proved Proposition 4.2.1 by simply observing that its contrapositive is true. We would write out this proof as follows.

Proof of Proposition 4.2.1 The contrapositive of the statement

$$ac \leq bc \Rightarrow c \leq 0$$

is the statement

$$c > 0 \Rightarrow ac > bc$$

which is just the multiplicative law of inequalities since we are given that $a > b$. Thus the proposition is true. \square

4.4 Proving ‘or’ statements

Constructing a proof for composite statements involving ‘or’ usually makes use of a logical construction rather similar to proof by contradiction which it is convenient to consider at this point. Again let us consider an example.

Proposition 4.4.1 *If a and b are real numbers, then*

$$ab = 0 \Leftrightarrow a = 0 \text{ or } b = 0.$$

Constructing a proof. Recall from Chapter 2 that the statement ' $P \Leftrightarrow Q$ ' means ' $(P \Rightarrow Q)$ and $(Q \Rightarrow P)$ '. So there are two parts to the proof: a proof of the ' \Leftarrow ' statement and a proof of the ' \Rightarrow ' statement. We consider these in turn.

' \Leftarrow ': This statement is a restatement of a basic property of the number 0, that $0 \times b = 0 = a \times 0$ for real numbers a and b . This property was mentioned in the discussion at the end of Chapter 2.[†]

' \Rightarrow ': Adopting the direct strategy for proving the converse statement gives the following strategy.

Given	Goal
a, b real numbers $ab = 0$	$a = 0$ or $b = 0$

Now recall that ' P or Q ' is logically equivalent to '(not P) \Rightarrow Q ' (see Exercise 2.5) so that the goal may be rewritten ' $a \neq 0 \Rightarrow b = 0$ '. Adopting the direct strategy for proving this gives the following.

Given	Goal
a, b real numbers $ab = 0$ $a \neq 0$	$b = 0$

Since $a \neq 0$, we can divide through by a (or multiply through by $1/a$) so that $ab = 0 \Rightarrow b = 0$ as required.

A formal proof could be set out as follows.

Proof It is a basic property of 0 that $0 \times b = 0 = a \times 0$. Therefore $a = 0$ or $b = 0 \Rightarrow ab = 0$.

For the converse, suppose that a and b are real numbers such that $ab = 0$. To see that it follows that $a = 0$ or $b = 0$ suppose that $a \neq 0$. Then dividing $ab = 0$ through by a gives $b = 0$, as required. Hence $ab = 0 \Rightarrow a = 0$ or $b = 0$. \square

An alternative method of obtaining this result is by proof by cases. The trichotomy law of inequalities tells us that, for any real number a , $a < 0$ or $a = 0$ or $a > 0$. This gives three possibilities for a and similarly there are three possibilities for b , leading to nine possibilities

[†] Problems I, Question 6 asks for a formal proof of this result from Properties 2.3.1.

in all. These can be summarized in a table as follows.

	$a < 0$	$a = 0$	$a > 0$
$b < 0$	$ab > 0$	$ab = 0$	$ab < 0$
$b = 0$	$ab = 0$	$ab = 0$	$ab = 0$
$b > 0$	$ab < 0$	$ab = 0$	$ab > 0$

This comes from the multiplicative law of inequalities and the fact that $ab = 0$ if $a = 0$ or $b = 0$.

Now since all possibilities are included in this table we can read off Proposition 4.4.1 and also the following useful results.

Proposition 4.4.2 *If a and b are real numbers, then $ab > 0$ if and only if a and b have the same sign, i.e. ($a > 0$ and $b > 0$) or ($a < 0$ and $b < 0$).*

Proposition 4.4.3 *If a and b are real numbers, then $ab < 0$ if and only if a and b have opposite signs, i.e. ($a > 0$ and $b < 0$) or ($a < 0$ and $b > 0$).*

Formally the right to left implications in these results come from the multiplicative law of inequalities and the left to right implications are proved by contradiction using the above table which shows, for example, that if a and b do not have the same sign then ab is not positive.

Proposition 4.4.1 is used when we solve polynomial equations and in the same way we use the other two results to solve polynomial inequalities (see Exercise 6.2).

Exercises

4.1 Prove by contradiction that there do not exist integers m and n such that $14m + 21n = 100$.

4.2 Prove by contradiction that for any integer n

$$n^2 \text{ is odd} \Rightarrow n \text{ is odd.}$$

4.3 Prove the result of the previous exercise by writing down its contrapositive.

4.4 Prove, using the method given above for proving an ‘or’ statement, that if a is a real number such that $a^2 \geqslant 7a$ then $a \leqslant 0$ or $a \geqslant 7$.

4.5 Prove by contradiction from the trichotomy law that, for any real numbers a and b ,

$$a \leq b \text{ and } b \leq a \Rightarrow a = b.$$

4.6 Write down the contrapositive of the statement of Exercise 3.8(iv). Hence prove that, for all real numbers a and b ,

- (i) $|a| < |b|$ if and only if $a^2 < b^2$,
- (ii) $|a| = |b|$ if and only if $a^2 = b^2$.

4.7 Prove that, for all real numbers a and b ,

$$|a + b| \leq |a| + |b|.$$

Give a necessary and sufficient condition for equality.

5

The induction principle

The essence of the natural number concept is ... closure under the successor operation.[†]

Richard Dedekind (1888)

In this chapter we discuss a special proof technique which is particularly useful when proving statements about the positive integers.

5.1 Proof by induction

Suppose that we wish to prove that some property holds for all the positive integers $1, 2, 3, 4, \dots$. It is often difficult, or even impossible, to prove such statements simply from basic rules of arithmetic. What these rules fail to capture is the fact that the positive integers come in a sequence with any number obtainable by starting from the number 1 and adding 1 to it enough times. The integer $n + 1$ is called the *successor* of the integer n . Thus, if we start with the integer 1 and form its successor, and then its successor, and so on, then given any positive integer eventually it will be reached. This idea can be formulated more precisely as follows.

Axiom 5.1.1 (The induction principle) *Suppose, that $P(n)$ is a statement involving a general positive integer n . Then $P(n)$ is true for all positive integers $1, 2, 3, \dots$ if*

- (i) *$P(1)$ is true, and*
- (ii) *$P(k) \Rightarrow P(k + 1)$ for all positive integers k .*

Before discussing the induction principle further, here is an example of how it is used.

[†] The significance of this quotation will be discussed further in Section 9.4.

Proposition 5.1.2 *For all positive integers n we have the inequality $n \leq 2^n$.*

Constructing a proof. When using the induction principle it is important to be clear about what constitutes the predicate $P(n)$. In this case $P(n)$ is the statement

$$n \leq 2^n.$$

Let us begin by comparing the two numbers n and 2^n in some particular cases.

n	1	2	3	4	5	6
2^n	2	4	8	16	32	64

From this we can see that the result certainly holds for $n = 1, 2, 3, 4, 5$ and 6 and it seems highly plausible that the result will hold for all positive integers n . However, testing any number of cases does not constitute a proof that the result will always hold. In this example the above table suggests more than just that the result holds for certain particular values of n . It demonstrates that the numbers in the second row are growing much more rapidly than the numbers in the first row and if this continues then it would be a strong indication that the result $P(n)$ holds for all positive integers n . The proof of the result by induction makes this argument precise.

Referring to Axiom 5.1.1, we see that it asserts that two statements will lead to the proposition.

- (i) The statement $P(1)$ simply says that $1 \leq 2$ which is certainly true. This is called the *base case*.
- (ii) The second statement that is needed is called the *inductive step*. We are to prove for each positive integer k that $P(k) \Rightarrow P(k+1)$, in other words that if $P(k)$ is true then so is $P(k+1)$. Here the statement $P(k)$ is often referred to as the *inductive hypothesis*, for the aim is to prove $P(k+1)$ under the hypothesis that $P(k)$ is true.

We can sum up what is needed for a direct proof of the inductive step in this case as follows.

Given	Goal
k a positive integer $k \leq 2^k$	$k+1 \leq 2^{k+1}$

In order to obtain the goal we try to relate it to the inductive hypothesis. So we start with one side of the inequality required and express it in

terms of one side of the inequality of the hypothesis. One possibility is the following.

$$\begin{aligned} k+1 &\leqslant 2^k + 1 \text{ (by inductive hypothesis)} \\ &\leqslant 2^k + k \text{ since } k \geqslant 1 \\ &\leqslant 2^k + 2^k \text{ (by inductive hypothesis)} \\ &= 2 \times 2^k = 2^{k+1}. \end{aligned}$$

Alternatively we can start on the other side as follows.

$$\begin{aligned} 2^{k+1} = 2 \times 2^k &\geqslant 2k \text{ (by inductive hypothesis)} \\ &= k + k \\ &\geqslant k + 1. \end{aligned}$$

We write out the formal proof (using the second approach) as follows.

Proof We use induction on n .

Base case: For $n = 1$, $2^n = 2$ and so, since $1 \leqslant 2$, $n \leqslant 2^n$.

Inductive step: Suppose now as inductive hypothesis that $k \leqslant 2^k$ for a positive integer k . Then $2^{k+1} = 2 \times 2^k \geqslant 2k$ (by inductive hypothesis) $= k + k \geqslant k + 1$ and so $2^{k+1} \geqslant k + 1$ as required.

Conclusion: Hence, by induction, $n \leqslant 2^n$ for all positive integers n . \square

The idea of induction is that, since $P(1)$ is true (explicitly checked) and also $P(1) \Rightarrow P(2)$ (special case of inductive step), we know that $P(2)$ is true, and now since $P(2) \Rightarrow P(3)$ we know that $P(3)$ is true, and so on: $P(3) \Rightarrow P(4) \Rightarrow P(5) \Rightarrow \dots$. Eventually this process will reach $P(n)$ for any specified positive integer n . It might be thought that this is ‘obvious’ and in a way it is. But this is because our intuitive ideas about what the integers are include more than the fact that they can be added, multiplied and compared in size. The induction principle is simply a formulation of something which we take for granted about the integers: that we can reach any positive integer by starting from 1 and repeatedly adding 1. Suppose that we think of the integers lined up like dominoes. The inductive step tells us that they are close enough for each domino to knock over the next one, the base case tells us that the first domino falls over, the conclusion is that they all fall over.[†]

[†] The fault in this analogy is that it takes time for each domino to fall and so a domino which is a long way along the line won’t fall over for a long time. Mathematical implication is outside time.

Formally, the induction principle is another axiom about the integers, in addition to the algebraic and order axioms.

It is important to realize that we cannot *prove* a result like Proposition 5.1.2 by considering each case in turn. For any specific value of n we can check the result by calculation. For example, consider $n = 8$: since $2^8 = 256$ and $8 \leq 256$, the statement $P(8)$ is true. But however many individual cases we checked numerically we would not know that the result always held. Indeed there are mathematical statements (such as statement (iv) in Section 1.1) which are known to be true for a huge number of special cases but which have not yet been proved. Proof by induction is not the only way of proving general statements about the positive integers but it does provide an enormously powerful technique.

In writing out proofs by induction it is important to make it clear that this is the method being used and to be absolutely clear what is the statement $P(n)$ that is being proved. If you do no more in developing a proof before writing out a formal proof you should certainly write down what the statement $P(n)$ is.

A template for proofs by induction

It is a good approach for your proofs to follow a standard pattern. First identify the statement $P(n)$ and be clear what the statements $P(1)$, $P(k)$, $P(k + 1)$ each say. Then when you write out the formal proof use the following template.

Proof We use induction on n .

Base case: [Prove the statement $P(1)$]

Inductive step: Suppose now as inductive hypothesis that [$P(k)$ is true] for some positive integer k . Then [deduce that $P(k + 1)$ is true]. This proves the inductive step.

Conclusion: Hence, by induction, [$P(n)$ is true] for all positive integers n . □

There are many variants of this layout. In particular, the conclusion line is often omitted and including the words ‘base case’, ‘inductive step’ and ‘conclusion’ is not usual. However, as you begin to apply the inductive method, using this template helps to emphasize what such a proof involves. The first two parts (base case and inductive step) are

concerned with verifying the conditions in Axiom 5.1.1 and then the last part (conclusion) invokes the axiom.

Here is another example with the proof laid out according to the above template [with a few comments in brackets].

Proposition 5.1.3 *For all positive integers n the number $n^2 + n$ is even.*

Proof We use induction on n .

[In this case the statement $P(n)$ to be proved for all positive integers is ' $n^2 + n$ is even' or equivalently '2 divides $n^2 + n$ ' which means that ' $n^2 + n = 2q$ for some integer q ' (using Definitions 2.2.1 and 2.2.2).]

Base case: For $n = 1$, $n^2 + n = 1 + 1 = 2 = 2 \times 1$, an even number, as required.

Inductive step: Suppose now as inductive hypothesis that $k^2 + k$ is even for some positive integer k . Then $k^2 + k = 2q$ for some integer q .

[Notice now that the statement $P(k + 1)$ is ' $(k + 1)^2 + (k + 1)$ is even'.]

Then $(k+1)^2+(k+1)=k^2+2k+1+k+1=(k^2+k)+2k+2=2q+2k+2$ (by inductive hypothesis) $= 2(q+k+1) = 2p$, where p is the integer $q+k+1$, and so $(k+1)^2+(k+1)$ is even as required.

Conclusion: Hence, by induction, $n^2 + n$ is even for all positive integers n . \square

Often the symbol n is used again when dealing with the inductive step instead of introducing the new symbol k , i.e. the inductive step reads $P(n) \Rightarrow P(n + 1)$ for all positive integers n . The reason for introducing a new letter is that it is easier to write down $P(k + 1)$ by substituting $k + 1$ for n in $P(n)$. Substituting $n + 1$ for n to obtain $P(n + 1)$ can lead to confusion and a common error in inductive proofs is getting $P(k + 1)$ wrong. I would recommend avoiding the double use of the symbol n at least until you are very familiar with inductive proofs.

The examples given in this chapter are quite simple so that we can concentrate on the method. There will be many more examples in this book and the method is very common. Quite a bit of ingenuity may be required in proving the inductive step and even, on occasion, in formulating the statement $P(n)$ properly. The reader will sometimes meet inductive proofs presented informally using phrases like 'and so on' with a comment that a formal argument can be written out using induction; in these cases it can be useful for the reader to try to do this.

5.2 Changing the base case

The induction principle is used to prove a statement about positive integers by first proving the statement for the integer 1 as the base case and then proving that if it holds for some positive integer then it necessarily holds for its successor. However, the same idea can be used starting from any integer as the base case. Suppose that n_0 is an integer, positive, negative or zero. Induction can be used to prove that a statement $P(n)$ is true for all integers n such that $n \geq n_0$. The base case is now $P(n_0)$ and the inductive step is $P(k) \Rightarrow P(k+1)$ for $k \geq n_0$. The basic template given above becomes the following.

Proof We use induction on n .

Base case: [Prove the statement $P(n_0)$]

Inductive step: Suppose now as inductive hypothesis that [$P(k)$ is true] for some integer k such that $k \geq n_0$. Then [deduce that $P(k+1)$ is true]. This proves the inductive step.

Conclusion: Hence, by induction, [$P(n)$ is true] for all integers $n \geq n_0$. □

This is illustrated in the following result comparing the sizes of n^2 and 2^n . Calculating these numbers for low values of n gives the following table.

n	1	2	3	4	5	6	7	8
n^2	1	4	9	16	25	36	49	64
2^n	2	4	8	16	32	64	128	256

This suggests the following result.

Proposition 5.2.1 *For all integers n such that $n \geq 4$, we have the inequality $n^2 \leq 2^n$.*

Constructing a proof. The inductive step of a proof by induction on n reads

$$k^2 \leq 2^k \Rightarrow (k+1)^2 \leq 2^{k+1}$$

for integers $k \geq 4$. We can achieve the right-hand side of the conclusion inequality by multiplying the hypothesis inequality by 2 giving

$$2k^2 \leq 2^{k+1}.$$

Now, if we can prove that $(k+1)^2 \leq 2k^2$ then we can complete the proof of the inductive step using

$$(k+1)^2 \leq 2k^2 \leq 2^{k+1} \Rightarrow (k+1)^2 \leq 2^{k+1}.$$

But this inequality is readily proved for $k \geq 4$ by expanding the brackets and simplifying.

Proof We use induction on n .

Base case: For $n = 4$, $n^2 = 16$ and $2^n = 16$ and so $n^2 \leq 2^n$.

Inductive step: Suppose now as inductive hypothesis that $k^2 \leq 2^k$ for some $k \geq 4$. Then $2^{k+1} = 2 \times 2^k \geq 2k^2$ (by inductive hypothesis). So we will have proved that $2^{k+1} \geq (k+1)^2$ if we can prove that $2k^2 \geq (k+1)^2$. But $2k^2 \geq (k+1)^2 \Leftrightarrow 2k^2 \geq k^2 + 2k + 1 \Leftrightarrow k^2 \geq 2k + 1$ and, since $k \geq 4$, $k^2 \geq 4k \geq 2k + 2 \geq 2k + 1$ so that $k^2 \geq 2k + 1$. Hence $2k^2 \geq (k+1)^2$ and so we have deduced that $(k+1)^2 \leq 2^{k+1}$ as required to complete the inductive step.

Conclusion: Hence, by induction, $n^2 \leq 2^n$ for all $n \geq 4$. \square

Notice that induction starting from a base case other than 1 is not really an extension of the induction principle in Axiom 5.1.1. Consider the statement that $P(n)$ is true for all $n \geq n_0$. If we put $m = n - n_0 + 1$ then $n \geq n_0$ if and only if $m \geq 1$. Thus, since $n = m + n_0 - 1$, $P(n)$ is true for all $n \geq n_0$ if and only if $P(m + n_0 - 1)$ is true for $m \geq 1$. The inductive proof of $P(n)$ with base case $n = n_0$ is essentially identical to the inductive proof of $P(m + n_0 - 1)$ with base case $m = 1$. For example, the result of Proposition 5.2.1 can be rewritten as $(m+3)^2 \leq 2^{m+3}$ for $m \geq 1$. In this form, the result can be proved by induction with base case $m = 1$ and if the reader writes out such a proof it will be clear that it is almost identical to the proof given above.

5.3 Definition by induction

Consider the following result.

Proposition 5.3.1 *The sum of the first n positive integers $1+2+\dots+n$ is equal to $\frac{1}{2}n(n+1)$.*

Whenever you see a line of dots indicating ‘and so on’ this indicates a *definition* by induction (sometimes called a definition by recursion).

In this case, a more precise notation for the sum of the first n positive integers is $\sum_{i=1}^n i$.

Definition 5.3.2 Given a sequence of numbers $a(1), a(2), \dots$, the numbers $\boxed{\sum_{i=1}^n a(i)}$ for positive integers n are defined inductively by the following statements:

- (i) $\sum_{i=1}^1 a(i) = a(1)$; and
- (ii) $\sum_{i=1}^{k+1} a(i) = \sum_{i=1}^k a(i) + a(k+1)$ for $k \geq 1$.

Again we have a base case which tells us what the notation means in the case $n = 1$ and an inductive step which tells us what it means for $n = k + 1$ in terms of what it means for $n = k$. For any specific value of n we can evaluate the expression by repeated use of the inductive step. Thus, for example,

$$\begin{aligned}\sum_{i=1}^3 a(i) &= \sum_{i=1}^2 a(i) + a(3) \quad (\text{by (ii) for } k = 2) \\ &= \sum_{i=1}^1 a(i) + a(2) + a(3) \quad (\text{by (ii) for } k = 1) \\ &= a(1) + a(2) + a(3) \quad (\text{by (i)}).\end{aligned}$$

Using this notation we can rewrite Proposition 5.3.1 as follows.

Proposition 5.3.1 For positive integers n ,

$$\sum_{i=1}^n i = \frac{1}{2}n(n+1).$$

In this case $\sum_{i=1}^n i$ is defined using Definition 5.3.2 with $a(i) = i$.

Constructing a proof. We have to make use of the inductive definition in constructing a proof by induction. In this case the statement $P(n)$ is

the equation in the proposition. So $P(k)$ is

$$\sum_{i=1}^k i = \frac{1}{2}k(k+1)$$

and $P(k+1)$ is

$$\sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)((k+1)+1) = \frac{1}{2}(k+1)(k+2).$$

Let us proceed directly to the formal proof.

Proof We use induction on n .

Base case: For $n = 1$, $\sum_{i=1}^n i = 1$ and $\frac{1}{2}n(n+1) = \frac{1}{2} \cdot 1 \cdot 2 = 1$ and therefore $\sum_{i=1}^n i = \frac{1}{2}n(n+1)$.

Inductive step: Suppose now as inductive hypothesis that

$$\sum_{i=1}^k i = \frac{1}{2}k(k+1)$$

for some positive integer k . Then

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) \quad (\text{by definition}) \\ &= \frac{1}{2}k(k+1) + (k+1) \quad (\text{by inductive hypothesis}) \\ &= \frac{1}{2}(k+1)(k+2) \end{aligned}$$

and so

$$\sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)(k+2)$$

as required.

Conclusion: Hence, by induction, $\sum_{i=1}^n i = \frac{1}{2}n(n+1)$ for all positive integers n . \square

Inductive definitions are implicit in the definitions of several very common functions involving the non-negative integers.

Here are some familiar examples.

Definition 5.3.3 For any real number x , the powers $\boxed{x^n}$ for non-negative† integers n are defined inductively by:

- (i) $x^0 = 1$; and
- (ii) $x^{k+1} = x \cdot x^k$ for non-negative integers k .

If you look back to the proof of Proposition 5.1.2 you will see that we made use of this in the form $2^{k+1} = 2 \times 2^k$.

In the expression x^n , the number n is called the *index* or the *exponent* and the number x is called the *base*.

Definition 5.3.4 For non-negative integers n , the numbers $\boxed{\text{factorial } n}$, written $\boxed{n!}$, are defined inductively by:

- (i) $0! = 1$; and
- (ii) $(k+1)! = (k+1) \times k!$ for non-negative integers k .

Notice that $n = 0$ is the base case in this definition.

Indeed, even the basic operations of addition and multiplication of integers can be defined inductively starting from the notion of successor (see Definition 9.4.3).

5.4 The strong induction principle

For completeness at this point we consider another variant of the inductive method although if the reader is meeting this method of proof for the first time the remainder of this chapter (apart from the exercises) should be omitted at first reading. The method will not be used subsequently until the proof of Proposition 23.1.2.

Sometimes we discover that $P(k+1)$ is not implied by $P(k)$ alone but is implied by the truth of $P(k)$ together with some or all of $P(1)$, $P(2)$, ..., $P(k-1)$. In this case we work with the following version of induction.

Axiom 5.4.1 (The strong induction principle) Suppose that $P(n)$

† This definition allows $x = 0$ and $n = 0$ and sets 0^0 to be 1. This is the convention only in certain contexts such as Exercise 5.4 where we use the notation $\sum_{i=0}^n x^i$ to represent the geometric progression $1 + x + x^2 + \dots + x^n$ even when $x = 0$. However, some care is required and in certain other contexts it is not possible to attach a sensible meaning to 0^0 . A little more is said about this difficulty in the solution to Exercise 5.6 and in a footnote to Example 9.2.4(b).

is a statement involving a general positive integer n . Then $P(n)$ is true for all positive integers n if

- (i) $P(1)$ is true, and
- (ii) $[P(n) \text{ holds for all positive integers } n \leq k] \Rightarrow P(k+1)$, for all positive integers k .

It is not difficult to see that this is equivalent to Axiom 5.1.1.

In this case the basic template is as follows.

Proof We use (strong) induction on n .

Base case: [Prove the statement $P(1)$]

Inductive step: Suppose now as inductive hypothesis that $[P(n) \text{ is true for all positive integers } n \leq k]$ for some positive integer k . Then [deduce that $P(k+1)$ is true]. This proves the inductive step.

Conclusion: Hence, by induction, $[P(n) \text{ is true}]$ for all positive integers n . □

As an illustration of the use of this form of induction we introduce the Fibonacci numbers.

Definition 5.4.2 For each positive integer n define the number u_n inductively as follows.

$$\begin{aligned} u_1 &= 1, \\ u_2 &= 1, \\ u_{k+1} &= u_{k-1} + u_k \quad \text{for } k \geq 2. \end{aligned}$$

The beginning of this sequence of numbers is 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ..., and the sequence is known as the *Fibonacci sequence*. The important observation which concerns us now is that each number

† Leonardo of Pisa (ca. 1180–1250), who published his best known book *Liber abaci* in 1202, wrote under the name of Fibonacci. He was largely responsible for introducing Hindu–Arabic algebra and numerals to Europe and is often considered the greatest European mathematician of the Middle Ages. His name was attached to these numbers by the nineteenth century number theorist Edouard Lucas because of a problem in the *Liber abaci* concerned with the reproduction of rabbits whose solution involves them (see Problems I, Question 24). The early numbers occur frequently in nature, for example the number of petals in most flowers is a Fibonacci number. Also the sequence has many beautiful mathematical properties and there is even a scholarly journal *The Fibonacci Quarterly* devoted to articles about the sequence and related topics.

is determined not simply by the previous one as in a simple inductive definition but by the previous *two* numbers. This means that we must specify the first two numbers as the base case of the definition.

Proposition 5.4.3 (The Binet† formula) *The Fibonacci numbers are given by the following formula:*

$$u_n = (\alpha^n - \beta^n)/\sqrt{5},$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$.

It should be observed that α and β are the roots of the equation $x^2 - x - 1 = 0$ and so $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. The reader may find it remarkable that this formula for these *integers* involves $\sqrt{5}$ which is most certainly not an integer; in fact, as we will see in Chapter 13, it is not even a rational number! There is in fact a general procedure for finding a general formula for sequences defined in this way (these are called *linear recursive sequences* or *linear difference equations*) which bears a close resemblance to elementary methods for solving linear differential equations. This method leads to a quadratic equation when each term of the sequence depends on the previous two terms.

The number α was called *the ratio* by the Greeks and in the sixteenth century became known as *the golden ratio*. A rectangle whose sides are in this ratio is called a *golden rectangle* and a construction for such a rectangle is given in Book Six of the *Elements* of Euclid. Such a rectangle was considered to have ideal proportions: it is characterized by the fact that on the removal from the end of the rectangle of a square with sides equal to the shorter sides of the rectangle the remaining rectangle is similar to the original rectangle (and so is also a golden rectangle). As n increases, the ratio of successive Fibonacci numbers u_{n+1}/u_n approaches the number α .

Proof The above formula may be proved by strong induction on n . In this case $P(n)$ is the statement in the proposition.

Base case: For $n = 1$, the formula gives $(\alpha - \beta)/\sqrt{5} = ((1 + \sqrt{5}) - (1 - \sqrt{5}))/2\sqrt{5} = 1 = u_1$.

Since the inductive formula does not apply until u_3 we have also to deal with the case $n = 2$ by calculation. For $n = 2$, the formula gives $(\alpha^2 - \beta^2)/\sqrt{5} = (\alpha - \beta)/\sqrt{5} = 1 = u_2$ using the facts that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$.

† J.P.M. Binet was a French mathematician of the early nineteenth century.

Inductive step: Now suppose as inductive hypothesis that the formula holds for all positive integers n such that $n \leq k$ for some positive integer $k \geq 2$. Then

$$\begin{aligned} u_{k+1} &= u_{k-1} + u_k \quad (\text{by definition of the sequence}) \\ &= ((\alpha^{k-1} - \beta^{k-1}) + (\alpha^k - \beta^k)) / \sqrt{5} \\ &\quad (\text{by inductive hypothesis}) \\ &= ((\alpha^{k-1}(1 + \alpha) - \beta^{k-1}(1 + \beta)) / \sqrt{5} \\ &= (\alpha^{k+1} - \beta^{k+1}) / \sqrt{5} \\ &\quad (\text{again using } \alpha^2 = \alpha + 1 \text{ and } \beta^2 = \beta + 1) \end{aligned}$$

as required to prove the formula for $n = k + 1$.

Conclusion: Hence, by induction, the formula holds for all positive integers n . \square

Exercises

5.1 Prove by induction on n that, for all positive integers n , $n^3 - n$ is divisible by 3.

5.2 Prove by induction on m that $m^3 \leq 2^m$ for $m \geq 10$.

5.3 Prove by induction on n that, for all positive integers n , $n \geq 1$.

5.4 Prove by induction on n that, for any real number $x \neq 1$ and for integers $n \geq 0$,

$$\sum_{i=0}^n x^i = \frac{1 - x^{n+1}}{1 - x}.$$

5.5 Prove that, for any real numbers a and b and for integers $n \geq 0$,

$$\sum_{i=0}^n (a + ib) = \frac{1}{2}(n + 1)(2a + nb).$$

5.6 For non-negative integers n define the number u_n inductively as follows.

$$\begin{aligned} u_0 &= 0, \\ u_{k+1} &= 3u_k + 3^k \quad \text{for } k \geq 0. \end{aligned}$$

Prove that $u_n = n3^{n-1}$ for all non-negative integers n .

5.7 Prove by induction on n that, for any real numbers x and y and for non-negative integers m and n :

- (i) $x^n y^n = (xy)^n$;
- (ii) $x^{m+n} = x^m x^n$;
- (iii) $(x^m)^n = x^{mn}$.

[These statements are known as the laws of exponents or the laws of indices.]

Problems I: Mathematical statements and proofs

1. By using truth tables prove that, for all statements P and Q , the statement ' $P \Rightarrow Q$ ' and its *contrapositive* ' $(\text{not } Q) \Rightarrow (\text{not } P)$ ' are equivalent. In Example 1.2.3 identify which statement is the contrapositive of statement (i) $(f(a) = 0 \Rightarrow a > 0)$. Find another pair of statements in that list which are the contrapositives of each other.
2. By using truth tables prove that, for all statements P and Q , the three statements (i) ' $P \Rightarrow Q$ ', (ii) ' $(P \text{ or } Q) \Leftrightarrow Q$ ' and (iii) ' $(P \text{ and } Q) \Leftrightarrow P$ ' are equivalent.
3. Prove that the three basic connectives 'or', 'and' and 'not' can all be written in terms of the single connective 'notand' where ' P notand Q ' is interpreted as 'not $(P \text{ and } Q)$ '.
4. Prove the following statements concerning positive integers a , b and c .
 - (i) $(a \text{ divides } b) \text{ and } (a \text{ divides } c) \Rightarrow a \text{ divides } (b + c)$.
 - (ii) $(a \text{ divides } b) \text{ or } (a \text{ divides } c) \Rightarrow a \text{ divides } bc$.
5. Which of the following conditions are *necessary* for the positive integer n to be divisible by 6 (proofs not necessary)?
 - (i) 3 divides n .
 - (ii) 9 divides n .
 - (iii) 12 divides n .
 - (iv) $n = 12$.
 - (v) 6 divides n^2 .
 - (vi) 2 divides n and 3 divides n .

- (vii) 2 divides n or 3 divides n .

Which of these conditions are *sufficient*?

- 6.** Use the properties of addition and multiplication of real numbers given in Properties 2.3.1 to deduce that, for all real numbers a and b ,

- (i) $a \times 0 = 0 = 0 \times a$,
- (ii) $(-a)b = -ab = a(-b)$,
- (iii) $(-a)(-b) = ab$.

- 7.** Prove by contradiction the following statement concerning an integer n .

$$n^2 \text{ is even} \Rightarrow n \text{ is even.}$$

[You may suppose that an integer n is odd if and only if $n = 2q + 1$ for some integer q . This is proved later as Proposition 11.3.4.]

- 8.** Prove the following statements concerning a real number x .

- (i) $x^2 - x - 2 = 0 \Leftrightarrow x = -1 \text{ or } x = 2$.
- (ii) $x^2 - x - 2 > 0 \Leftrightarrow x < -1 \text{ or } x > 2$.

- 9.** Prove by contradiction that there does not exist a largest integer.

[Hint: Observe that for any integer n there is a greater one, say $n + 1$. So begin your proof]

Suppose for contradiction that there is a largest integer. Let this integer be n]

- 10.** What is wrong with the following proof that 1 is the largest integer?

Let n be the largest integer. Then, since 1 is an integer we must have $1 \leq n$. On the other hand, since n^2 is also an integer we must have $n^2 \leq n$ from which it follows that $n \leq 1$. Thus, since $1 \leq n$ and $n \leq 1$ we must have $n = 1$. Thus 1 is the largest integer as claimed.

What does this argument prove?

- 11.** Prove by contradiction that there does not exist a smallest positive real number.

- 12.** Prove by induction on n that, for all positive integers n , 3 divides $4^n + 5$.

13. Prove by induction on n that $n! > 2^n$ for all integers n such that $n \geq 4$.

14. Prove Bernoulli's inequality

$$(1+x)^n \geq 1+nx$$

for all non-negative integers n and real numbers $x > -1$.

15. For which non-negative integer values of n is $n! \geq 3^n$?

16. Prove by induction on n that

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1},$$

for all positive integers n .

17. For a positive integer n the number a_n is defined inductively by

$$\begin{aligned} a_1 &= 1, \\ a_{k+1} &= \frac{6a_k + 5}{a_k + 2} \quad \text{for } k \text{ a positive integer.} \end{aligned}$$

Prove by induction on n that, for all positive integers, (i) $a_n > 0$ and (ii) $a_n < 5$.

18. Given a sequence of numbers $a(1), a(2), \dots$, the number $\prod_{i=1}^n a(i)$ is defined inductively by

$$(i) \prod_{i=1}^1 a(i) = a(1), \text{ and}$$

$$(ii) \prod_{i=1}^{k+1} a(i) = \left(\prod_{i=1}^k a(i) \right) a(k+1) \text{ for } k \geq 1.$$

Prove that $\prod_{i=1}^n (1 + x^{2^{i-1}}) = (1 - x^{2^n}) / (1 - x)$ for $x \neq 1$.

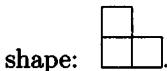
What happens if $x = 1$?

19. Prove that

$$\prod_{i=2}^n \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$$

for integers $n \geq 2$.

20. Prove that, for a positive integer n , a $2^n \times 2^n$ square grid with any one square removed can be covered using L-shaped tiles of the following



21. Suppose that x is a real number such that $x + 1/x$ is an integer. Prove by induction on n that $x^n + 1/x^n$ is an integer for all positive integers n .

[For the inductive step consider $(x^k + 1/x^k)(x + 1/x)$.]

22. Prove that

$$\frac{1}{n} \sum_{i=1}^n x_i \geq \left(\prod_{i=1}^n x_i \right)^{1/n}$$

for positive integers n and positive real numbers x_i .

[It does not seem to be possible to give a direct proof of this result using induction on n . However, it can be proved for $n = 2^m$ for $m \geq 0$ by induction on m . The general result now follows by proving the converse of the usual inductive step: if the result holds for $n = k + 1$, where k is a positive integer, then it holds for $n = k$.]

23. For non-zero real numbers x we may extend Definition 5.3.3 to a definition of powers x^n for all integers n by defining $x^{-m} = 1/x^m$ for integers $m > 0$. With this definition prove the laws of exponents for any non-zero real numbers x and y and integers m and n :

- (i) $x^n y^n = (xy)^n$;
- (ii) $x^{m+n} = x^m x^n$;
- (iii) $(x^m)^n = x^{mn}$.

[Hint: Start from Exercise 5.7.]

24. Fibonacci's rabbit problem may be stated as follows:

How many pairs of rabbits will be produced in a year, beginning with a single pair, if in every month each pair bears a new pair which become productive from the second month on?

Assuming that no rabbits die, express the number after n months as a Fibonacci number and hence answer the problem. Using a calculator and the Binet formula (Proposition 5.4.3) find the number after three years.

25. Let u_n be the n th Fibonacci number (Definition 5.4.2). Prove, by induction on n (without using the Binet formula Proposition 5.4.3), that

$$u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$$

for all positive integers m and n .

Deduce, again using induction on n , that u_m divides u_{mn} .

26. Suppose that n points on a circle are all joined in pairs. The points are positioned so that no three joining lines are concurrent in the interior of the circle. Let a_n be the number of regions into which the interior of the circle is divided. Draw diagrams to find a_n for $n \leq 6$.

Prove that a_n is given by the following formula.

$$\begin{aligned} a_n &= n + \binom{n-1}{2} + \binom{n-1}{3} + \binom{n-1}{4} \\ &= 1 + n(n-1)(n^2 - 5n + 18)/24. \end{aligned}$$

[Here $\binom{m}{r}$ denotes the binomial coefficient $\frac{m!}{r!(m-r)!}$ discussed in more detail in Chapter 12.]

Part II

Sets and functions

6

The language of set theory

The students' task in learning set theory is to steep themselves in unfamiliar and essentially shallow generalities till they become so familiar that they can be used with almost no conscious effort.

Paul R. Halmos, *Naive set theory* (adapted slightly).

The language of set theory is used throughout mathematics. Many general results involve 'an integer n ' or 'a real number a ' and, to start with, set theory notation provides a simple way of asserting for example that n is an integer. However, it turns out that this language is remarkably flexible and powerful and in much mathematics it is indispensable for a proper expression of the ideas involved.

In the second part of this book we introduce the basic vocabulary of the language of sets and functions. The third part of the book will then provide some experience in using this language as we use it to give a precise formulation of the idea of counting, one of the earliest mathematical concepts.

6.1 Sets

At this introductory level it is sufficient to define the notion of *set* as any well-defined collection of objects. We can think of a set as a box containing certain objects. In this section some ways of specifying sets are introduced and also some frequently used notation.

We frequently use a single letter to denote a set. This represents a further stage of mathematical abstraction. The reader will already have accepted the abstract notion of a positive integer, for example 'two' is abstracted from 'two apples' and 'two chairs'. Now we move on to consider the set of all positive integers as a single mathematical object. Each time there is further step of abstraction like this it takes time to

become familiar with new sorts of objects. At the end of this chapter we will make a further abstraction step when we consider sets which are collections of sets!

Particular sets which are often used have standard symbols to represent them. In this book the following will be used.

\mathbb{Z} denotes the set of all integers.[†]

\mathbb{Z}^+ denotes the set of all positive integers (natural[‡] or counting numbers): 1, 2, 3, etc.

\mathbb{Z}^{\geq} denotes the set of all non-negative integers: 0, 1, 2, 3, etc.

\mathbb{Q} denotes the set of all rational numbers (fractions).

\mathbb{R} denotes the set of all real numbers (i.e. numbers expressible as infinite decimals).

\mathbb{R}^+ denotes the set of all positive real numbers.

\mathbb{R}^{\geq} denotes the set of all non-negative real numbers.

\mathbb{C} denotes the set of all complex numbers.

The objects in a set are called the *elements*, *members* or *points* of the set. We write

$$x \in E$$

to denote the fact that the object x is an element of the set E . Thus for example ' $a \in \mathbb{R}$ ' is read ' a is an element of the set of real numbers' or more simply just ' a is a real number'. The symbol ' \in ', first used in this way by the Italian mathematician Giuseppe Peano towards the end of the nineteenth century, is a variant of the Greek letter epsilon and care should normally be taken to distinguish it from that letter which is usually written ' ε ' or ' ϵ '. However, some books do not make this distinction and use epsilon in place of ' \in '. It is common to use upper case letters to represent sets and lower case to represent elements but this is not always appropriate: in geometry it is usual to use upper case letters to represent points and lower case letters to represent lines (which are sets of points); another exception occurs when a set is itself considered as an element of another set.

The negation of the statement $x \in A$ is written $x \notin A$. Thus $\sqrt{2} \notin \mathbb{Q}$ is the statement that $\sqrt{2}$ is not a rational number.

There are basically three ways of specifying a set: we can list the

[†] This symbol comes from 'Zahlen', the German word for 'numbers'.

[‡] Some people include the number 0 in the set of natural numbers but this seems to me unnatural as we usually start counting at 1. Because of this ambiguity, in this book we will normally refer to 'the non-negative integers' or 'the positive integers' depending on whether or not the number 0 is included.

elements, specify a condition for membership, or give a formula or algorithm constructing the elements of the set.

(a) Listing the elements of a set

When we list the elements of a set we denote the set by enclosing the elements in curly brackets. Thus

$$A = \{1, 3, \pi, -14\}$$

is the statement that A is the set whose four elements are 1, 3, π and -14 . In this case we have $1 \in A$ and $2 \notin A$. Notice that the order in which the elements are listed is unimportant and repeating an element makes no difference. Thus, for the above set A we also have

$$A = \{\pi, 3, -14, 1\} = \{\pi; 3, \pi, 1, -14, -14\}.$$

On the face of it the listing notation is only practical for sets with a small number of elements. However it can be extended to large or even infinite sets. For example we can write

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$$

where as usual the dots are read ‘and so on’.

(b) The conditional definition of a set

Alternatively, a set may be described by specifying some condition which determines whether or not an object is an element of the set. Let us illustrate this with an example. Consider the set B defined as follows:

$$B = \{n \in \mathbb{Z} \mid 0 < n < 6\}.$$

Here we write $n \in \mathbb{Z}$ simply to indicate the sort of objects that we are considering. The statement $0 < n < 6$ is a predicate. The definition means that B is the set of integers which when substituted in this predicate give a true proposition, i.e. given an integer n ,

$$n \in B \Leftrightarrow 0 < n < 6.$$

Of course we could have described this particular set by listing the elements,

$$B = \{1, 2, 3, 4, 5\},$$

but in some cases this is difficult or impossible.

In the conditional definition of a set the vertical line† ‘|’ is read as ‘such that’ and so the above definition would be read as ‘ B is the set of integers n such that $0 < n < 6$ ’ or just ‘ B is the set of integers between 0 and 6’. This last reading, which makes no reference to the variable ‘ n ’, demonstrates that the symbol n in this definition represents a *dummy variable*: its only rôle is to indicate the internal logic of the definition and it can be replaced by any other symbol (not already in use) without any change in meaning. Thus we could equally write

$$B = \{ \alpha \in \mathbb{Z} \mid 0 < \alpha < 6 \}.$$

Notice that, although $0 < n < 6$ is a predicate and so a mathematical statement in the sense of Chapter 1, $\{ n \in \mathbb{Z} \mid 0 < n < 6 \}$ is not a statement; it is simply a mathematical object and can be no more true or false than the number 2 can be true or false. However, we can make statements about this object, such as ‘ $2 \in \{ n \in \mathbb{Z} \mid 0 < n < 6 \}$ ’ which is true, or ‘ $m \in \{ n \in \mathbb{Z} \mid 0 < n < 6 \}$ ’ which is equivalent to ‘ $m \in \mathbb{Z}$ and $0 < m < 6$ ’.

(c) The constructive definition of a set

The other systematic method of describing a set is to give a formula (or more generally an algorithm) constructing the elements of the set. For example

$$\{ n^2 \mid n \in \mathbb{Z} \} = \{ 0, 1, 4, 9, 16, \dots \}$$

is the set of integer squares, which means that the formula n^2 constructs the elements of the set as n takes all possible integer values, i.e. an element is in the set if and only if it can be written as n^2 for some integer n . Notice that in this case all non-zero elements in the set arise twice. This makes no difference to the set so that for example $\{ n^2 \mid n \in \mathbb{Z}^{\geq} \}$ defines the same set.

Similarly,

$$\{ 2q \mid q \in \mathbb{Z} \} = \{ \dots, -4, -2, 0, 2, 4, 6, \dots \}$$

is the set of even integers, and

$$\{ a/b \mid a, b \in \mathbb{Z}, b \neq 0 \}$$

is the set of rational numbers, \mathbb{Q} . This last example illustrates the

† Alternative notations are to use a colon ‘:’ or a semi-colon ‘;’ here instead of ‘|’ as follows: $B = \{ n \in \mathbb{Z} : 0 < n < 6 \}$ or $\{ n \in \mathbb{Z} ; 0 < n < 6 \}$.

convention that when more than one condition is listed after the symbol ‘|’ this means that all the conditions must be satisfied for an object to be in the set so that the word ‘and’ is understood.

Equality of sets

Quite commonly problems in mathematics take the form of seeking to pass between different ways of specifying the elements of a set. For example when we learn how to solve quadratic equations of the form $ax^2 + bx + c = 0$, where a , b and c are given real numbers, we are learning how to list the elements of the set $\{x \in \mathbb{R} \mid ax^2 + bx + c = 0\}$, or possibly the set $\{x \in \mathbb{C} \mid ax^2 + bx + c = 0\}$ if we allow complex solutions.

Definition 6.1.1 Two sets A and B are **equal**, written $A = B$, if they have precisely the same elements, i.e. $A = B$ means $x \in A \Leftrightarrow x \in B$.

To put it another way: a set is determined by its elements. Notice that this means that to show that two sets A and B are equal it is necessary to prove two things (although they can often be done together in simple cases): every element of A is an element of B and conversely every element of B is an element of A .

Example 6.1.2 $\{x \in \mathbb{R} \mid x^2 - x - 2 = 0\} = \{-1, 2\}$.

Constructing a proof. This is another way of stating that, for x a real number,

$$x^2 - x - 2 = 0 \Leftrightarrow x = -1 \text{ or } x = 2.$$

This is easily proved by the factorization method.

Proof For x a real number, $x^2 - x - 2 = 0 \Leftrightarrow (x - 2)(x + 1) = 0 \Leftrightarrow x - 2 = 0$ or $x + 1 = 0$ (by Proposition 4.4.1) $\Leftrightarrow x = 2$ or $x = -1$. Hence $x^2 - x - 2 = 0$ if and only if $x = -1$ or $x = 2$, as required. \square

At this stage it is convenient to introduce two other ideas from set theory.

Definition 6.1.3 The **empty set** is the unique set which has no elements at all. It is denoted by the symbol \emptyset .

Thus the statement that the quadratic equation $x^2 + 2x + 2 = 0$ has no real solutions may be written $\{x \in \mathbb{R} \mid x^2 + 2x + 2 = 0\} = \emptyset$.

Take care to distinguish ' \emptyset ' which is a variant of a Scandinavian letter from the Greek letter phi written ' ϕ '.

Definition 6.1.4 Given sets A and B we say that A is a subset of B ,

written $A \subseteq B$, or $B \supseteq A$, when every element of A is an element of B , i.e. $x \in A \Rightarrow x \in B$. If A and B are in addition unequal so that B contains some element not contained in A , then we say that A is a proper subset of B and write $A \subset B$.†

Thus

$$A = B \Leftrightarrow (A \subseteq B \text{ and } B \subseteq A).$$

It is important to distinguish between the symbols \in and \subseteq although they are closely related as follows:

$$a \in A \Leftrightarrow \{a\} \subseteq A.$$

If sets are defined by predicates then there is a correspondence between the notions of 'implication' and 'subset': the universal statement that $P(a) \Rightarrow Q(a)$ for all $a \in A$ is equivalent to the statement that the set $\{a \in A \mid P(a)\}$ is a subset of $\{a \in A \mid Q(a)\}$.

Notice that if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$ since $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in C$ together imply that $x \in A \Rightarrow x \in C$. Furthermore $\emptyset \subseteq A$ for all sets A whereas $A \subseteq \emptyset$ only if $A = \emptyset$.

6.2 Operations on sets

Definition 6.2.1 Given two sets A and B we can form the set of elements which lie both in A and in B . This is called the intersection of A and B and is denoted by $A \cap B$. Thus

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

† Some mathematicians use \subset where \subseteq is used in this book. In fact when Peano originally introduced this notation he used it the other way round, writing $A \supset B$ to indicate that A is a subset of B !

Two sets A and B are said to be disjoint if $A \cap B = \emptyset$, i.e. A and B have no elements in common.

Definition 6.2.2 Given two sets A and B we can form the set of elements which lie in A or lie in B . This is called the union of A and B and is denoted by $A \cup B$. Thus

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

Definition 6.2.3 Given two sets A and B we can form the set of elements which lie in A but not in B . This is called the difference of A and B and is denoted by† $A - B$. Thus

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Notice that $A \cap A = A = A \cup A$, $A \cap \emptyset = \emptyset$, $A \cup \emptyset = A$, $A - A = \emptyset$ and $A - \emptyset = A$.

Proposition 6.2.4 Given any two sets A and B , the three sets $A \cap B$, $A - B$ and $B - A$ are pairwise disjoint (i.e. each pair of these sets is disjoint) and

$$A \cup B = (A \cap B) \cup (A - B) \cup (B - A).$$

Probably the simplest way to prove a statement like this is by means of truth tables as follows.

Proof Consider the truth tables on the following page.

The fact that the final two columns of the second table are the same tells us that the above equality of sets holds. The fact that no row has more than one T in the third, fourth and fifth columns of the first table

† The reader should be aware that this notation is sometimes used in algebra to denote the set $\{a - b \mid a \in A, b \in B\}$. In this case the difference of the two sets A and B is denoted by $A \setminus B$.

tells us that the three corresponding sets are disjoint.

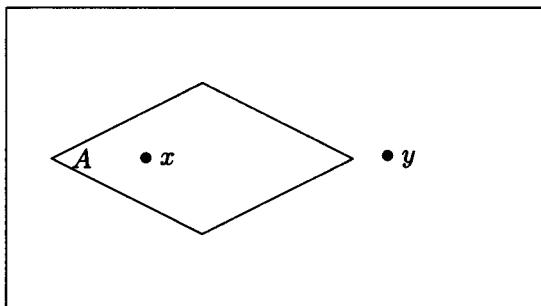
$x \in A$	$x \in B$	$x \in A \cap B$	$x \in A - B$	$x \in B - A$
T	T	T	F	F
T	F	F	T	F
F	T	F	F	T
F	F	F	F	F

$x \in A$	$x \in B$	$x \in (A \cap B) \cup (A - B) \cup (B - A)$	$x \in A \cup B$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

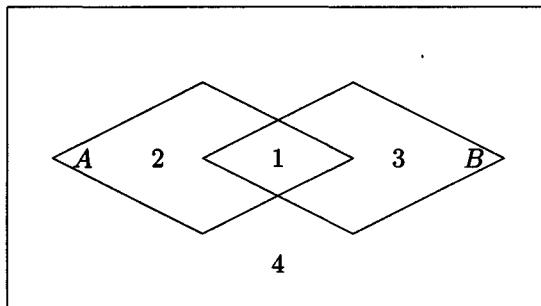
□

In the truth tables in the above proof the columns are headed by statements $x \in A$, $x \in B$, etc. which can be true or false, not simply by the names of the sets A , B , etc. which would not be statements.

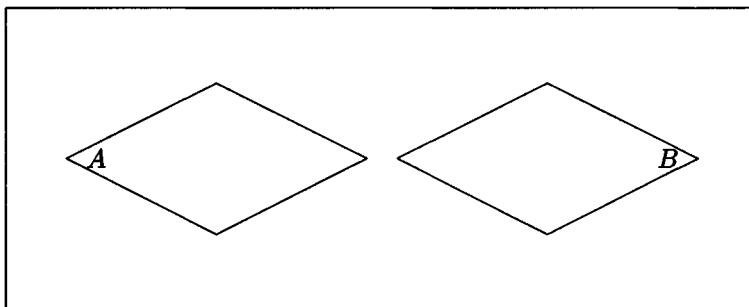
This proof illustrates the close relationship between the logical connectives introduced in Chapter 1 and the operations on sets defined above in terms of those connectives. Proofs of the above type are usually illustrated by a *Venn diagram*. We indicate a set A by the interior region of some curve drawn on the page so that the elements of the set correspond to points in the region. Thus for example in the following diagram $x \in A$ but $y \notin A$.



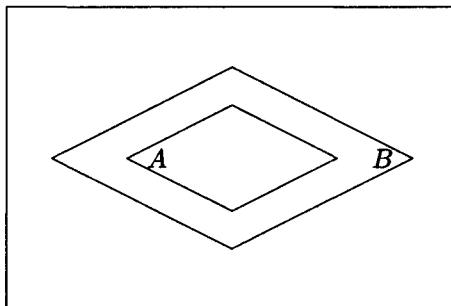
Two general sets A and B are described by two overlapping regions. Consider the following diagram.



Here the interior of the left-hand rhombus (regions 1 and 2) denotes A and the interior of the right-hand rhombus (regions 1 and 3) denotes B . Then the four rows of the above truth tables correspond to the four regions in the diagram. Thus region 1 corresponds to $A \cap B$, region 2 corresponds to $A - B$, region 3 corresponds to $B - A$ and the three regions 1, 2 and 3 together give $A \cup B$. The fact that regions 1, 2 and 3 are disjoint corresponds to the fact that the three sets on the right-hand side of Example 6.2.4 are disjoint and the fact that these three regions together make up $A \cup B$ corresponds to the equality of sets in Proposition 6.2.4. From this point of view the result is essentially obvious. Care is needed in using this sort of diagrammatic proof in more elaborate examples because unless proper care is taken it is sometimes possible to draw a diagram that does not include all possible regions or some feature of the diagram has nothing to do with the set theory (see for example the solution to Exercise 6.6). Notice that this diagram does not imply that $A \cap B$ is non-empty for it may be that there are no elements in the region 1. However, if we were given that $A \cap B = \emptyset$ then we could denote this by the following Venn diagram.



We can represent $A \subseteq B$ as follows.



6.3 The power set

Definition 6.3.1 The power set of a set X , denoted by $\mathcal{P}(X)$, is the set of all subsets of the set X . Thus $A \in \mathcal{P}(X)$ is another way of writing $A \subseteq X$.

Example 6.3.2 If $X = \{a, b, c\}$ then

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}.$$

Notice that the empty set \emptyset is an element of the power set $\mathcal{P}(X)$ for any set X since $\emptyset \subseteq X$. A set like $\{a\}$ with a single element is called a *singleton*. It is important to distinguish the singleton set $\{a\}$ from the element a . In particular the singleton $\{\emptyset\}$ is to be distinguished from the empty set \emptyset : a box containing an empty box is not an empty box!

It is often the case that all the sets we are considering are subsets of some fixed set, say the set of real numbers. We then consider this to be the *universal set*.

Definition 6.3.3 Once we have fixed a universal set U we can define the complement of any $A \in \mathcal{P}(U)$, denoted by A^c , to be the difference of U and A . Thus

$$A^c = U - A = \{x \in U \mid x \notin A\}.$$

For example, if the universal set is \mathbb{Z} , the set of integers, and E is the set of even integers, then the complement E^c is the set of odd integers.

The intersection, union and complement of subsets of some universal set U correspond to the logical connectives ‘and’, ‘or’ and ‘not’. The relationships between these operations may be summed up in the following theorem.

Theorem 6.3.4 *Let A , B and C be subsets of some universal set U (i.e. $A, B, C \in \mathcal{P}(U)$). Then we have the following identities.*

- (i) associativity: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.
- (ii) commutativity: $A \cup B = B \cup A$, $A \cap B = B \cap A$.
- (iii) distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- (iv) De Morgan laws:[†] $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$.
- (v) complementation: $A \cup A^c = U$, $A \cap A^c = \emptyset$.
- (vi) double complement: $(A^c)^c = A$.

These can be proved by truth tables or Venn diagrams. Alternatively they can be proved by using logical argument from the definitions. Let us illustrate this by writing out the proof of one part.

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof of ‘ \subseteq ’: Suppose that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in (B \cup C)$. Since $x \in B \cup C$, $x \in B$ or $x \in C$. If $x \in B$ then, since $x \in A$ as well, we have $x \in A \cap B$ and so $x \in (A \cap B) \cup (A \cap C)$ as required. On the other hand, if $x \notin B$, then we must have $x \in C$ and so, since also $x \in A$, we have $x \in A \cap C$ and so $x \in (A \cap B) \cup (A \cap C)$.

Proof of ‘ \supseteq ’: Suppose now that $x \in (A \cap B) \cup (A \cap C)$. Then $x \in A \cap B$ or $x \in A \cap C$. If $x \in A \cap B$, then $x \in A$ and $x \in B$ so that $x \in A$ and $x \in B \cup C$ which gives $x \in A \cap (B \cup C)$ as required. On the other hand if $x \notin A \cap B$ then $x \in A \cap C$ and again we get $x \in A \cap (B \cup C)$. \square

We can now use these results to derive other set identities by algebraic manipulation. Here is an example.

Proposition 6.3.5

$$(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D).$$

[†] These results was observed independently in the nineteenth century by the British mathematician Augustus De Morgan and the United States mathematician Benjamin Peirce (see C.B. Boyer and U.C. Merzbach, *A history of mathematics*, Wiley, Second edition 1989). They correspond to the equivalence of the statements ‘not (P and Q)’ and ‘(not P) or (not Q)’ commented on in the solution to Exercise 1.2.

Proof First notice that commutativity means that distributivity on one side implies distributivity on the other side so that Theorem 6.3.4(iii) implies that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

$$\begin{aligned} & (A \cup B) \cap (C \cup D) \\ &= (A \cap (C \cup D)) \cup (B \cap (C \cup D)) \quad \text{by distributivity} \\ &= (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D) \quad \text{by distributivity.} \end{aligned}$$

The associativity of the union operation means that we do not need any additional brackets here. \square

Exercises

6.1 The following are standard subsets of the set of real numbers known as the real intervals with endpoints the real numbers a and b .

The *open interval*: $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.

The *closed interval*: $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

The *right half-open interval*: $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$.

The *left half-open interval*: $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$.

- (i) Prove that $0 \notin (0, 1)$, $0 \in [0, 1]$, $0 \in [0, 1)$ and $0 \notin (0, 1]$.
- (ii) Find the elements of the set $[a, b] - (a, b)$.
- (iii) Prove that $(a, b) = \emptyset$ if and only if $a \geq b$. [Hint: Prove the contrapositive.]
Find the corresponding results for the other real intervals with endpoints a and b .
- (iv) Prove that, if $a \leq b$, then $[a, b] \subseteq (c, d)$ if and only if $c < a$ and $b < d$.

6.2 Prove that

- (i) $\{x \in \mathbb{R} \mid x^2 + x - 2 = 0\} = \{1, -2\}$,
- (ii) $\{x \in \mathbb{R} \mid x^2 + x - 2 < 0\} = (-2, 1)$,
- (iii) $\{x \in \mathbb{R} \mid x^2 + x - 2 > 0\} = \{x \in \mathbb{R} \mid x < -2\} \cup \{x \in \mathbb{R} \mid x > 1\}$.

6.3 Find predicates which determine the following subsets of the set of integers \mathbb{Z} : (i) $\{3\}$, (ii) $\{1, 2, 3\}$, (iii) $\{1, 3\}$.

6.4 By using a truth table prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Draw a Venn diagram to illustrate the proof.

6.5 Prove that

- (i) $A \subseteq B \Leftrightarrow A \cup B = B$,
- (ii) $A \subseteq B \Leftrightarrow A \cap B = A$.

6.6 Prove by contradiction that, if $A \cap B \subseteq C$ and $x \in B$, then $x \notin A - C$.
[Work from the definitions of ' $A \cap B$ ', ' $A - C$ ', and ' \subseteq '.]

6.7 Using the fact that an implication is equivalent to its contrapositive, prove that, for subsets of a universal set U , $A \subseteq B$ if and only if $B^c \subseteq A^c$.

7

Quantifiers

In Chapter 1 a predicate was described as an expression containing one or more free variables; it becomes a proposition, and so is true or false, when a specific value is assigned to each free variable. Of course whether this proposition is true or is false usually depends on the values selected.

However, we saw in the last chapter that a proposition can be created from a predicate in another way – by making a statement about the set of values of the free variables which make it true. Many results in mathematics take the form of listing the values of this set, for example when we solve an equation. But often results simply address the question of whether there is any choice of values of the free variables resulting in a true proposition and whether there is any choice resulting in a false proposition. Statements that such values exist are known as existential statements. Statements that they do not can be thought of as universal statements. We met examples of universal statements when discussing implications in Chapter 2.

In this chapter we discuss general universal and existential statements.

7.1 Universal statements

Suppose that $P(a)$ is a predicate with a single free variable a with possible values in a set A . Usually $P(a)$ is true for some elements of the set A and false for others, and in the last chapter we described how such a predicate could be used to describe a subset of A , denoted by $\{a \in A \mid P(a)\}$, the subset of elements of A for which the statement $P(a)$ is true. In certain cases this subset is the whole of A ; the statement that this occurs is a *universal statement*.

Definition 7.1.1 The notation $\boxed{\forall a \in A, P(a)}$ is an alternative way of writing

$$\{ a \in A \mid P(a) \} = A.$$

It is read: ‘for each element a in the set A the proposition $P(a)$ is true’ or ‘ $P(a)$ is true for each a in the set A ’.

In this notation, the comma between ‘ $\forall a \in A$ ’ and the predicate ‘ $P(a)$ ’ is included simply to clarify the expression. Sometimes brackets are used. The symbol ‘ \forall ’ is called the *universal quantifier symbol* and is read ‘for each’, ‘for every’, ‘for all’ or ‘for any’. In this book we will adopt the practice of putting quantifiers before the predicates to which they refer. However, we will usually write these statements in words and in this case show more flexibility about the order.

As an example consider Proposition 3.1.4 which asserts that $a^2 > 0$ for any non-zero real number a . This is a statement about the set of non-zero real numbers, $\mathbb{R} - \{0\}$. The predicate is ‘ $a^2 > 0$ ’. We may write the statement in symbols as

$$\forall a \in \mathbb{R} - \{0\}, a^2 > 0$$

or equivalently

$$\{ a \in \mathbb{R} - \{0\} \mid a^2 > 0 \} = \mathbb{R} - \{0\}.$$

A third way of writing the statement is as the universal implication

$$a \in \mathbb{R} - \{0\} \Rightarrow a^2 > 0$$

and if you look back to Chapter 3 you will see that this is how we proved the statement.

Notice that in all three of these expressions a is a ‘dummy’ or ‘bound’ variable and can be changed to any other symbol without changing the meaning. For example

$$\forall x \in \mathbb{R} - \{0\}, x^2 > 0$$

is equivalent to the above statements.

7.2 Existential statements

We now turn to the negation of a universal statement: the statement that it is false. In Chapter 2 we considered the statement $x > 0 \not\Rightarrow x \geq 1$ for real numbers x and explained that this meant that the universal

statement $x > 0 \Rightarrow x \geq 1$, which is shorthand for the statement $\forall x \in \mathbb{R} (x > 0 \Rightarrow x \geq 1)$, is false. Table 2.1.2 described the behaviour for different values of x and of course, for any x such that $0 < x < 1$, $x > 0$ is true and $x \geq 1$ is false so that $x > 0 \Rightarrow x \geq 1$ is false. However, to demonstrate that $\forall x \in \mathbb{R} (x > 0 \Rightarrow x \geq 1)$ is false we simply have to show that there is a single value of $x \in \mathbb{R}$ for which $x > 0 \Rightarrow x \geq 1$ is false, i.e. $x > 0$ and $x \not\geq 1$, in other words the set $\{x \in \mathbb{R} \mid x > 0 \text{ and } x \not\geq 1\}$ is non-empty. The simplest way to do this is to give a specific element in the set, such as $1/2$: $1/2 > 0$ and $1/2 \not\geq 1$. Such a statement, that the subset defined by a predicate is non-empty, is called an *existential statement*.

Definition 7.2.1 The notation $\boxed{\exists a \in A, P(a)}$ is an alternative way of writing

$$\{a \in A \mid P(a)\} \neq \emptyset.$$

It is read: ‘for some element a in the set A the proposition $P(a)$ is true’ or ‘ $P(a)$ is true for some a in the set A ’.

The symbol ‘ \exists ’ is called the *existential quantifier symbol* and is read ‘for some’, ‘for at least one’ or sometimes ‘there exists ... such that’.

Remarks 7.2.2 Notice that the word ‘any’ sometimes indicates a universal statement and sometimes an existential statement.

The normal meaning of ‘any’ is ‘every’ as in ‘ $a^2 \geq 0$ for any real number a ’. This is a universal statement which can be written symbolically as ‘ $\forall a \in \mathbb{R}, a^2 \geq 0$ ’. However, in negative or interrogative statements ‘any’ is used idiomatically to mean ‘some’. For example, ‘There is not any real real number a such that $a^2 < 0$ ’ is asserting that the existential statement ‘ $\exists a \in \mathbb{R}, a^2 < 0$ ’ is false. And ‘Is there any real number a such that $a^2 = 2$?’ is asking whether the existential statement ‘ $\exists a \in \mathbb{R}, a^2 = 2$ ’ is true.

Fowler† gives some non-mathematical examples: ‘Have you any bananas?’ with the possible answers ‘No we haven’t any bananas’ and ‘Yes we have some bananas’.

Real care is required with questions involving ‘any’. ‘Is there any integer a such that $a \geq 1$?’ seems clear enough and is asking whether ‘ $\exists a \in \mathbb{Z}, a \geq 1$ ’ is true. But ‘Is $a \geq 1$ for any integer a ?’ seems less clear

† H.W. Fowler, *A dictionary of modern English usage* (revised by Ernest Gowers), Oxford University Press, Second edition 1968.

to me and might be taken to asking about the same statement as the first question, ' $\exists a \in \mathbb{Z}, a \geq 1$ ' (which is true) but might also be taken to be asking about ' $\forall a \in \mathbb{Z}, a \geq 1$ ' (which is false). Great care is needed in using 'for any' in interrogative statements.

7.3 Proving statements involving quantifiers

An enormous number of results in advanced mathematics take the form of asserting the truth or falsehood of some universal or existential statement; this is one of the factors which distinguishes advanced from elementary mathematics and many of the results in this book take this form. This section provides an overview of the main methods of proof but in effect much of the whole book is about proving such results.

(a) *Proving statements of the form $\forall a \in A, P(a)$*

We usually prove statements of this form by rewriting them in the form

$$a \in A \Rightarrow P(a).$$

An example of this is the proof of Proposition 3.1.4 which we have already discussed.

(b) *Proving statements of the form $\exists a \in A, P(a)$*

We often prove statements of this form by simply exhibiting a particular element $a \in A$ for which $P(a)$ is true. This is *proof by example*.

Example 7.3.1 To prove $\exists n \in \mathbb{Z}, n^2 = 9$.

Solution Observe that $3 \in \mathbb{Z}$ and $3^2 = 9$ and so $n = 3$ provides an example proving this statement. \square

There are, however, less direct methods of proving existential statements such as the use of the counting arguments which will be considered in Chapter 11.

(c) *Proving statements involving both quantifiers*

Very many statements involve both quantifiers. Consider the result of Exercise 3.3.

Proposition 7.3.2 *For integers n , if n is even then n^2 is even.*

This is a universal implication: $\forall n \in \mathbb{Z} (n \text{ is even} \Rightarrow n^2 \text{ is even})$. However, the hypothesis that n is even is an existence statement, which may be written $\exists q \in \mathbb{Z}, n = 2q$. We can use this by making use of some specific integer q such that $n = 2q$. Thus we begin the proof of this result, by the direct method, as follows.

Suppose that n is an even integer. Then $n = 2q$ for some integer q .

The conclusion which we are aiming for is the statement that n^2 is even, which may be written, again spelling out the definition, $\exists q \in \mathbb{Z}, n^2 = 2q$. Recall that in such statements the symbol ‘ q ’ is a dummy variable and its only rôle is to glue the notation together: in words we could write this as ‘ n^2 is twice some integer.’ We could replace q by any other symbol not already in use, for example $\exists p \in \mathbb{Z}, n^2 = 2p$. Indeed in this case we ought to do this since the symbol q is already in use: when we wrote ‘Then $n = 2q$ for some integer q ’ we were using q to denote some specific integer with the property that $n = 2q$. It is only by doing this that we can make use of the existence statement. We can now proceed to find an integer p such that $n^2 = 2p$ and complete the proof as follows.

Therefore $n^2 = (2q)^2 = 4q^2 = 2(2q^2)$ and so, since $2q^2$ is an integer, n^2 is even.

Hence, if n is even, then n^2 is even.

This is actually written out without reference to ‘ p ’ although we could have said ‘ $n^2 = 2p$ where $p = 2q^2$ is an integer and so n^2 is even.’

There is a genuine ambiguity about the statement ‘ $n = 2q$ for some $q \in \mathbb{Z}$ ’. It may be the existential statement that the integer q exists and this is what is meant by the statement $\exists q \in \mathbb{Z}, n = 2q$. Alternatively, it may be the statement that q is a specific integer such that $n = 2q$ as occurs in this proof. The statement with the second meaning is possible because of the statement with the first meaning, and we could make this clear by writing out the proof as follows.

Suppose that n is even. Then $\exists q \in \mathbb{Z}, n = 2q$. So let q_1 be an integer such that $n = 2q_1$. Then $n^2 = (2q_1)^2 = 2(2q_1^2)$. Hence, since $2q_1^2$ is an integer, $\exists p \in \mathbb{Z}, n^2 = 2p$. Thus n^2 is even.

Hence, if n is even then n^2 is even.

In practice this distinction is blurred and I would encourage the reader not to worry about it – it is a case where ambiguity is better than

pedantry. Most problems are avoided so long as a different dummy variable is used each time a definition involving a quantifier is used in the proof.

7.4 Disproving statements involving quantifiers

The idea of disproving statements can appear a little strange at first, but to some extent this is a matter of presentation: disproving ' P ' is the same as proving 'not P '.

(a) *Disproving statements of the form $\forall a \in A, P(a)$*

We have already observed that the negation of this statement is the statement

$$\exists a \in A, \text{not } P(a)$$

and so we can disprove it by giving a single example for which it is false. This is called *disproof by counterexample* to $P(a)$.

Example 7.4.1 To disprove the statement $\forall x \in \mathbb{R}, x^2 > 2$.

Solution A counterexample is provided by $x = 1$ since $1 \in \mathbb{R}$ and $1^2 = 1 \leqslant 2$. \square

Great care is required in interpreting negatives of universal statements in everyday speech. For example consider the statement 'All the members of the class are not here' which would normally be taken to be the negative of the universal statement 'All the members of the class are here', in other words 'Some member of the class is not here.' This differs from our careful usage. Consider a mathematical statement of the same structure: 'All the numbers in the set are not even.' This must mean the same as 'All the numbers in the set are odd' since 'odd' means the same as 'not even'. But the everyday usage indicated above would give 'Some number in the set is odd.' Take care to use language forms which are not open to misunderstanding: if we wish to indicate an absence from a class then we should say 'Not all the members of the class are here.' But then, away from mathematics, one can have a lot of fun with ambiguity!

(b) *Disproving statements of the form $\exists a \in A, P(a)$*

The negation of this statement, often written

$$\exists a \in A, P(a),$$

is the statement

$$\forall a \in A, \text{not } P(a)$$

and this gives one way of disproving the statement. We made use of this fact in the proof of Proposition 2.2.4. Here is another very simple and familiar example.

Proposition 7.4.2 *There does not exist a real number x such that $x^2 = -1$.*

Proof We know that, for all $x \in \mathbb{R}$, we have the inequality $x^2 \geq 0$ and so $x^2 \neq -1$. Hence there does not exist $x \in \mathbb{R}$ such that $x^2 = -1$. \square

The other way of disproving an existence statement is by contradiction. Here we show that the statement $P(a)$ where $a \in A$ necessarily leads to a contradiction. Proposition 4.1.1 which is a non-existence statement was proved using this method.

7.5 Proof by induction

We can reformulate the method of proof by induction using the language of set theory. Recall from Chapter 5 that induction is used to prove statements of the form $\forall n \in \mathbb{Z}^+, P(n)$. Such a statement can be rewritten as $\{n \in \mathbb{Z}^+ \mid P(n)\} = \mathbb{Z}^+$. Thus induction can be thought of as a method for proving that certain subsets of \mathbb{Z}^+ , the set of positive integers, are in fact the whole set. From this point of view we can express the induction principle (Axiom 5.1.1) as follows.

Axiom 7.5.1 (The induction principle reformulated) *Suppose that A is a subset of \mathbb{Z}^+ , the set of positive integers. Then $A = \mathbb{Z}^+$ if*

- (i) $1 \in A$, and
- (ii) $\forall k \in \mathbb{Z}^+ (k \in A \Rightarrow k + 1 \in A)$.

This statement reduces to Axiom 5.1.1 if we put $A = \{n \in \mathbb{Z}^+ \mid P(n)\}$. It can be deduced from Axiom 5.1.1 if we write $P(n)$ for the predicate $n \in A$.

Induction is quite often formulated in this more formal way.

7.6 Predicates involving more than one free variable

We have already met a number of universal and existential statements involving more than one variable. If $P(a, b)$ is a predicate involving two free variables $a \in A$ and $b \in B$ then we can form propositions involving quantifiers as follows.

- (i) $\forall a \in A, \forall b \in B, P(a, b).$
- (ii) $\exists a \in A, \exists b \in B, P(a, b).$
- (iii) $\forall a \in A, \exists b \in B, P(a, b).$
- (iv) $\exists b \in B, \forall a \in A, P(a, b).$
- (v) $\forall b \in B, \exists a \in A, P(a, b).$
- (vi) $\exists a \in A, \forall b \in B, P(a, b).$

The meaning of the first two of these is fairly clear. Examples of these which we have already met are as follows.

Proposition 3.1.1 $\forall a, b \in \mathbb{R}^+, a < b \Rightarrow a^2 < b^2.$

Proposition 3.2.1 $\forall a, b \in \mathbb{R}, a < b \Rightarrow 4ab < (a + b)^2.$

Proposition 4.1.1 *It is not true that $\exists m, n \in \mathbb{Z}, 14m + 20n = 101.$*

Notice in these examples that ' $\forall a, b \in A$ ' is a shorthand for ' $\forall a \in A, \forall b \in A$ ' and similarly for ' \exists '.

Statements involving both quantifiers require some care in particular regarding the order of the quantifiers. Consider for example the predicate ' $m < n$ ' involving positive integers m and n .

Example 7.6.1 $\forall m \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+, m < n.$

This is the statement that $\{m \in \mathbb{Z}^+ \mid \exists n \in \mathbb{Z}^+, m < n\} = \mathbb{Z}^+$ or that $m \in \mathbb{Z}^+ \Rightarrow (\exists n \in \mathbb{Z}^+, m < n)$. Notice how the use of the single quantifier ' $\exists n \in \mathbb{Z}^+$ ' leads to a predicate ' $\exists n \in \mathbb{Z}^+, m < n$ ' with a single free variable m . We can then consider for which values of m this predicate is true. In this case we are considering the assertion that it holds for all positive integers m . This means that for each positive integer m , there exists a greater integer n . This is clearly the case and we can prove it by example: take $n = m + 1$. We can write out a formal proof as follows.

Proof This result is true because, given a positive integer m , if we put $n = m + 1$ then n is a positive integer and $m < n$. \square

Example 7.6.2 $\exists n \in \mathbb{Z}^+, \forall m \in \mathbb{Z}^+, m < n.$

This is the statement that the set $\{n \in \mathbb{Z}^+ \mid \forall m \in \mathbb{Z}^+, m < n\}$ is non-empty. For a positive integer n to be in this set we must have $\forall m \in \mathbb{Z}^+, m < n$, in other words it must be greater than all positive integers. But it certainly isn't greater than n itself and so we can disprove the statement $\forall m \in \mathbb{Z}^+, m < n$ by the counterexample $m = n$. Writing this out formally gives the following.

Proof This result is false because, for each positive integer n , if we put $m = n$ then m is a positive integer and $m \not< n$ so that $m = n$ provides a counterexample to the statement $\forall m \in \mathbb{Z}^+, m < n$ which is therefore false. \square

Alternatively, the proof might be written more briefly as follows leaving the reader to sort out the quantifiers.

Proof This result is false because, for each positive integer n , if we put $m = n$ then m is a positive integer and $m \not< n$. \square

Example 7.6.3 $\forall n \in \mathbb{Z}^+, \exists m \in \mathbb{Z}^+, m < n.$

Let us consider the set $\{n \in \mathbb{Z}^+ \mid \exists m \in \mathbb{Z}^+, m < n\}$. This is the set of positive integers which are strictly greater than some other positive integer. If $n > 1$ then n does lie in this set since we can take $m = n - 1$ but on the other hand 1 is not an element of this set since $\forall m \in \mathbb{Z}^+, m \geq 1$. Hence $\{n \in \mathbb{Z}^+ \mid \exists m \in \mathbb{Z}^+, m < n\} = \mathbb{Z}^+ - \{1\}$. Since 1 does not lie in this set the universal statement is false. All we need say is the following.

Proof This statement is false and a counterexample is $n = 1$ since $m \not< 1$ for all positive integers m . \square

Example 7.6.4 $\exists m \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+, m < n.$

This is the statement that the set $\{m \in \mathbb{Z}^+ \mid \forall n \in \mathbb{Z}^+, m < n\}$ is non-empty. For a positive integer m to be in this set we must have $\forall n \in \mathbb{Z}^+, m < n$, in other words it must be smaller than all positive integers. But it certainly isn't smaller than itself and so we can disprove the statement $\forall n \in \mathbb{Z}^+, m < n$ by the counterexample $n = m$. Writing this out formally gives the following.

Proof This result is false because, for each positive integer m , if we put $n = m$ then n is a positive integer and $m \not< n$ so that $n = m$ provides a counterexample to the statement $\forall n \in \mathbb{Z}^+, m < n$ which is therefore false. \square

The alternative more usual briefer form is as follows.

Proof This result is false because, for each positive integer m , if we put $n = m$ then n is a positive integer and $m \not< n$. \square

The reader should carefully compare the proofs in Example 7.6.2 and Example 7.6.4. Although in both cases the implication used is that if $m = n$ then $m \not< n$, in the first example we start from a general positive integer n and then define m by $m = n$, whereas in the second example we start from a general positive integer m and then define n by $n = m$. The distinction may be clarified when the reader does Exercise 7.2.

7.7 The Cartesian product of two sets

At the beginning of this chapter we introduced quantifiers in terms of properties of the subset defined by a predicate involving one free variable. Predicates involving more than one free variable also define subsets – of a set known as the Cartesian product. For simplicity we restrict attention to the case of two free variables.

Definition 7.7.1 Given sets X and Y , the Cartesian product of X and Y , denoted by $X \times Y$, is the set of all ordered pairs (x, y) where $x \in X$ and $y \in Y$. Thus

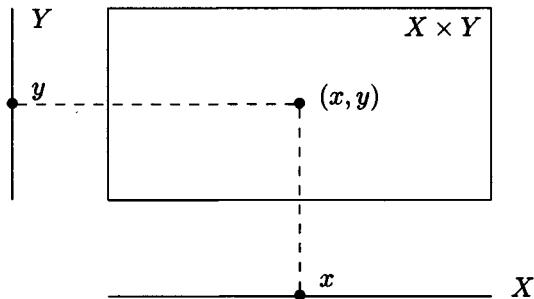
$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

In referring to an ordered pair in this definition we mean that two such pairs, (x_1, y_1) and (x_2, y_2) , are equal, $(x_1, y_1) = (x_2, y_2)$, if and only if $x_1 = x_2$ and $y_1 = y_2$. We say that the ordered pair (x, y) has coordinates x and y .

When $Y = X$ we write $X \times X = X^2$.

We can picture points in the Cartesian product as follows using lines to represent the sets X and Y and a rectangle to represent $X \times Y$. It is

customary to use a horizontal line to denote the first set and a vertical line to denote the second set.



Examples 7.7.2 (a) For $X = \{a, b, c\}$ and $Y = \{a, b\}$,

$$X \times Y = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b)\}$$

and

$$Y \times X = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c)\}.$$

Notice that these two sets are different.

(b) $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the familiar 2-dimensional Euclidean plane.

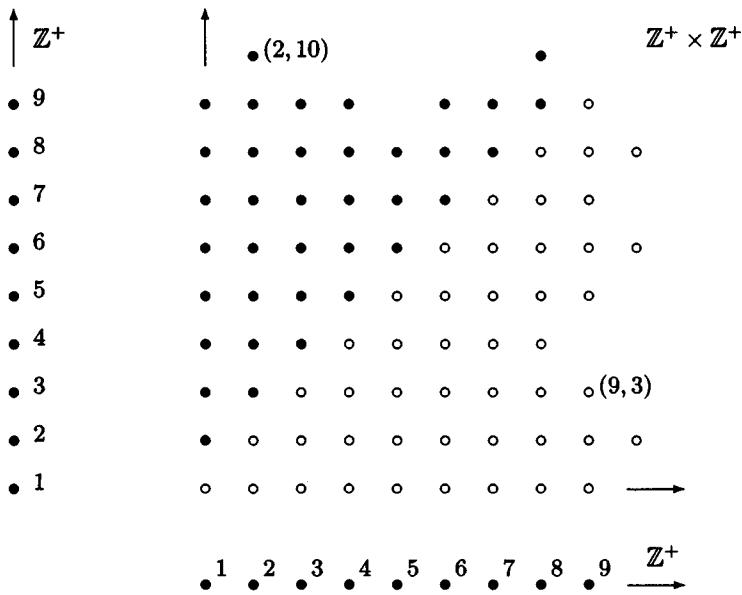
Now given a predicate $P(a, b)$ involving free variables $a \in A$ and $b \in B$, we can define the subset $\{(a, b) \in A \times B \mid P(a, b)\}$ of the Cartesian product. This is familiar in \mathbb{R}^2 from the study of plane curves using the methods of Cartesian geometry; we can describe certain subsets of \mathbb{R}^2 by giving an *equation*. For example we say that the circle with centre $(0, 0)$ and radius 1 has equation $x^2 + y^2 = 1$ to mean that the set of points in \mathbb{R}^2 which lie on this circle is given by $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$.

Example 7.7.3 To illustrate the relationship between universal and existential statements involving a predicate with two free variables and the subset defined by the predicate we look again at the examples considered in the previous section. We can draw part of the picture of the subset

$$\{(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid m < n\} \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$$

as in the diagram on the next page.

Here the solid dots (\bullet) indicate the elements of the Cartesian product for which the predicate $m < n$ is true and the circles (\circ) those for which



it is false. Thus $(2, 10)$ is in the subset determined by the predicate whereas $(9, 3)$ is not.

We now consider each example in turn.

Example 7.6.1 $\forall m \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+, m < n$. This is true because each vertical line of elements in the Cartesian product contains an element in the subset, for example $\{m\} \times \mathbb{Z}^+$, the vertical line of points whose first coordinate is m , contains the point $(m, m + 1)$.

Example 7.6.2 $\exists n \in \mathbb{Z}^+, \forall m \in \mathbb{Z}^+, m < n$. This is false because no horizontal line lies entirely in the subset, for example $\mathbb{Z}^+ \times \{n\}$, the horizontal line of points whose second coordinate is n , contains the point (n, n) which does not lie in the subset.

Example 7.6.3 $\forall n \in \mathbb{Z}^+, \exists m \in \mathbb{Z}^+, m < n$. This is false because there is a horizontal line containing no elements of the subset, namely the line $\mathbb{Z}^+ \times \{1\}$.

Example 7.6.4 $\exists m \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+, m < n$. This is false because each vertical line contains a point not in the subset, for example $\{m\} \times \mathbb{Z}^+$ contains the point (m, m) .

To conclude this chapter here are some standard results relating the Cartesian product to union and intersection.

Proposition 7.7.4 *For all sets A , B , C and D the following hold:*

- (i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- (ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
- (iii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;
- (iv) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

These statements may be proved directly from the definitions. As an illustration here is a proof of part (ii). (Part (iv) appears as Exercise 7.7 and part (iii) appears in Problems II, Question 13.)

Proof of part (ii) A proof that two sets are equal requires us to prove two set inclusions. In this case we can do them together as follows.

$$\begin{aligned} (x, y) \in A \times (B \cap C) &\Leftrightarrow x \in A \text{ and } y \in B \cap C \\ &\Leftrightarrow x \in A \text{ and } y \in B \text{ and } y \in C \\ &\Leftrightarrow (x, y) \in A \times B \text{ and } (x, y) \in A \times C \\ &\Leftrightarrow (x, y) \in (A \times B) \cap (A \times C). \end{aligned}$$

Thus $(x, y) \in A \times (B \cap C) \Leftrightarrow (x, y) \in (A \times B) \cap (A \times C)$ as required. \square

Exercises

7.1 Determine the following sets:

- (i) $\{ m \in \mathbb{Z}^+ \mid \exists n \in \mathbb{Z}^+, m \leq n \}$,
- (ii) $\{ m \in \mathbb{Z}^+ \mid \forall n \in \mathbb{Z}^+, m \leq n \}$,
- (iii) $\{ n \in \mathbb{Z}^+ \mid \exists m \in \mathbb{Z}^+, m \leq n \}$,
- (iv) $\{ n \in \mathbb{Z}^+ \mid \forall m \in \mathbb{Z}^+, m \leq n \}$.

7.2 Prove or disprove the following statements.

- (i) $\forall m, n \in \mathbb{Z}^+, m \leq n$.
- (ii) $\exists m, n \in \mathbb{Z}^+, m \leq n$.
- (iii) $\forall m \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+, m \leq n$.
- (iv) $\exists m \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+, m \leq n$.
- (v) $\forall n \in \mathbb{Z}^+, \exists m \in \mathbb{Z}^+, m \leq n$.
- (vi) $\exists n \in \mathbb{Z}^+, \forall m \in \mathbb{Z}^+, m \leq n$.

7.3 Prove or disprove the following statements.

- (i) $\forall m, n \in \mathbb{Z}, m \leq n.$
- (ii) $\exists m, n \in \mathbb{Z}, m \leq n.$
- (iii) $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}, m \leq n.$
- (iv) $\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, m \leq n.$
- (v) $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m \leq n.$
- (vi) $\exists n \in \mathbb{Z}, \forall m \in \mathbb{Z}, m \leq n.$

7.4 Prove or disprove each of the following statements.

- (i) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0.$
- (ii) $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x + y = 0.$
- (iii) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy = 0.$
- (iv) $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, xy = 0.$
- (v) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy = 1.$
- (vi) $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, xy = 1.$
- (vii) $\forall n \in \mathbb{Z}^+, (n \text{ is even or } n \text{ is odd}).$
- (viii) $(\forall n \in \mathbb{Z}^+, n \text{ is even}) \text{ or } (\forall n \in \mathbb{Z}^+, n \text{ is odd}).$

7.5 Prove the following:

$$(\exists q \in \mathbb{Z}, n = 2q + 1) \Rightarrow (\exists p \in \mathbb{Z}, n^2 = 2p + 1).$$

7.6 Write the following universal statement in terms of quantifiers and prove it.

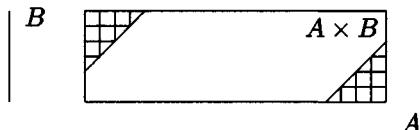
For integers a and b , if a and b are even then so is $a + b$.

7.7 For sets A, B, C and D prove that

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D),$$

and give an example to show that these sets are not always equal.

7.8 Suppose that the set $\{(a, b) \mid P(a, b)\}$ is given by the triangular regions in the diagram below.



Decide whether each of the following statements is true or false.

- (i) $\forall a \in A, \exists b \in B, P(a, b).$
- (ii) $\exists b \in B, \forall a \in A, P(a, b).$
- (iii) $\forall b \in B, \exists a \in A, P(a, b).$
- (iv) $\exists a \in A, \forall b \in B, P(a, b).$

7.9 Find a reformulation of Axiom 5.4.1 (the strong induction principle) as a method of proving that subsets of \mathbb{Z}^+ are the whole set (similar to Axiom 7.5.1).

8

Functions

The notion of *function* is one of the most fundamental in mathematics. It is probably familiar to the reader in the context of calculus, and it is here that the concept was first clarified and the difference between a function and a formula properly understood in the early years of the nineteenth century. Today, the language of functions is used throughout mathematics.

In this chapter the function concept is introduced. We discuss various ways of defining a function and consider the graph of a function.

8.1 Functions and formulae

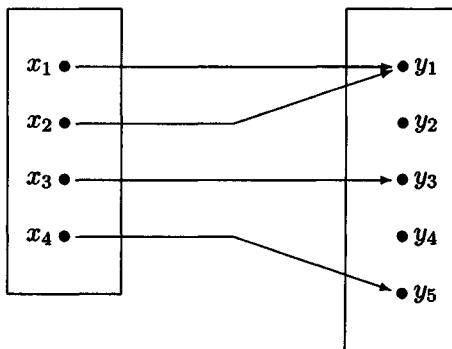
Definition 8.1.1 Suppose that X and Y are sets. A function, map or mapping from the set X to the set Y is the assignment of a unique element of Y to each element of X . If f is a function from X to Y we write $f: X \rightarrow Y$ and denote the element of Y assigned to an element $x \in X$ by $f(x)$ writing $x \mapsto f(x)$. The element $f(x) \in Y$ is called the value of f at $x \in X$ or the image of x under f . The set X is called the domain of the function f and the set Y is called the codomain.

Example 8.1.2 The most basic way of describing a function is by listing the values. For example, given $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4, y_5\}$, the following table determines a function $f: X \rightarrow Y$.

x	x_1	x_2	x_3	x_4
$f(x)$	y_1	y_1	y_3	y_5

We determine the value of the function at an element of X by locating that element in the first row and reading down to the second row. Notice that each element of the domain X occurs precisely once in the first row so that this is a well-defined procedure. On the other hand elements of the codomain Y may occur once in the second row, but they may also occur more than once or not at all: an element of the codomain may be the value of the function at several elements of the domain or may not be a value at all.

We can picture this function as follows.



Here we find the value of f at an element of the domain X by following the arrow which begins at that element. Each element of the domain lies at the beginning of just one arrow so this is a well-defined procedure. However, elements in the codomain may lie at the end of one arrow, several arrows or no arrow at all.

Yet another way of describing a function is as follows. Think of the elements of the codomain set as boxes. The function describes how to place the objects of the domain set in these boxes. Thus the function under consideration would be pictured as follows.

y_1	y_2	y_3	y_4	y_5
x_1 x_2		x_3		x_4

Again notice that each element of the domain set occurs precisely once

in the picture. However, any given box, corresponding to an element of the codomain, may contain one object, several objects or none at all.

The reader may wonder at this variety of ways of thinking about a function. It is important to realize that mathematicians develop a variety of ways of thinking about the rather abstract concepts they deal with. Any given way may suit one person better than another and each leads to different insights: it can be useful to be aware of several.

Example 8.1.3 Suppose that $X = \{a, b, c\}$ and $Y = \{d, e\}$. Then there are precisely eight functions from the set X to the set Y given as follows.

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$
a	d	d	d	d	e	e	e	e
b	d	d	e	e	d	d	e	e
c	d	e	d	e	d	e	d	e

Here the functions f_1 and f_8 are examples of *constant functions*. Given sets X and Y and any element $y_0 \in Y$ there is a *constant function* $c_{y_0}: X \rightarrow Y$ given by $c_{y_0}(x) = y_0$ for all $x \in X$.

Of course a function can have the same set as domain and codomain as in the next example.

Example 8.1.4 Suppose that $Z = \{a, b\}$. Then there are precisely four functions from Z to Z as follows.

x	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$
a	a	a	b	b
b	a	b	a	b

In this case the functions g_1 and g_4 are constant functions. The function g_2 is an example of an *identity function*. Given a set X , the *identity function* on X , $I_X: X \rightarrow X$, is given by $I_X(x) = x$ for all $x \in X$.

Describing a function by listing the values is only practical when the domain set is small and impossible if the domain set is infinite. The most common way of describing a function f is by giving a *formula* for f which provides a procedure for finding the value of the function at each element of the domain. When defining a function using a formula it is important to be clear about which sets are the domain and the codomain of the function.

Example 8.1.5 Recall that $\mathbb{R}^{\geq 0}$ denotes the subset of \mathbb{R} , the set of real numbers, given by $\{x \in \mathbb{R} \mid x \geq 0\}$. Consider the following four functions:

- (i) $f_1: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_1(x) = x^2$;
- (ii) $f_2: \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}$ given by $f_2(x) = x^2$;
- (iii) $f_3: \mathbb{R} \rightarrow \mathbb{R}^{\geq 0}$ given by $f_3(x) = x^2$;
- (iv) $f_4: \mathbb{R}^{\geq 0} \rightarrow \mathbb{R}^{\geq 0}$ given by $f_4(x) = x^2$.

Notice that, although the formula $f_i(x) = x^2$ is the same for each of these four functions, they are considered to be four distinct functions since the domain and codomain are part of the definition of the function. We will see later that these four functions have different properties even though they are given by the same formula.

We need to take care that the formula makes sense for each element of the domain.

Example 8.1.6 The formula $f_1(x) = \frac{x^2 + x - 2}{x - 1}$ does not define a function $\mathbb{R} \rightarrow \mathbb{R}$ since it gives no value for $x = 1$. When working with the set of real numbers it is quite common not to specify the domain and codomain of a function given by a formula. The convention is that, if these are not specified, then we take as the domain the subset of \mathbb{R} consisting of the numbers for which the formula makes sense and we take \mathbb{R} as the codomain. Using this convention the above formula for f_1 defines a function $f_1: \mathbb{R} - \{1\} \rightarrow \mathbb{R}$.

If we really want a function with domain \mathbb{R} then in an example like this there are two basic techniques for extending f_1 .

Rewriting the formula: We can rewrite the formula in such a way that it makes sense for all real numbers x using

$$(x^2 + x - 2)/(x - 1) = (x - 1)(x + 2)/(x - 1) = x + 2$$

for $x \neq 1$. Then $f_2(x) = x + 2$ does define a function on \mathbb{R} , i.e. with domain \mathbb{R} , extending the function f_1 .

Explicit definition: Alternatively we can explicitly specify the value of the function at the element 1 where the formula for f_1 does not work. Thus

$$f_3(x) = \begin{cases} \frac{x^2 + x - 2}{x - 1} & \text{if } x \neq 1, \\ 3 & \text{if } x = 1, \end{cases}$$

defines a function $f_3: \mathbb{R} \rightarrow \mathbb{R}$.

Notice that we may specify the values at individual points any way we like. It doesn't have to relate in a sensible way to the values elsewhere. In defining $f_3(1)$ we selected that value given by the formula $x + 2$ so that f_2 and f_3 are in fact the same function. However, we could extend the function f_1 to the whole of \mathbb{R} in a different way. For example

$$f_4(x) = \begin{cases} \frac{x^2 + x - 2}{x - 1} & \text{if } x \neq 1, \\ 42 & \text{if } x = 1, \end{cases}$$

is another way of extending the function f_1 to the whole of \mathbb{R} .

Example 8.1.7 In some cases, for example $x \mapsto 1/x$, there appears to be no way of rewriting the formula to include in the domain of definition points where it gives no value (in this case $x = 0$). But in these cases we can still use the second method. For example

$$g(x) = \begin{cases} 1/x & \text{if } x \neq 0, \\ 73 & \text{if } x = 0, \end{cases}$$

is a perfectly respectable function $g: \mathbb{R} \rightarrow \mathbb{R}$.

We can use different formulae for different parts of the domain as in the following example.

Example 8.1.8 The *modulus function* $x \mapsto |x|$ is defined on \mathbb{R} by

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

Notice here that the value of the function at 0 is given twice, since $0 \geq 0$ and $0 \leq 0$. This isn't a problem since the two formulae ($x \mapsto x$ and $x \mapsto -x$) give the same value (namely 0) for $x = 0$. But when specifying a function in this way we do need to be careful to check that it is *well-defined* (i.e. there is a uniquely specified value) at each point.

Definition 8.1.9 Two functions $f: X \rightarrow Y$ and $g: X \rightarrow Y$ are equal, written $f = g$, when they have the same value at each point of the domain X , i.e. $f(x) = g(x)$ for all $x \in X$. Notice that it is implicit in this definition that two equal functions have the same domain and the same codomain.

Example 8.1.10 The functions f_2 and f_3 of Example 8.1.6 are equal even though they are defined in different ways. Thus it is not the process leading to the values which determines the function but what the values are. Of course, in defining f_3 the value of $f_3(1)$ was selected precisely so that they would be equal.

We have seen in Example 8.1.6 how to extend the domain of a function. We can also make the domain smaller.

Definition 8.1.11 Suppose that $f: X \rightarrow Y$ is a function and A is a subset of X , i.e. $A \subseteq X$. Then we can define a function $g: A \rightarrow Y$ by $g(a) = f(a)$ for all $a \in A$. This function is called the restriction of f to A and is denoted by $f|A$.

Examples 8.1.12 (a) In Example 8.1.3 $f_1|\{a, b\} = f_2|\{a, b\}$ and is the constant function taking the value d .

(b) In Example 8.1.5 $f_2 = f_1|\mathbb{R}^{\geq}$ and $f_4 = f_3|\mathbb{R}^{\geq}$.

(c) In Example 8.1.6 $f_2|(\mathbb{R} - \{1\}) = f_4|(\mathbb{R} - \{1\}) = f_1$.

8.2 Composition of functions

Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$. Then, given an element $x \in X$, the function f assigns to it an element $y = f(x) \in Y$ and now the function g assigns to this an element $g(y) = g(f(x)) \in Z$. Thus using f and g an element of Z has been assigned to x . This process defines a function with domain X and codomain Z called the composite of f and g .

Definition 8.2.1 Given two functions $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ the composite of f and g , denoted by $g \circ f: X \rightarrow Z$ or simply $gf: X \rightarrow Z$, is defined by

$$g \circ f(x) = g(f(x)) \quad \text{for all } x \in X.$$

The order of the f and g in this definition should be carefully noted. Since we have adopted the convention (usual† in most areas of mathematics) of writing the symbol for the function on the left of the element

† But not used universally. In some branches of algebra it is quite common to write the value $f(x)$ as xf or even x^f .

where it is being evaluated (viz. $f(x)$) it is natural to denote the function obtained by applying f and then applying g by the symbol $g \circ f$ which presents them (from left to right) in the opposite order to their application. We can write the following to indicate this:

$$g \circ f: X \xrightarrow{f} Y \xrightarrow{g} Z.$$

Examples 8.2.2 (a) The function $x \mapsto (x + 1)^2$ from \mathbb{R} to \mathbb{R} is the composite of the function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x + 1$ and the function $g: \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = x^2$ because

$$g \circ f(x) = g(f(x)) = (x + 1)^2 \quad \text{for all } x \in X.$$

Notice that the order does matter here because

$$f \circ g(x) = f(g(x)) = x^2 + 1;$$

composition of functions is not in general *commutative*. It is not usually a good idea to refer simply to ‘the composite of f and g ’ when both orders are possible since there is no well-established convention about which order these words indicate. It is best to use the symbolism $g \circ f$ or $f \circ g$ in order to be quite clear.

(b) Suppose that A is a subset of a set X . Then we may define a function $i: A \rightarrow X$ by $i(a) = a$ for all $a \in A$. This function is called the *inclusion function* of A into X . If now $f: X \rightarrow Y$ is a function, then the composite $f \circ i: A \rightarrow Y$ is equal to the restriction $f|_A: A \rightarrow Y$ of f to A .

(c) Suppose that $f: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = x^2 + 1$ and $g: \mathbb{R} - \{0\} \rightarrow \mathbb{R}$ is defined by $g(x) = 1/x$. Then strictly speaking the composite $g \circ f$ is not defined since the codomain of f is not the same as the domain of g .

However, every value of f lies in the domain of g since $x^2 + 1 \geq 1 > 0$ for all real numbers x so that g can be evaluated at each value of f . In a case like this we can still attach a meaning to the composite $g \circ f$ as the function given by $g \circ f(x) = g(f(x))$. This gives the function $\mathbb{R} \rightarrow \mathbb{R}$ determined by $g \circ f(x) = 1/(x^2 + 1)$.

Proposition 8.2.3 Suppose that $f: X \rightarrow Y$, $g: Y \rightarrow Z$ and $h: Z \rightarrow W$ are functions. Then

- (i) $(h \circ g) \circ f = h \circ (g \circ f): X \rightarrow Z$,
- (ii) $f \circ I_X = f = I_Y \circ f: X \rightarrow Y$.

Proof These results are proved simply by evaluating the functions. For example, given $x \in X$, both the functions in (i) assign $h(g(f(x)))$ to this element and so the functions are equal. \square

Notice that the first part of Proposition 8.2.3 means that we can write $h \circ g \circ f$ without ambiguity. Composition of functions is *associative*.

8.3 Sequences

Definition 8.3.1 A function $f : \mathbb{Z}^+ \rightarrow A$ is called a sequence in the set A .

The study of sequences in \mathbb{R} or \mathbb{C} is of great importance in advanced calculus and numerical analysis. Sequences may be defined by a formula, such as $n \mapsto n^2$, $n \mapsto 1/n$, $n \mapsto 2^n$, $n \mapsto (1 + 1/n)^n$ and $n \mapsto 1/n!$. But more interesting are those sequences defined inductively. We saw in Chapter 5 that strictly speaking formulae involving the exponent n or the factorial $n!$ really have to be defined inductively. Another example of an inductively defined sequence considered there was the Fibonacci sequence.

It is common in advanced calculus to solve numerical problems by generating a sequence of numbers x_n which provide increasingly good approximations to the solution as n increases – the sequence converges to a limit which is the required solution.[†]

One important reason for becoming adept at handling quantifiers is to be able to handle the definition of the limit of a sequence. To illustrate the ideas we introduce the idea of a null sequence, a sequence with limit 0.

Definition 8.3.2 Given a sequence $f : \mathbb{Z}^+ \rightarrow \mathbb{R}$ of real numbers, we say that the sequence is null, written $\lim f = 0$ or $\lim_{n \rightarrow \infty} f(n) = 0$, when

$$\forall \varepsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+ (n \geq N \Rightarrow |f(n)| < \varepsilon).$$

[†] A good example is the Newton–Raphson method for solving an equation, described in most books on advanced calculus (see for example G.B. Thomas and R.S. Finney, *Calculus and analytic geometry*, Addison-Wesley, Eighth edition 1992).

The use of ε for a general positive real number in this definition is traditional. This is not the place to investigate the full implications of this definition which involves *three* quantifiers! Here is a simple example of its use.

Example 8.3.3 The sequence $n \mapsto 1/\sqrt{n}$ is null.

Constructing a proof. We are required to prove that

$$\forall \varepsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+, \forall n \in \mathbb{Z}^+ (n \geq N \Rightarrow 1/\sqrt{n} < \varepsilon).$$

[Notice that $|1/\sqrt{n}| = 1/\sqrt{n}$.] So suppose we are given $\varepsilon \in \mathbb{R}^+$. Then to demonstrate the existence of the integer N we examine when $1/\sqrt{n} < \varepsilon$.

$$1/\sqrt{n} < \varepsilon \Leftrightarrow 1/n < \varepsilon^2 \Leftrightarrow n > 1/\varepsilon^2.$$

Hence so long as we choose a positive integer N such that $N > 1/\varepsilon^2$ we will have $n \geq N \Rightarrow n > 1/\varepsilon^2 \Rightarrow 1/\sqrt{n} < \varepsilon$ as required.

So for example, if $\varepsilon = 1$ then we must choose $N > 1$, if $\varepsilon = 1/2$ then we must choose $N > 4$, and if $\varepsilon = 1/100$ then $N > 10000$. The smaller the number ε the greater the number N is required to be. But whatever the positive real number ε is the condition $N > 1/\varepsilon^2$ tells us how large N has to be.

Proof Given a positive real number ε , $1/\sqrt{n} < \varepsilon$ if and only if $n > 1/\varepsilon^2$. Hence if we choose $N > 1/\varepsilon^2$ then $n \geq N$ implies that $n > 1/\varepsilon^2$ so that $1/\sqrt{n} < \varepsilon$ is required. \square

This type of proof involving multiple quantifiers is quite elaborate and this is in fact an extremely simple example. More complicated examples are not considered in this book but are dealt with in detail in books on infinite sequences and series, advanced calculus and analysis.[†]

8.4 The image of a function

Given a function $f: X \rightarrow Y$, it is not necessary that every element of Y is a value of the function. For example the function $\mathbb{R} \rightarrow \mathbb{R}$ given by $x \mapsto x^2$ does not have -1 as a value. Thus we can obtain a subset of Y by considering those elements which are values.

[†] See, for example, R. Haggerty, *Fundamentals of mathematical analysis*, Addison-Wesley, Second edition 1993.

Definition 8.4.1 Given a function $f: X \rightarrow Y$, the subset of the codomain Y consisting of those elements which are values of f is called the image of f and is denoted by Im f . Thus

$$\text{Im } f = \{ f(x) \mid x \in X \}.$$

This means that the function f provides a constructive definition of the set $\text{Im } f$, as discussed in Chapter 6.

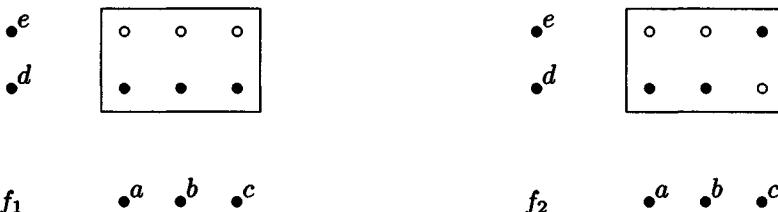
8.5 The graph of a function

Definition 8.5.1 Suppose that $f: X \rightarrow Y$ is a function. Then we define the graph of f to be the subset of the Cartesian product $X \times Y$ given by

$$G_f = \{ (x, y) \in X \times Y \mid y = f(x) \} = \{ (x, f(x)) \mid x \in X \}.$$

Remarks 8.5.2 In the case that X and Y are subsets of \mathbb{R} this is the usual idea of the graph of a function. Work in calculus makes it clear that the graph gives a great deal of information about the function and that it is useful to develop skill in drawing graphs.

Example 8.5.3 The graphs of the functions f_1 and f_2 of Example 8.1.3 are as follows.



Here we indicate the elements of the graph by solid dots (\bullet).

The graph of the function $f: X \rightarrow Y$ is a particular example of a subset of the Cartesian product $X \times Y$ determined by a predicate: the predicate is $y = f(x)$. Not every subset of $X \times Y$ arises as the graph of a function. Each column $\{x_0\} \times Y$ must contain a single element, namely

$(x_0, f(x_0))$. However, the function f is determined by its graph G_f , for, given $x_0 \in X$, there is a unique element $(x, y) = (x_0, y_0) \in G_f$ such that $x = x_0$, and then $f(x_0) = y_0$.†

Exercises

8.1 Define functions f and $g: \mathbb{R}^2 \rightarrow \mathbb{R}$ by:

$$\begin{aligned}f(x, y) &= \frac{x+y}{2} + \frac{|x-y|}{2}; \\g(x, y) &= \begin{cases} x & \text{if } x \geq y, \\ y & \text{if } x \leq y. \end{cases}\end{aligned}$$

Prove that the function g is well-defined. Prove that $f = g$.

8.2 Define functions f and $g: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = x^3$ and $g(x) = 1 - x$. Find the functions (i) $f \circ f$, (ii) $f \circ g$, (iii) $g \circ f$, (iv) $g \circ g$.

List the elements of the set $\{x \in \mathbb{R} \mid fg(x) = gf(x)\}$.

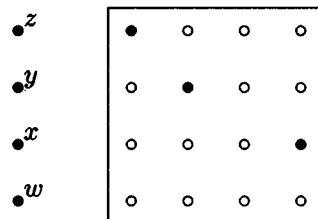
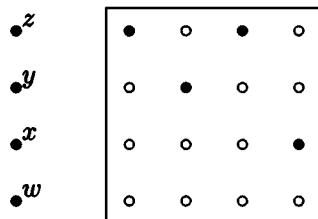
8.3 Find functions $f_i: \mathbb{R} \rightarrow \mathbb{R}$ with images as follows:

- (i) $\text{Im } f_1 = \mathbb{R}$;
- (ii) $\text{Im } f_2 = \mathbb{R}^+$;
- (iii) $\text{Im } f_3 = \mathbb{R} - \mathbb{Z}$;
- (iv) $\text{Im } f_4 = \mathbb{Z}$.

8.4 Prove that the sequence $n \mapsto 1/n$ is null.

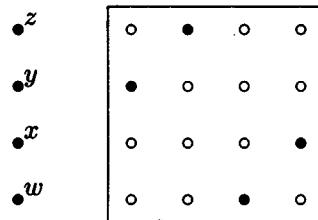
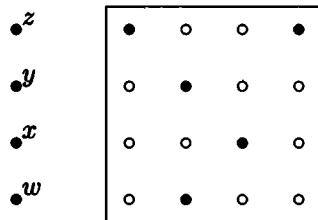
8.5 Let $X = \{a, b, c, d\}$ and $Y = \{w, x, y, z\}$. Which of the following subsets of $X \times Y$ is the graph of a function $f: X \rightarrow Y$? For those which are write down a table for the corresponding function as in Example 8.1.3. Explain why the others are not graphs of functions.

† Our definition of a function (Definition 8.1.1) is usually considered rather informal in more advanced mathematics. There a function is defined to be a graph: in other words a function $X \rightarrow Y$ is defined to be a subset of $X \times Y$ in which each element of X occurs as the first coordinate of an element precisely once (see for example Daniel J. Velleman, *How to prove it, a structured approach*, Cambridge University Press, 1994).



(i) \bullet^a \bullet^b \bullet^c \bullet^d

(ii) \bullet^a \bullet^b \bullet^c \bullet^d



(iii) \bullet^a \bullet^b \bullet^c \bullet^d

(iv) \bullet^a \bullet^b \bullet^c \bullet^d

9

Injections, surjections and bijections

In defining a function $f: X \rightarrow Y$ we insist that a unique element of Y is assigned to each element of X . However, we do not require that each element of Y is assigned to some element of X nor do we prevent the possibility of the same element of Y being assigned to several (or even all the) elements of X . By imposing additional conditions concerning the number of elements of X to which elements of Y are assigned we get functions with particular properties. In this chapter we consider functions with particularly good properties and in particular functions which are *bijections* for which we can define an inverse function.

9.1 Properties of functions

Definition 9.1.1 Suppose that $f: X \rightarrow Y$ is a function.

(i) If no element of Y is assigned to more than one element of X , i.e. the function takes a different value for each point of the domain, then we say that the function f is an **injection** (or that it is injective or one-to-one). In symbols we can write this

$$\forall x_1, x_2 \in X, (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$$

or equivalently using the contrapositive

$$\forall x_1, x_2 \in X, (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

(ii) If each element of Y is assigned to some element of X , i.e. each point of the codomain is a value of the function, then we say that the

function f is a surjection (or that it is surjective or onto). In symbols we can write this

$$\forall y \in Y, \exists x \in X, y = f(x).$$

(iii) If f is both an injection and a surjection then we say that it is a bijection (or that it is bijective or one-to-one and onto).

We can reformulate these definitions using the notion of a *pre-image*.

Definition 9.1.2 For a function $f: X \rightarrow Y$, given an element $y \in Y$ a pre-image of y (under f) is an element $x \in X$ such that $y = f(x)$.

So f is an injection if and only if every element of Y has at most one pre-image; f is a surjection if and only if every element of Y has at least one pre-image; and f is a bijection if and only if every element of Y has precisely one pre-image.

These ideas are simply expressed in terms of the various models for a function introduced in the previous chapter. If a function is described by listing the values of the function as in Example 8.1.2 then we find the pre-images of an element of the codomain by locating its occurrences in the list of values and reading up to the corresponding elements of the first row. Thus a function is injective when no element occurs more than once in the list of values, it is surjective when every element of the codomain does occur in the list of values and bijective when every element of the codomain occurs precisely once in the list of values.

In terms of the picture representing the function by arrows from the domain to the codomain (see page 90) we find pre-images by following arrows backwards. Thus, for example, a function is bijective if every point of the codomain is at the end of precisely one arrow.

Finally, if we think of a function as a procedure for placing the elements of the set X into a set of boxes Y (see page 90) then a pre-image of a particular box $y \in Y$ is simply an element which is placed in that box. From this point of view, f is injective when no two elements are placed in the same box, it is surjective when no box is left empty, and it is bijective when each box contains precisely one element.

Examples 9.1.3 (a) In Example 8.1.3 all the functions apart from the constant functions f_1 and f_8 are surjections. None of the functions are

injections.

(b) In Example 8.1.4 the non-constant functions f_2 and f_3 are bijections. Notice that, for any set X , the identity function I_X is a bijection.

(c) In Example 8.1.5 the function f_1 is neither an injection (since $(-1)^2 = 1^2 = 1$) nor a surjection (since there is no real number x such that $x^2 = -1$); the function f_2 is an injection (since $0 \leq x_1 < x_2 \Rightarrow x_1^2 < x_2^2$) but not a surjection; the function f_3 is a surjection but not an injection; and the function f_4 is a bijection. This example illustrates the importance of the domain and the codomain. For example, if a result has been proved for injections then it can be applied to f_2 and to f_4 but not to f_1 and f_3 .

Remarks 9.1.4 Notice that we can easily convert any function into a surjection by changing the codomain. Recall that, given a function $f: X \rightarrow Y$, the *image* of f , denoted by $\text{Im } f$, is the set of values of f . The assignment determining the function f also determines a function $f^+: X \rightarrow \text{Im } f$ (i.e. $f^+(x) = f(x)$) which is a surjection.

Since the definitions of injectivity and surjectivity involve universal and existential statements, proofs and disproofs of these properties usually follow the format discussed in Chapter 7.

Example 9.1.5 To determine whether the function $f_1: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_1(x) = x + 1$ is an injection, a surjection or a bijection.

For injectivity, it is usually easiest to use the second formulation:

$$f_1(x_1) = f_1(x_2) \Rightarrow x_1 = x_2.$$

Filling in the definition of the function this gives

$$x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$$

which is certainly true so that f_1 is injective.

For surjectivity, we rewrite the definition as usual as a universal implication:

$$y \in \mathbb{R} \Rightarrow \exists x \in \mathbb{R}, y = f_1(x).$$

If we put the definition of the function into this then it is easy to prove the existential statement by example. For

$$y = f_1(x) \Leftrightarrow y = x + 1 \Leftrightarrow x = y - 1$$

which tells us that, given $y \in \mathbb{R}$, then $y = f_1(x)$ if $x = y - 1$ so that y does have a pre-image under f_1 . Hence f_1 is surjective and so a bijection.

In fact, what is written above is rather inefficient; we can often prove bijectivity in one fell swoop. The best way to discover whether a function is injective or surjective can be to investigate the pre-images of a general element in the codomain using the approach used above for surjectivity. In this case if y is a general element of the codomain \mathbb{R} then

$$\begin{aligned} x \text{ is a pre-image of } y &\Leftrightarrow y = f_1(x) \\ &\Leftrightarrow y = x + 1 \\ &\Leftrightarrow x = y - 1. \end{aligned}$$

This shows that each element y of \mathbb{R} has precisely one pre-image, namely $y - 1$, so that the function is a bijection.

We can write out the solution to this problem quite briefly as follows.

Solution Since $y = f_1(x) \Leftrightarrow y = x + 1 \Leftrightarrow x = y - 1$, for $x, y \in \mathbb{R}$, we see that each element y of \mathbb{R} has precisely one pre-image under f_1 . Hence f_1 is a bijection. \square

Example 9.1.6 To determine whether the function $f_2: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ given by $f_2(x) = x + 1$ is injective, surjective or bijective.

This function is given by the same formula as the previous example. If we try the pre-image approach we get almost the same argument:

$$\begin{aligned} x \text{ is a pre-image of } y &\Leftrightarrow y = f_2(x) \\ &\Leftrightarrow y = x + 1 \\ &\Leftrightarrow x = y - 1. \end{aligned}$$

The difference becomes clear when we ask whether the formula for the pre-image makes sense. Remember that if x is to be a pre-image then it must certainly lie in the domain \mathbb{R}^+ (otherwise $f_2(x)$ isn't even defined). But, given $y \in \mathbb{R}^+$, $y - 1 \in \mathbb{R}^+$ if and only if $y - 1 > 0$ (by the definition of \mathbb{R}^+), i.e. $y > 1$. So we see that y has a pre-image if and only if $y > 1$. This proves that the image of f_2 is the set $\{y \in \mathbb{R}^+ \mid y > 1\}$ and, since this is not the whole of \mathbb{R}^+ , f_2 is not surjective. As usual, in the formal proof we give an explicit counterexample, an element of \mathbb{R}^+ which is not a value of the function.

However, the function is injective and the proof is just the same as in the previous example.

Solution The function is injective since, for $x_1, x_2 \in \mathbb{R}^+$, $f_2(x_1) = f_2(x_2) \Rightarrow x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$. However, if $x \in \mathbb{R}^+$ then $x > 0$ so that $f_2(x) = x + 1 > 1$. Thus $1/2$ is not a value of f_2 which is not then surjective. \square

Example 9.1.7 To determine whether the function $f_3: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_3(x) = 4x^2 - 4x + 2$ is injective, surjective or bijective.

This time the pre-image approach gives

$$\begin{aligned} y = f_3(x) &\Leftrightarrow y = 4x^2 - 4x + 2 \\ &\Leftrightarrow y = (2x - 1)^2 + 1 \\ &\Leftrightarrow x = (1 \pm \sqrt{y - 1})/2. \end{aligned}$$

Again we must check whether our formula for the pre-image makes sense. Now if $y < 1$ then $y - 1$ has no (real) square root and so in that case the formula has no meaning. Looking back through the steps above we see what the problem is: $y = (2x - 1)^2 + 1$ tells us that if y is a value then $y \geq 1$. This tells us that f_3 is not surjective.

The other thing we notice in the formula for the pre-image is the symbol \pm . This means that x is a pre-image for y if and only if $x = (1 + \sqrt{y - 1})/2$ or $x = (1 - \sqrt{y - 1})/2$. In other words if $\sqrt{y - 1}$ exists and is non-zero, then y has two pre-images. For example, taking $y = 2$ for which $\sqrt{y - 1} = 1$,† we obtain $f_3(x) = 2 \Leftrightarrow x = (1 \pm 1)/2$, i.e. $x = 1$ or $x = 0$. So f_3 is not injective.

Solution Because $f_3(0) = f_3(1) = 2$, the function is not injective.

For a real number x , $f_3(x) = 4x^2 - 4x + 2 = (2x - 1)^2 + 1 \geq 1$. Thus 0 is not a value of f_3 and so it is not surjective. \square

Notice that in presenting this proof no indication is given of how we found the counterexample to injectivity. Formally this is not required for the proof. In a case like this it is not difficult to spot such a counterexample (for example from the graph of the function or from rewriting the formula as $(2x - 1)^2 + 1$) but it is often a good idea to help the reader by indicating how you found the counterexample.

† We adopt the usual convention that if y is a non-negative real number then \sqrt{y} represents the non-negative square root of y , i.e. $x = \sqrt{y}$ if and only if $y = x^2$ and $x \geq 0$.

Example 9.1.8 To determine whether the function $f_4: \mathbb{R}^+ \rightarrow \{x \in \mathbb{R}^+ \mid x \geq 1\}$ given by $f_4(x) = 4x^2 - 4x + 2$ is injective, surjective or bijective.

The pre-image approach gives just the same formula as in the previous example. However, if y is in the codomain then $y \geq 1$ and so the square root in the formula for a pre-image element does determine a real number. Furthermore $(1 + \sqrt{y-1})/2 > 1/2$ and so this gives one pre-image for y showing that f_4 is surjective. For $y > 1$, we have a second pre-image precisely when $(1 - \sqrt{y-1})/2 > 0$ which occurs when $\sqrt{y-1} < 1$, i.e. $y < 2$. This proves that f_4 is not injective since elements y in the codomain have two pre-images if $y < 2$. However, it is probably more satisfying to give two specific elements of the domain where the function takes the same value; we can get these by taking $y = 5/4$ which has $\sqrt{y-1} = 1/2$ and so the pre-images $(1 \pm 1/2)/2$, i.e. $3/4$ and $1/4$.

Sketching the graph of this function is a great aid to seeing what is going on. The reader should do this.

Solution Notice that $y = f_4(x) \Leftrightarrow x = (1 \pm \sqrt{y-1})/2$. The function is surjective since given $y \geq 1$, $y = f_4(x)$ for $x = (1 + \sqrt{y-1})/2 \in \mathbb{R}^+$. The function is not injective since $f_4(1/4) = f_4(3/4) = 5/4$. \square

9.2 bijections and inverses

Definition 9.2.1 A function $f: X \rightarrow Y$ is called **invertible** if† there exists a function $g: Y \rightarrow X$ such that

$$y = f(x) \Leftrightarrow x = g(y) \quad \text{for all } x \in X \text{ and for all } y \in Y.$$

In this case we call g an **inverse (function)** of f and write $g = f^{-1}$.

The symmetry of the definition shows that in this case g is also invertible and f is an inverse of g .

This means then that corresponding to the assignment of an element of Y to each element of X there is a reverse assignment of an element of X to each element of Y .

† The reader should note the way that the word ‘if’ is used in this definition. It really means ‘if and only if’ since we are defining the meaning of the word ‘invertible’. Saying that f is invertible means precisely the same as saying that there is a function g with the properties given. This usage in definitions is very common although it has on the whole been avoided so far in this book.

Example 9.2.2 Suppose that $f: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = 2x + 1$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $g(x) = (x - 1)/2$. Then, for $x, y \in \mathbb{R}$,

$$y = f(x) \Leftrightarrow y = 2x + 1 \Leftrightarrow x = (y - 1)/2 \Leftrightarrow x = g(y).$$

Thus f and g are invertible and each is the inverse of the other.

Theorem 9.2.3 *Let $f: X \rightarrow Y$. Then f is invertible if and only if it is a bijection. Furthermore, if it is invertible, then its inverse function is unique.*

Constructing a proof. Intuitively this result is pretty clear. For example if we think of the model of the function given by placing elements from the set X in the set of boxes Y then we have observed that if the function is bijective there is precisely one element of X in each box. In this case the inverse function is given by associating to each box the element which it contains. Furthermore this procedure is only possible if there is only one element in each box which means that f is bijective.

The formal proof makes these ideas a bit more precise in terms of the formal definitions of bijectivity and inverse and is constructed as so often by simply spelling out these definitions. It may seem quite long, but if you are clear about what you are trying to do there is really only one possible way forward at each stage and so the proof more or less writes itself.

The last part of the theorem asserts that f has a unique inverse. This means that f has an inverse (for this is what is meant by stating that it is invertible) but only one inverse. Uniqueness statements are very common. The usual approach to proving them is illustrated in this case: we demonstrate that if g_1 and g_2 are inverses of f then $g_1 = g_2$. Arguments of this type have already been met in proofs of the injectivity of a function f , for this asserts that each value of the function has a unique pre-image: this is proved by demonstrating that if x_1 and x_2 are pre-images of the same element then $x_1 = x_2$ (see for example Example 9.1.5).

Proof For the first statement two things have to be proved.

(a) ' f invertible $\Rightarrow f$ bijective': Suppose that f is invertible. Then, by definition, there is an inverse function $g: Y \rightarrow X$ so that

$$y = f(x) \Leftrightarrow x = g(y) \quad \text{for all } x \in X \text{ and for all } y \in Y.$$

Now to prove that f is bijective we must prove that f is surjective and that it is injective.

For injectivity, suppose that $x_1, x_2 \in X$ are such that $f(x_1) = f(x_2)$; then we must prove that $x_1 = x_2$. Put $y_0 = f(x_1) = f(x_2)$. Then $y_0 = f(x_1) \Rightarrow x_1 = g(y_0)$ (from the definition of the inverse) but on the other hand $y_0 = f(x_2) \Rightarrow x_2 = g(y_0)$. Hence $x_1 = g(y_0) = x_2$ as required.

For surjectivity suppose that $y_0 \in Y$. We must demonstrate that there exists an element $x_0 \in X$ such that $y_0 = f(x_0)$. Put $x_0 = g(y_0)$. Then it is immediate from the definition of an inverse function that $y_0 = f(x_0)$ as required.

(b) ' f bijective $\Rightarrow f$ invertible': Suppose that f is bijective. To show that it is invertible we must construct an inverse function $g: Y \rightarrow X$. Suppose that $y_0 \in Y$. Since f is a bijection, y_0 has precisely one pre-image, say $x_0 \in X$, such that $f(x_0) = y_0$. So we can define a function by the rule that, for each $y \in Y$, $g(y)$ is the unique element $x \in X$ such that $f(x) = y$. It follows from this definition that

$$y = f(x) \Leftrightarrow x = g(y) \quad \text{for all } x \in X \text{ and for all } y \in Y$$

and so g is an inverse of f .

(c) ' f invertible \Rightarrow it has a unique inverse': Suppose that f is invertible and $g_1: Y \rightarrow X$ and $g_2: Y \rightarrow X$ are inverse functions for f . To demonstrate that $g_1 = g_2$ we must show that $g_1(y) = g_2(y)$ for all $y \in Y$. Let $y_0 \in Y$. Then put $x_1 = g_1(y_0)$ and $x_2 = g_2(y_0)$ so that we are required to prove that $x_1 = x_2$. This is easy because $x_1 = g_1(y_0) \Rightarrow y_0 = f(x_1)$ and $x_2 = g_2(y_0) \Rightarrow y_0 = f(x_2)$ so that $f(x_1) = f(x_2)$. But now, since f is invertible it is bijective (by (a)) and so in particular injective. It follows that $x_1 = x_2$, i.e. $g_1(y_0) = g_2(y_0)$ as required. \square

Because of this theorem the words ‘bijective’ and ‘invertible’ are used interchangeably when referring to functions. Many standard functions are not actually bijections but by suitable restrictions of the domain and codomain can be converted into bijections. Here are some examples from calculus.

Examples 9.2.4 (a) The function $\sin: \mathbb{R} \rightarrow \mathbb{R}$ is neither injective (since, for example, $\sin 0 = \sin \pi$) nor surjective (since, for example, there is no real number x such that $\sin x = 2$). To define an inverse function \sin^{-1} we restrict the domain and the codomain of \sin so that it is bijective. Surjectivity is easy: we simply change the codomain to the image of \sin ,

i.e. $\text{Im}(\sin)$, which is the set $[-1, 1] = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ (since we know that each number in this set arises as a value of the sine function on \mathbb{R}). Injectivity is not much harder for we know that as x varies from $-\pi/2$ to $\pi/2$ the value of $\sin x$ increases steadily from -1 to 1 (sketch the graph). So we take as our domain $[-\pi/2, \pi/2] = \{x \in \mathbb{R} \mid -\pi/2 \leq x \leq \pi/2\}$. To sum up, the function†

$$\sin: [-\pi/2, \pi/2] \rightarrow [-1, 1]$$

is a bijection. By the above theorem it has an inverse

$$\sin^{-1}: [-1, 1] \rightarrow [-\pi/2, \pi/2].$$

In making this definition we had to choose a subset of \mathbb{R} on which the sine function was injective. There are many possibilities, for example $[\pi/2, 3\pi/2]$, and each has its own inverse function. The above choice is the most natural and the function it leads to is called the *principal value* of the inverse.

In the same way we can restrict the cosine and tangent functions to obtain inverse functions

$$\cos^{-1}: [-1, 1] \rightarrow [0, \pi]$$

and

$$\tan^{-1}: \mathbb{R} \rightarrow (-\pi/2, \pi/2).$$

(b) Given $n \in \mathbb{Z}^+$, the function $x \mapsto x^n$ is a bijection $\mathbb{R} \rightarrow \mathbb{R}$ for n odd and so in this case we do have an inverse function $\mathbb{R} \rightarrow \mathbb{R}$, the *n th root function*, denoted by‡ $x \mapsto x^{1/n}$ or $x \mapsto \sqrt[n]{x}$.

† Strictly speaking this function should have a different name in order to indicate the change of domain and codomain. However, it is usual to use the same name.

‡ The notation $x^{1/n}$ is selected so that the law of exponents holds: $(x^{1/n})^n = (x^n)^{1/n} = x^1 = x$. With this definition it is possible to give some indication of the problem in defining 0^0 referred to in Definition 5.3.3. Notice that $0^{1/n}$ is defined to be 0. Furthermore, we have observed (Exercise 8.4) that the sequence $1/n$ is null, $\lim 1/n = 0$, which suggests that we ought to define $0^0 = 0$. However, if the law of indices is to hold then we must have $x^0 = 1$ for non-zero x (see the solution to Exercise 5.7) and this suggests that $0^0 = 1$, the convention adopted in this book. It is not possible to satisfy these conflicting demands. For $(x, y) \in \mathbb{R}^{\geq} \times \mathbb{R} - \{(0, 0)\}$ it is possible to define x^y extending the definition for integer exponents so that the laws of exponents are satisfied and so that the function of two variables $(x, y) \mapsto x^y$ is ‘continuous’. It is not possible to extend this ‘continuous’ function to the point $(0, 0)$. A full explanation of this, and the definition of ‘continuous’, is beyond the scope of this book (see for example K.G. Binmore, *Mathematical analysis, a straightforward approach*, Cambridge University Press, Second edition 1982).

On the other hand it is neither an injection nor a surjection when n is even. [The case $n = 2$ is typical and is discussed in Example 9.1.3(c).] In this case we restrict the domain and the codomain to \mathbb{R}^{\geq} so that we have a bijection. Thus the inverse function $x \mapsto x^{1/n} = \sqrt[n]{x}$ is a function $\mathbb{R}^{\geq} \rightarrow \mathbb{R}^{\geq}$. The convention is that for even n the expressions $x^{1/n}$ and $\sqrt[n]{x}$ represent the non-negative root of a non-negative real number x .

The following equivalent formulation of Definition 9.2.1 is often useful.

Proposition 9.2.5 *The functions $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are inverses of each other if and only if $g \circ f = I_X$ and $f \circ g = I_Y$.*

Proof ‘ \Rightarrow ’: Suppose that f and g are inverse to each other. Then

$$y = f(x) \Leftrightarrow x = g(y) \quad \text{for all } x \in X \text{ and all } y \in Y.$$

Now, given $x_0 \in X$, put $y_0 = f(x_0)$ so that $x_0 = g(y_0)$. Then $g \circ f(x_0) = g(y_0) = x_0$, i.e. $g \circ f = I_X$.

Similarly $f \circ g = I_Y$.

‘ \Leftarrow ’: Suppose that $g \circ f = I_X$ and $f \circ g = I_Y$. Suppose that $y_0 = f(x_0)$. Then $g(y_0) = g \circ f(x_0) = I_X(x_0) = x_0$. Thus $y = f(x) \Rightarrow x = g(y)$ for all $x \in X, y \in Y$.

Similarly, $x = g(y) \Rightarrow y = f(x)$ and so we have proved that f and g are inverses of each other. \square

9.3 Functions and subsets

In the previous section it has been demonstrated that a function f has an inverse f^{-1} if and only if it is a bijection. However, the reader will discover that the notation f^{-1} which has been used for the inverse function is used even when the function f is not a bijection. This chapter ends with a brief description of this more general use.

To begin with recall the definition of the power set (Definition 6.3.1): the power set $\mathcal{P}(X)$ of a set X is the set of subsets of X so that $A \in \mathcal{P}(X)$ means simply $A \subseteq X$. We now describe how given a function $f: X \rightarrow Y$ we can associate to it two functions between the power sets of X and Y (one in each direction) each of which captures the function f in a different way.

Definition 9.3.1 *Suppose that $f: X \rightarrow Y$ is a function.*

(i) The function $\vec{f} : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ is defined by

$$\vec{f}(A) = \{ f(x) \mid x \in A \}$$

for $A \in \mathcal{P}(X)$.

(ii) The function $\overleftarrow{f} : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ is defined by

$$\overleftarrow{f}(B) = \{ x \in X \mid f(x) \in B \}$$

for $B \in \mathcal{P}(Y)$.

Remarks 9.3.2 The notations \vec{f} and \overleftarrow{f} are non-standard. Most writers denote the function \vec{f} simply by f and denote the function \overleftarrow{f} by f^{-1} . With experience this does not lead to confusion (and is another example of how ambiguity can be better than pedantry). However, in this book the notations \vec{f} and \overleftarrow{f} will be used since it seems potentially confusing to have two different functions with the same name when meeting these ideas for the first time.

In the case of \vec{f} notice that each element x_0 of X corresponds to an element of $\mathcal{P}(X)$, namely the singleton subset $\{x_0\}$, and similarly for Y . So we can think of \vec{f} as an extension of f in the sense that

$$\vec{f}(\{x_0\}) = \{ f(x) \mid x \in \{x_0\} \} = \{ f(x) \mid x = x_0 \} = \{ f(x_0) \}.$$

Notice that $\vec{f}(X)$ is the image of f , $\text{Im}(f)$ (see Definition 8.4.1).

In the case of \overleftarrow{f} ,

$$\overleftarrow{f}(\{y_0\}) = \{ x \in X \mid f(x) \in \{y_0\} \} = \{ x \in X \mid f(x) = y_0 \}$$

for each $y_0 \in Y$. Thus $\overleftarrow{f}(\{y_0\})$ gives the set of pre-images of y_0 . In the box model of a function (page 90) this gives the set of elements in the box y_0 . Now, if f is a bijection with inverse f^{-1} , then $f(x) = y_0$ if and only if $x = f^{-1}(y_0)$ so that $\overleftarrow{f}(\{y_0\}) = \{f^{-1}(y_0)\}$ and we can think of \overleftarrow{f} as an extension of f^{-1} .

If f is not a bijection then $\overleftarrow{f}(\{y\})$ will not be a singleton subset for some elements of Y : if it is not a surjection then it will be empty for elements y not in the image, and if not an injection then it will contain more than one element for some y .

9.4 Peano's axioms for the natural numbers

The notion of the successor of an integer n was introduced in Section 5.1. Chapter 5 was headed by a quotation from Richard Dedekind suggesting that this idea captured the essence of the natural numbers (or positive integers). The necessary language is now available so that some indication of the ideas behind the Dedekind quotation can be given.

Definition 9.4.1 *The* $\boxed{\text{successor function}}$, $\boxed{s: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+}$, *is defined by*
 $s(n) = n + 1$ *for* $n \in \mathbb{Z}^+$.

Dedekind observed that the existence of the successor function together with the number 1 completely captures the properties of the natural numbers. These ideas are now usually associated with the name of the Italian mathematician Giuseppe Peano.[†]

Axioms 9.4.2 (Peano) *The set of positive integers \mathbb{Z}^+ is a set with a function $s: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ and an element $1 \in \mathbb{Z}^+$ such that*

- (i) *s is an injection,*
- (ii) *1 is not in the image of s , and*
- (iii) *for $A \subseteq \mathbb{Z}^+$, if $1 \in A$, and $n \in A \Rightarrow s(n) \in A$, then $A = \mathbb{Z}^+$.*

Notice that (iii) is just the induction axiom as reformulated in Axiom 7.5.1.

[†] The first exposition of these ideas was by Richard Dedekind in his book *Was sind und was sollen die Zahlen?* published in 1888. Peano formulated his axioms for the natural numbers in his book *Arithmetices principia, nova methodo exposita* published in 1889. Peano did not see Dedekind's work until his own book was in press and Peano's exposition using the language of set theory is considered to have been much more influential. It was in this book that he introduced notations for set membership (the modern symbol \in) and set inclusion (he used an inverted 'C' which he also used for implication – recall that it was observed in Section 6.1 that there is a strong connection between set inclusion and implication) and he seems to have been the first to clarify the distinction between set membership and set inclusion. Peano was a remarkable mathematician. It is curious that his 1889 book was written in Latin rather than the Italian or French he usually used. In his book about Peano (Reidel, 1980), Hubert Kennedy describes it as 'the unique romantic act of his scientific career' and suggests that it reflected Peano's awareness that he was doing something historic – after all, the great classics such as Isaac Newton's *Principia* had been written in Latin. The following year brought Peano's most striking achievement, his construction of a space-filling curve; this is a curve in the plane \mathbb{R}^2 given by continuous functions $x = f(t)$, $y = g(t)$ such that, as t varies over the interval $[0, 1]$, (x, y) passes through every point of the unit square $[0, 1] \times [0, 1]$. This was perhaps the first indication of the subtlety of the notion of dimension, confounding intuition, whose exploration has now led to the modern study of fractal sets. (See for example Donald M. Davis, *The nature and power of mathematics*, Princeton University Press, 1993.)

It is not difficult to prove (by induction) that, given any set X with a function $s : X \rightarrow X$ and a distinguished element $1 \in X$ satisfying these axioms, there is a bijection $X \rightarrow \mathbb{Z}^+$ under which the distinguished elements 1 and the successor functions correspond.† This is what is meant by saying that these statements provide axioms for the positive integers.

We can use s to define algebraic operations on \mathbb{Z}^+ inductively as follows.

Definition 9.4.3 (Peano) *The sum $m + n$ of positive integers m and n may be defined by induction on n by*

- (i) $m + 1 = s(m)$, and
- (ii) for $k \in \mathbb{Z}^+$, $m + s(k) = s(m + k)$.

The product of positive integers mn or $m \times n$ is now defined (making use of addition) by induction on n by

- (i) $m \times 1 = m$, and
- (ii) for $k \in \mathbb{Z}^+$, $m \times s(k) = m \times k + m$.

It is an interesting exercise to prove the basic algebraic properties of addition and multiplication starting from these definitions, for example the commutativity of addition $m + n = n + m$.

Exercises

9.1 Determine whether each of the following functions $\mathbb{R} \rightarrow \mathbb{R}$ is injective, surjective or bijective.

- (i) $f_1(x) = 2x + 5$.
- (ii) $f_2(x) = x^2 + 2x + 1$.
- (iii) $f_3(x) = x^2 - 2x$.
- (iv) $f_4(x) = \begin{cases} 1/x & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$

9.2 In each of the above examples consider the effect of changing the domain and the codomain to \mathbb{R}^+ .

† See for example G. Birkhoff and S. Mac Lane, *A survey of modern algebra*, Macmillan, Fourth edition 1977.

9.3 Find inverses for the following functions:

- (i) $f_1: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_1(x) = 3x + 2$;
- (ii) $f_2: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_2(x) = x^3 + 1$.

9.4 Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are injections. Prove that $g \circ f: X \rightarrow Z$ is an injection.

9.5 Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are bijections of sets. Prove that the composite $g \circ f: X \rightarrow Z$ is also a bijection and that

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}: Z \rightarrow Y \rightarrow X.$$

9.6 Let $f: X \rightarrow Y$ be a function with graph $G_f \subseteq X \times Y$. Prove that f is surjective if and only if $\forall y \in Y$, $(X \times \{y\} \cap G_f) \neq \emptyset$.

9.7 Let $f: X \rightarrow Y$ be a function and $B_1, B_2 \in \mathcal{P}(Y)$. Prove that

- (i) $B_1 \subseteq B_2 \Rightarrow \overleftarrow{f}(B_1) \subseteq \overleftarrow{f}(B_2)$,
- (ii) $\overleftarrow{f}(B_1 \cap B_2) = \overleftarrow{f}(B_1) \cap \overleftarrow{f}(B_2)$,
- (iii) $\overleftarrow{f}(B_1 \cup B_2) = \overleftarrow{f}(B_1) \cup \overleftarrow{f}(B_2)$.

Prove that the converse of the first of these statements is not universally true (by constructing a counterexample).

Problems II: Sets and functions

1 Prove the following statements:

- (i) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\} = \{x \in \mathbb{Z} \mid 0 < x < 3\}$;
- (ii) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 < 0\} = \{x \in \mathbb{R} \mid x < 2\} \cap \{x \in \mathbb{R} \mid x > 1\}$;
- (iii) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 > 0\} = \{x \in \mathbb{R} \mid x > 2\} \cup \{x \in \mathbb{R} \mid x < 1\}$.

2. By using a truth table prove that, for sets A , B and C ,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Draw a Venn diagram to illustrate the proof.

3. Prove the absorption laws:

- (i) $A \cap (A \cup B) = A$;
- (ii) $A \cup (A \cap B) = A$.

4. Prove by contradiction or otherwise that $A \cap B = A \cap C$ and $A \cup B = A \cup C$ if and only if $B = C$.

5. Using truth tables, prove that for sets A , B and C ,

- (i) $(A \cup C) - B \subseteq (A - B) \cup C$,
- (ii) $(A \cap C) - B = (A - B) \cap C$.

Draw Venn diagrams to illustrate the proofs.

Prove that there is equality in the first of these results if and only if $B \cap C = \emptyset$.

Deduce from the second of these results that

$$(A - B) \cap C = \emptyset \text{ if and only if } A \cap C \subseteq B.$$

6. Use the distributivity law to prove that

$$(A \cap B) \cup (B \cap C) \cup (C \cap A) = (A \cup B) \cap (B \cup C) \cap (C \cup A).$$

7. For subsets of a universal set U prove that $B \subseteq A^c$ if and only if $A \cap B = \emptyset$. By taking complements deduce that $A^c \subseteq B$ if and only if $A \cup B = U$. Deduce that $B = A^c$ if and only if $A \cap B = \emptyset$ and $A \cup B = U$.

8. Given sets $A, B \in \mathcal{P}(X)$, their *symmetric difference* is defined by

$$A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

Prove that

- (i) the symmetric difference is associative, $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ for all $A, B, C \in \mathcal{P}(X)$,
- (ii) there exists a unique set $N \in \mathcal{P}(X)$ such that $A \Delta N = A$ for all $A \in \mathcal{P}(X)$
[Hint: Guess what N is!],
- (iii) for each $A \in \mathcal{P}(X)$, there exists a unique $A' \in \mathcal{P}(X)$ such that $A \Delta A' = N$,
- (iv) for each $A, B \in \mathcal{P}(X)$, there exists a unique set C such that $A \Delta C = B$.

9. Using the notation of the previous problem, prove that for sets $A, B, C, D \in \mathcal{P}(X)$

$$A \Delta B = C \Delta D \Leftrightarrow A \Delta C = B \Delta D.$$

10. We define half-infinite† intervals as follows:

$$\begin{aligned} (a, \infty) &= \{x \in \mathbb{R} \mid x > a\}; \\ [a, \infty) &= \{x \in \mathbb{R} \mid x \geq a\}. \end{aligned}$$

Prove that

- (i) $(a, \infty) \subseteq [b, \infty) \Leftrightarrow a \geq b$,
- (ii) $[a, \infty) \subseteq (b, \infty) \Leftrightarrow a > b$.

† The symbol ‘ ∞ ’ used in the notation in this question does not represent a number ‘infinity’. The expression (a, ∞) is used by analogy with (a, b) , where b is a real number, but the definitions are different (cf. Exercise 6.1). In this book no meaning is attached to the symbol ‘ ∞ ’ on its own and it is only used in the notations in this question and in Definition 8.3.2. Further discussion of this use of the symbol can be found in books on analysis, for example R. Haggerty, *Fundamentals of mathematical analysis*, Addison-Wesley, Second edition 1993.

11. Give a proof or a counterexample for each of the following statements:

- (i) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0;$
- (ii) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x - y > 0;$
- (iii) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0;$
- (iv) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy > 0;$
- (v) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, xy > 0;$
- (vi) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, xy \geq 0;$
- (vii) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, xy \geq 0;$
- (viii) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y > 0 \text{ or } x + y = 0);$
- (ix) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y > 0 \text{ and } x + y = 0);$
- (x) $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0) \text{ and } (\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0).$

12. Suppose that $A \subseteq \mathbb{Z}$. Write the following statement entirely in symbols using the quantifiers \forall and \exists . Write out the negative of this statement in symbols.

There is a greatest number in the set A .

Give an example of a set A for which this statement is true. Give another example for which it is false.

13. Prove that, for sets A, B, C and D ,

- (i) $A \times (B \cup C) = (A \times B) \cup (A \times C),$
- (ii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D),$

14. Define functions f and $g: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = x^2$ and $g(x) = x^2 - 1$.

Find the functions $f \circ f$, $f \circ g$, $g \circ f$, $g \circ g$.

List the elements of the set $\{x \in \mathbb{R} \mid fg(x) = gf(x)\}$.

15. Given $A \in \mathcal{P}(X)$ define the *characteristic function* $\chi_A: X \rightarrow \{0, 1\}$ by

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \notin A, \\ 1 & \text{if } x \in A. \end{cases}$$

Suppose that A and B are subsets of X .

- (i) Prove that the function $x \mapsto \chi_A(x)\chi_B(x)$ (multiplication of integers) is the characteristic function of the intersection $A \cap B$.
- (ii) Find the subset C whose characteristic function is given by

$$\chi_C(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x).$$

16. Determine which of the following functions $f_i: \mathbb{R} \rightarrow \mathbb{R}$ are injective, which are surjective and which are bijective. Write down an inverse function of each of the bijections.

- (i) $f_1(x) = x - 1;$
- (ii) $f_2(x) = x^3;$
- (iii) $f_3(x) = x^3 - x;$
- (iv) $f_4(x) = x^3 - 3x^2 + 3x - 1;$
- (v) $f_5(x) = e^x;$
- (vi) $f_6(x) = \begin{cases} x^2 & \text{if } x \geq 0, \\ -x^2 & \text{if } x \leq 0. \end{cases}$

17. Functions $f: \mathbb{R} \rightarrow \mathbb{R}$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ are defined as follows.

$$\begin{aligned} f(x) &= \begin{cases} x+2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x-2 & \text{if } x > 1. \end{cases} \\ g(x) &= \begin{cases} x-2 & \text{if } x < -1, \\ -x & \text{if } -1 \leq x \leq 1, \\ x+2 & \text{if } x > 1. \end{cases} \end{aligned}$$

Find the functions $f \circ g$ and $g \circ f$. Is g the inverse of the function f ? Is f injective or surjective? How about g ? Sketch and compare the graphs of these functions.

18. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are surjections. Prove that the composite $g \circ f: X \rightarrow Z$ is a surjection.

19. Let $f: X \rightarrow Y$ be a function. Prove that there exists a function $g: Y \rightarrow X$ such that $f \circ g = I_Y$ if and only if f is a surjection. [g is called a *right inverse* of f .]

20. Let $f: X \rightarrow Y$ be a function and $A_1, A_2 \in \mathcal{P}(X)$.

- (i) Prove that $A_1 \subseteq A_2 \Rightarrow \vec{f}(A_1) \subseteq \vec{f}(A_2)$. Prove that the converse is not universally true. Give a simple condition on f which is equivalent to the converse.
- (ii) Prove that $\vec{f}(A_1 \cap A_2) \subseteq \vec{f}(A_1) \cap \vec{f}(A_2)$. Prove that equality is not universally true.
- (iii) Prove that $\vec{f}(A_1 \cup A_2) = \vec{f}(A_1) \cup \vec{f}(A_2)$.

21. Let $f: X \rightarrow Y$ be a function. Prove that

- (i) f is injective $\Leftrightarrow \overline{f}$ is injective $\Leftrightarrow \overleftarrow{f}$ is surjective,
- (ii) f is surjective $\Leftrightarrow \overline{f}$ is surjective $\Leftrightarrow \overleftarrow{f}$ is injective.

22. Starting from Peano's axioms prove that if $n \in \mathbb{Z}^+$ and $n \neq 1$ then n is a successor, i.e. $s(a) = n$ for some $a \in \mathbb{Z}^+$.

[Let $A = \text{Im}(s) \cup \{1\}$ and prove that $A = \mathbb{Z}^+$.]

23. Starting from Definition 9.4.3 prove that addition of positive integers is

- (i) associative, i.e. $(a + b) + c = a + (b + c)$ for positive integers a, b, c ,
- (ii) commutative, i.e. $a + b = b + a$ for positive integers a, b .

[For (ii), prove first of all that $a + 1 = 1 + a$ by induction on a .]

Part III

Numbers and counting

10

Counting

One, two, buckle my shoe;
Three, four, knock at the door;
Five, six, pick up sticks;
Seven, eight, lay them straight;
Nine, ten, a big fat hen.
Eleven, twelve, dig and delve;
Thirteen, fourteen, maids a-courtin';
Fifteen, sixteen, maids a-kissing;
Seventeen, eighteen, maids a-waitin';
Nineteen, twenty, my plate's empty.

Traditional.

Perhaps the oldest mathematical activity is counting. Some of the earliest words we learn as children are the names of the first few natural numbers and counting games are very common. In this chapter the counting process is formulated mathematically as the constructing of a bijection from a standard set of positive integers to the set of the elements being counted. This allows us to consider precisely what we mean by the number of elements in a set and what it means for a set to be finite.

10.1 Counting finite sets

Recall that we have suggested that a set can be thought of as a box containing the elements of the set. The process of counting the elements in the set or box can be carried out by removing them in turn one by one while reciting the names of the positive integers in order: ‘one’, ‘two’, ‘three’, and so on. When we have exhausted the elements, we say that the last number recited is the number of elements in the set, or the *cardinality* of the set. Sometimes, instead of removing the elements we simply point to them in turn as when we count the number of people in a

room, but the idea is the same. What this amounts to is the construction of a bijection from the standard set

$$\mathbb{N}_n = \{1, 2, \dots, n\} = \{i \in \mathbb{Z} \mid 1 \leq i \leq n\},$$

the set of the first n positive integers for some positive integer n , to the set being counted. As we count a set X , the counting process effectively defines a bijection $f: \mathbb{N}_n \rightarrow X$ by setting $f(1)$ equal to the first element of X which we count, $f(2)$ equal to the second element of X which we count, and so on. The function f is an injection because we do not count any element twice and it is a surjection because every element is counted. When we have constructed the bijection $f: \mathbb{N}_n \rightarrow X$ we can list the elements of the set $X = \{x_1, x_2, \dots, x_n\}$ where we write $x_i = f(i)$. Thus the function f is described by the following table.

i	1	2	3	\dots	$n - 1$	n
$f(i)$	x_1	x_2	x_3	\dots	x_{n-1}	x_n

Because f is a bijection each element of X occurs precisely once in the second row.

We can formulate this as a mathematical definition. It is natural to extend the definition to include the empty set, the set with no elements.[†]

Definition 10.1.1 *Given a set X , if there is a bijection $f: \mathbb{N}_n \rightarrow X$ then we say that the cardinality of X , or the number of elements in X , is n and write $|X| = n$.*

The cardinality of the empty set is defined to be 0, $|\emptyset| = 0$.

Examples 10.1.2 (a) The cardinality of the set $A = \{k \in \mathbb{Z} \mid 25 < k \leq 30\}$ is 5. When we list the elements of the set, say $\{29, 26, 30, 27, 28\}$, we are essentially constructing a bijection $f: \mathbb{N}_5 \rightarrow A$. The bijection corresponding to this listing is given by the following table.

i	1	2	3	4	5
$f(i)$	29	26	30	27	28

This is not the most obvious way of counting this set. The bijection

[†] In fact we could define \mathbb{N}_0 to be the empty set so that the case of cardinality 0 is covered by the bijection definition. However, the reader meeting set theory for the first time may be worried by the bijection between two empty sets (it is the function whose graph is the empty subset of $\emptyset \times \emptyset = \emptyset!$) and so it seems best to keep this case separate.

$g: \mathbb{N}_5 \rightarrow A$ corresponding to the obvious way of counting it is given by the following table.

i	1	2	3	4	5
$g(i)$	26	27	28	29	30

(b) The cardinality of the set \mathbb{N}_n is n for the identity map provides a bijection $\mathbb{N}_n \rightarrow \mathbb{N}_n$. Another bijection $f: \mathbb{N}_n \rightarrow \mathbb{N}_n$ is given by $f(i) = n - i$.

There is one rather subtle difficulty about this definition: we need to be sure that if we count a set in two different ways then we get the same answer. For example, in Example 10.1.2(a), we gave two ways of counting the set $\{ k \in \mathbb{Z} \mid 25 < k \leq 30 \}$ and there are others. However, whatever order we use to list this set of integers we find that the fifth element is the last one.

It is common to count a set more than once if we want to be sure about the number of elements in it. If a set is counted twice, for example when counting the number of people in a room, and the answers differ then we assume either that a mistake was made on one or both occasions (in other words the person counting failed to construct a bijection; it can be difficult to be sure that you have an injection and that you have a surjection if people keep moving about!) or that it wasn't the same set (somebody entered or left the room and so was counted on one occasion but not the other). In other words we assume that if mistakes are avoided then the answer will be the same even though we do not assume that the bijections will be the same. We can formulate this assumption as follows.

Proposition 10.1.3 *Suppose that $f: \mathbb{N}_m \rightarrow X$ and $g: \mathbb{N}_n \rightarrow X$ are bijections with the same codomain. Then $m = n$.*

We need to know this in order that the above definition of the number of elements in a set gives a *well-defined* number. Very often in mathematics definitions are made which involve some choices. Demonstrating that the notion defined is well-defined amounts to proving that it is independent of these choices, in other words different choices lead to the same answer. The notion of cardinality provides a good example of such a definition.

At this point the reader may consider that the author has taken leave of his senses. Surely it is absolutely obvious that the number of elements

in a set is a well-defined notion and two different orders of counting cannot lead to a different answer. This may be so, although our experience is only based on relatively small sets and modern physics suggests that care may be needed when we come to deal, say, with a set of electrons. In Chapter 14 we will look briefly at infinite sets and see there how misleading our intuition can be. It is often the case in mathematics that we know what properties we want some notion to have. The real question is how to define the notion mathematically. If we were unable to prove Proposition 10.1.3 then this would call into question whether Definition 10.1.1 is the right one. It has often taken many years to get a definition right, giving an appropriate mathematical formulation of the meaning of a word which successfully captures the intuitive concept. For example the search for the most useful definition of continuity when applied to functions $\mathbb{R} \rightarrow \mathbb{R}$ took over a hundred years.

Constructing a proof of Proposition 10.1.3. In spite of being intuitively ‘obvious’ this is not an easy result; it would be remarkable for a student to find a proof without some assistance. One difficulty is that it involves a set X about which we know very little. Let us summarize what we are trying to achieve.

Given	Goal
bijection $f: \mathbb{N}_m \rightarrow X$ bijection $g: \mathbb{N}_n \rightarrow X$	$m = n$

To proceed, notice that the goal does not involve the set X . However, since f and g are bijections they are invertible with inverses $f^{-1}: X \rightarrow \mathbb{N}_m$ and $g^{-1}: X \rightarrow \mathbb{N}_n$ which are also bijections. So the composite

$$g^{-1} \circ f: \mathbb{N}_m \xrightarrow{f} X \xrightarrow{g^{-1}} \mathbb{N}_n$$

is also a bijection (with inverse $f^{-1} \circ g$). Thus we can use the bijections f and g to construct a bijection $\mathbb{N}_m \rightarrow \mathbb{N}_n$. Now the statement that such a bijection exists does not involve the set X . This suggests the following strategy for proving the proposition.

Given	Goal
bijection $\mathbb{N}_m \rightarrow \mathbb{N}_n$	$m = n$

If we can prove this then we will be home since the given statement follows from the hypotheses in the proposition. Notice that this implication is just a special case of the result we are trying to prove with $X = \mathbb{N}_n$ for we then automatically have a bijection $g: \mathbb{N}_n \rightarrow \mathbb{N}_n$ given

by the identity map. It is quite common to prove a general result by reducing it to some special case.

Now to tackle this implication we look back to the definition of a bijection: a function is a bijection if and only if it is an injection and a surjection. So we might begin by examining what can be deduced simply from the injectivity of a function $\mathbb{N}_m \rightarrow \mathbb{N}_n$. Intuitively this implies that $m \leq n$, suggesting the following first step.

Given	Goal
$\text{injection } \mathbb{N}_m \rightarrow \mathbb{N}_n$	$m \leq n$

In fact this implication on its own would be sufficient for our needs. For a bijection $h: \mathbb{N}_m \rightarrow \mathbb{N}_n$ is an injection and has an inverse $h^{-1}: \mathbb{N}_n \rightarrow \mathbb{N}_m$ which is also a bijection and so an injection. Applying the implication to h gives $m \leq n$ and applying it to h^{-1} gives $n \leq m$. But $m \leq n$ and $n \leq m$ only if $m = n$ (see Exercise 4.5).

This process of reducing a result to be proved to successively simpler or more concrete statements is common in constructing proofs. To keep track of what we are doing it can be useful to formulate these other statements as propositions or theorems in their own right; sometimes the word ‘lemma’ is used instead, indicating that a result’s primary interest is as a stepping stone in the proof of some more striking result or results.

In this case it turns out that the implication we have reached is of sufficient interest to be stated formally as a lemma. So we do this now and write out the formal proof that Proposition 10.1.3 follows from it. We will then return to the proof of the lemma in the next chapter.

Proof of Proposition 10.1.3 This result follows from the following result to be proved in the next chapter.

Lemma 10.1.4 *If there exists an injection $\mathbb{N}_m \rightarrow \mathbb{N}_n$ then $m \leq n$.*

For, given bijections $f: \mathbb{N}_m \rightarrow X$ and $g: \mathbb{N}_n \rightarrow X$, they are invertible with inverses $f^{-1}: X \rightarrow \mathbb{N}_m$ and $g^{-1}: X \rightarrow \mathbb{N}_n$ which are also bijections. So the composite $g^{-1} \circ f: \mathbb{N}_m \rightarrow \mathbb{N}_n$ is a bijection, and so an injection. It follows from the lemma that $m \leq n$.

But now we can reverse the rôles of f and g . The composite $f^{-1} \circ g: \mathbb{N}_n \rightarrow \mathbb{N}_m$ is an injection and so again by the lemma $n \leq m$.

Since we have proved that $m \leq n$ and $n \leq m$ it follows that $m = n$ as required. \square

Of course not all sets can be counted. For example if we start counting the positive integers in the obvious way we never come to an end. It is useful to distinguish sets for which the counting process does end from those which do not; to distinguish finite sets from infinite sets.

Definition 10.1.5 *Given a set X , if $|X| = n$ for some non-negative integer n then we say that the set is finite. If this is not the case then we say that the set is infinite.*

Thus saying that a set X is finite means that either it is empty or there exists a bijection $\mathbb{N}_n \rightarrow X$ for some positive integer n .

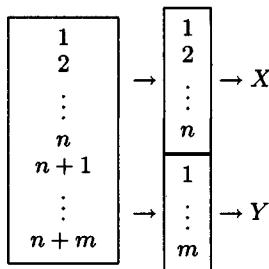
10.2 Two basic counting principles

There are two basic counting principles which are frequently used and extremely powerful. The first seems almost too simple to state.

Theorem 10.2.1 (The addition principle) *Suppose that X and Y are disjoint finite sets. Then $X \cup Y$ is finite and $|X \cup Y| = |X| + |Y|$.*

Constructing a proof. The form of words used in the conclusion of this result sometimes causes confusion. Because it is an ‘and’ statement the reader might imagine that it is necessary to prove the first statement and then to prove the second statement. But in fact the first statement is an immediate consequence of the second and, with what we have done so far, the only way to prove that a set is finite is to prove that it has cardinality equal to some non-negative integer. Since X and Y are finite sets, $|X|$ and $|Y|$ are non-negative integers and thus so is $|X| + |Y|$. We obtain the result by simply proving that $X \cup Y$ has cardinality equal to $|X| + |Y|$.

Notice that since the set X is finite then either X is empty or there is a bijection $\mathbb{N}_n \rightarrow X$ for some positive integer n . It is necessary to consider these two cases separately and similarly for Y . The cases when X or Y has cardinality 0 are trivial. In the other cases the result seems obvious since we simply count the elements in the set X , say n , and then count the elements of Y starting at $n + 1$. The following proof simply translates this intuitive idea into the language of bijections, using the bijections to X and Y to give a bijection to $X \cup Y$ as indicated in the diagram on the next page.



Proof Let $|X| = n$ and $|Y| = m$. We are required to prove that $|X \cup Y| = n + m$. If $n = 0$ then X is the empty set and so $X \cup Y = Y$ so that automatically $|X \cup Y| = |Y| = m = 0 + m$. Similarly the result is clear if $m = 0$. So let us consider the case when n and m are both positive.

Since $|X| = n$ and $|Y| = m$ there are bijections $f: \mathbb{N}_n \rightarrow X$ and $g: \mathbb{N}_m \rightarrow Y$. We can now define a bijection $h: \mathbb{N}_{n+m} \rightarrow X \cup Y$ as follows.

$$h(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq n, \\ g(i-n) & \text{if } n+1 \leq i \leq n+m. \end{cases}$$

This shows that $|X \cup Y| = m + n$. Notice that h is an injection because f and g are injections and $X \cap Y = \emptyset$; h is a surjection because f and g are surjections. \square

At the end of this proof some details have been omitted. The reader might like to consider how to supply these details justifying the last sentence of the proof. This sentence does indicate how the hypotheses in the theorem are brought into play in the proof; it is important when writing out a proof to indicate at which point(s) hypotheses are used.

Corollary 10.2.2 *For a positive integer n , suppose that X_1, X_2, \dots, X_n is a collection of n pairwise disjoint finite sets (i.e. $i \neq j \Rightarrow X_i \cap X_j = \emptyset$).*

Then $X_1 \cup X_2 \cup \dots \cup X_n = \bigcup_{i=1}^n X_i$ is a finite set and

$$|X_1 \cup X_2 \cup \dots \cup X_n| = |X_1| + |X_2| + \dots + |X_n|.$$

Proof This is an easy induction proof using the theorem. The details are left as an exercise. \square

The second basic counting principle is a consequence of the first.

Theorem 10.2.3 (The multiplication principle) Suppose that X and Y are finite sets such that $|X| = n$ and $|Y| = m$. Then the Cartesian product $X \times Y$ is a finite set and $|X \times Y| = mn$.

Proof If either of X and Y is empty then so is $X \times Y$ and the result follows. So suppose that both sets are non-empty.

Let $f: \mathbb{N}_n \rightarrow X$ be a bijection and write $x_i = f(i)$. Then

$$X = \{x_1, x_2, \dots, x_n\} = \{x_1\} \cup \{x_2\} \cup \dots \cup \{x_n\}$$

and so

$$X \times Y = (\{x_1\} \times Y) \cup (\{x_2\} \times Y) \cup \dots \cup (\{x_n\} \times Y).$$

But now, if $g: \mathbb{N}_m \rightarrow Y$ is a bijection, then $i \mapsto (x_k, g(i))$ gives a bijection $\mathbb{N}_m \rightarrow \{x_k\} \times Y$ so that $|\{x_k\} \times Y| = m$. It follows from the previous corollary that $|X \times Y| = mn$. \square

Examples 10.2.4 (a) An element of $\mathbb{N}_9 \times \mathbb{N}_9$ is an ordered pair of positive integers each no greater than 9. The number of such pairs is $9 \times 9 = 81$ by the multiplication principle.

(b) What then is the number of ordered pairs of *distinct* positive integers no greater than 9? The function $n \mapsto (n, n)$ provides a bijection $\mathbb{N}_9 \rightarrow \{(n, n) \mid n \in \mathbb{N}_9\}$ showing that there are nine ordered pairs of equal integers. This set of ordered pairs is called the *diagonal set* in $\mathbb{N}_9 \times \mathbb{N}_9$ and is denoted by $\Delta(\mathbb{N}_9)$. We are interested in the cardinality of the complement of the diagonal set, $\mathbb{N}_9 \times \mathbb{N}_9 - \Delta(\mathbb{N}_9)$. However, $\mathbb{N}_9 \times \mathbb{N}_9$ is the disjoint union $\Delta(\mathbb{N}_9) \cup (\mathbb{N}_9 \times \mathbb{N}_9 - \Delta(\mathbb{N}_9))$ and so, by the addition principle,

$$|\mathbb{N}_9 \times \mathbb{N}_9| = |\Delta(\mathbb{N}_9)| + |\mathbb{N}_9 \times \mathbb{N}_9 - \Delta(\mathbb{N}_9)|$$

so that the number of ordered pairs of distinct positive integers no greater than 9, $|\mathbb{N}_9 \times \mathbb{N}_9 - \Delta(\mathbb{N}_9)|$, is $81 - 9 = 72$.

There are of course other ways of obtaining the same result. For example, there are nine possibilities for the first coordinate and for each of these there are then eight possibilities for the second coordinate so that the number of ordered distinct pairs is $9 \times 8 = 72$.

From this result we can deduce that the number of *unordered* distinct pairs is $72/2 = 36$ since each pair may be ordered in two ways.

10.3 The inclusion–exclusion principle

The addition principle in the last section leads on to an extremely powerful combinatorial technique known as the inclusion–exclusion principle. This is concerned with a situation where we have a finite number of finite sets of known cardinality (not in general disjoint) and we wish to know the number of elements which lie in their union. Let us consider the simplest example, two sets.

Proposition 10.3.1 *Suppose that X and Y are (not necessarily disjoint) finite sets. Then $X \cup Y$ is a finite set and*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Proof Recall from Proposition 6.2.4 that $X \cup Y = (X - Y) \cup (Y - X) \cup (X \cap Y)$, a union of disjoint sets, so that by the addition principle

$$|X \cup Y| = |X - Y| + |Y - X| + |X \cap Y|.$$

Similarly, $X = (X - Y) \cup (X \cap Y)$ is a union of disjoint sets and so

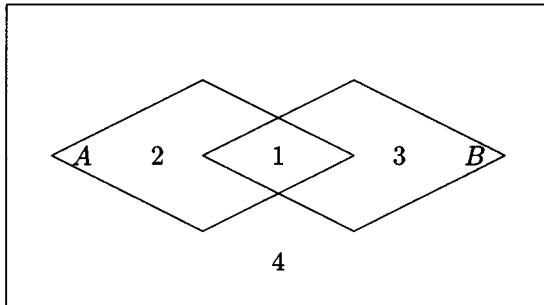
$$|X| = |X - Y| + |X \cap Y|.$$

Similarly $|Y| = |Y - X| + |X \cap Y|$. Thus

$$|X \cup Y| = (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| = |X| + |Y| - |X \cap Y|$$

as required. \square

This result is really obvious from the following Venn diagram.



Recall that $A \cup B$ consists of regions 1, 2 and 3; A consists of regions 1 and 2; B consists of 1 and 3; and $A \cap B$ consists of region 1. If we count A and then count B giving $|A| + |B|$ then we will have counted the elements in $A \cap B$ twice and so we take account of this by subtracting $|A \cap B|$.

The inclusion–exclusion principle is the generalization of this result to an arbitrary finite collection of sets. Consider the case of three sets.

Proposition 10.3.2 *Suppose that X , Y and Z are finite sets. Then $X \cup Y \cup Z$ is a finite set and*

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|. \quad (10.1)$$

Proof We apply Proposition 10.3.1 to $X \cup Y \cup Z = (X \cup Y) \cup Z$ and then apply it again to the sets which arise.

$$|(X \cup Y) \cup Z| = |X \cup Y| + |Z| - |(X \cup Y) \cap Z|; \quad (10.1)$$

$$|X \cup Y| = |X| + |Y| - |X \cap Y|; \quad (10.2)$$

$$\begin{aligned} |(X \cup Y) \cap Z| &= |(X \cap Z) \cup (Y \cap Z)| \\ &= |X \cap Z| + |Y \cap Z| - |(X \cap Z) \cap (Y \cap Z)| \\ &= |X \cap Z| + |Y \cap Z| - |X \cap Y \cap Z|. \end{aligned} \quad (10.3)$$

Substituting from equations (10.2) and (10.3) into equation (10.1) gives the result. \square

The general inclusion–exclusion principle is given as Problems III, Question 4. This proposition illustrates the inductive step in the proof. A number of applications appear later in the book.

Exercises

10.1 Suppose that X is a non-empty finite set of cardinality n . Prove that a set Y has $|Y| = n$ if and only if there exists a bijection $X \rightarrow Y$.

10.2 Prove Corollary 10.2.2.

10.3 Let $X = \{a, b, c\}$ and $Y = \{d, e\}$. What is the cardinality of the Cartesian product $X \times Y$? Write down an explicit bijection $\mathbb{N}_n \rightarrow X \times Y$ where $n = |X \times Y|$.

10.4 Each of a collection of 144 tiles is either triangular or square, either red or blue, and either wooden or plastic. Given that there are 68 wooden tiles, 69 red tiles, 75 triangular tiles, 36 red wooden tiles, 40 triangular wooden tiles, 38 red triangular tiles, and 23 red wooden triangular tiles, how many blue plastic square tiles are there?

11

Properties of finite sets

There are a number of special techniques available for proving results which involve finite sets. It is clearly possible to determine whether or not a finite set contains an element with a certain property simply by trying each element in turn. More interestingly it is possible on occasion to use ‘counting arguments’ to demonstrate the existence of an element with a certain property without considering the properties of individual elements at all. We consider these techniques in this chapter.

11.1 The pigeonhole principle

We begin by recalling the key step used in the last chapter to prove that the cardinality of a finite set is a well-defined concept. We left for this chapter the proof of the following result.

Lemma 10.1.4 *If there exists an injection $\mathbb{N}_m \rightarrow \mathbb{N}_n$ then $m \leq n$.*

Constructing a proof. Since this is a statement involving natural numbers a proof by induction is suggested. There are two natural numbers m and n in the statement and so there is a choice: induction on m or induction on n ? The following proof is by induction on n . The task of constructing an alternative proof by induction on m is left to the reader (see Problems III, Question 8).

The predicate $P(n)$ in this case is the following universal implication.

$$\forall m \in \mathbb{Z}^+ (\exists \text{ an injection } \mathbb{N}_m \rightarrow \mathbb{N}_n \Rightarrow m \leq n).$$

So the steps of the inductive proof are as follows.

Base case: It is not difficult to prove by contradiction that if there exists an injection $\mathbb{N}_m \rightarrow \mathbb{N}_1$ then $m = 1$. (Note that $m \leq 1 \Leftrightarrow m = 1$ for a positive integer m .)

Inductive step: For each $k \geq 1$ we must prove an implication which may be summarized as follows.

Given	Goal
$\forall m \in \mathbb{Z}^+ (\exists \text{ injection } N_m \rightarrow N_k \\ \Rightarrow m \leq k)$	$\forall m \in \mathbb{Z}^+ (\exists \text{ injection } N_m \rightarrow N_{k+1} \\ \Rightarrow m \leq k + 1)$

The variable m is a ‘dummy’ variable in both the given statement and the goal. To avoid confusion it is better as usual to replace m by some other symbol, say m_1 , in the goal statement so that it becomes $\forall m_1 \in \mathbb{Z}^+ (\exists \text{ injection } N_{m_1} \rightarrow N_{k+1} \Rightarrow m_1 \leq k + 1)$. The direct method of proving this is to suppose that $f: N_{m_1} \rightarrow N_{k+1}$ is an injection and then to seek to deduce that $m_1 \leq k + 1$. This may be summarized as follows.

Given	Goal
$\forall m \in \mathbb{Z}^+ (\exists \text{ injection } N_m \rightarrow N_k \\ \Rightarrow m \leq k)$	
$m_1 \in \mathbb{Z}^+$ injection $f: N_{m_1} \rightarrow N_{k+1}$	$m_1 \leq k + 1$

It is not possible to apply the given universal implication directly to the injection f since its codomain is N_{k+1} : to apply the given implication we need an injection into N_k and this may require a change of domain. The details of the proof follow [with additional comments in brackets].

Proof We prove Lemma 10.1.4 by induction on n .

Base case: This statement is trivial for $n = 1$ since, if $f: N_m \rightarrow N_1$, we must have $f(i) = 1$ for all $i \in N_m$ and this is not an injection if $m > 1$ since then, for example, $f(1) = f(2) = 1$. Thus if f is an injection then $m = 1 = n$.

[Notice that this is really a proof by contrapositive. What is actually proved is ‘ $m > 1 \Rightarrow f: N_m \rightarrow N_1$ is not an injection’ whose contrapositive is ‘ $f: N_m \rightarrow N_1$ is an injection $\Rightarrow m \leq 1$ ’.]

Inductive step: Suppose, for some $k \geq 1$, that the result is true for $n = k$. We must deduce that it holds for $n = k + 1$ so suppose that $f: N_{m_1} \rightarrow N_{k+1}$ is an injection.

[The aim now is to construct an injection $f_1: N_m \rightarrow N_k$ for some m to which we can apply the inductive hypothesis.]

We consider two cases.

(i) Suppose that $f(i) < k + 1$ for all $i \in N_m$. Then we can restrict the

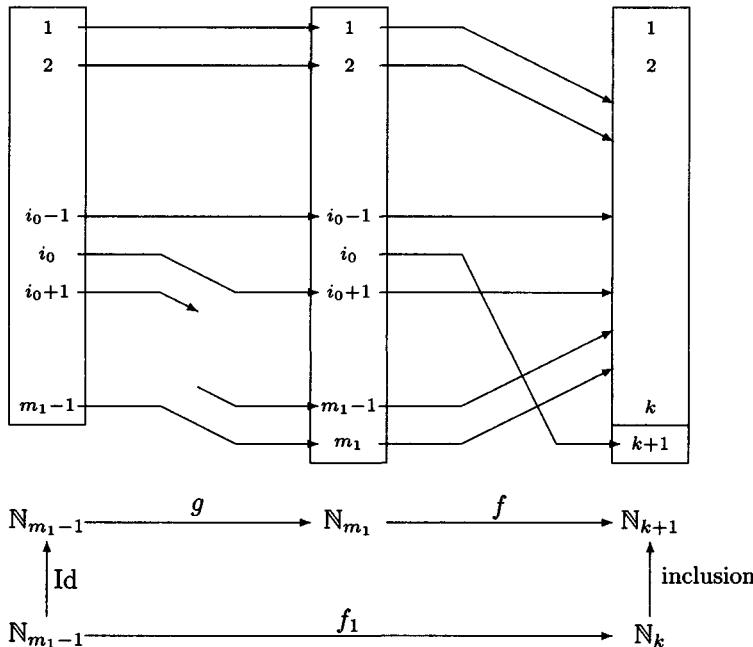
codomain and define a function $f_1: \mathbb{N}_{m_1} \rightarrow \mathbb{N}_k$ by $f_1(i) = f(i)$. The function f_1 is also an injection and so, by inductive hypothesis, $m_1 \leq k$ and so certainly $m_1 \leq k + 1$ as required.

[The function f_1 is an injection since $f_1(i_1) = f_1(i_2) \Rightarrow f(i_1) = f(i_2) \Rightarrow i_1 = i_2$ since f is an injection.]

(ii) On the other hand, suppose that $k+1$ is a value of f , say $f(i_0) = k+1$ where $i_0 \in \mathbb{N}_{m_1}$. In this case we can define an injection $g: \mathbb{N}_{m_1-1} \rightarrow \mathbb{N}_{m_1}$ by

$$g(i) = \begin{cases} i & \text{for } i < i_0, \\ i+1 & \text{for } i \geq i_0, \end{cases}$$

and then define $f_1 = f \circ g: \mathbb{N}_{m_1-1} \rightarrow \mathbb{N}_k$.



[Notice that if $i \neq i_0$ then $f(i) \neq f(i_0) = k+1$ since f is an injection so that $f(i) \in \mathbb{N}_k$.]

Then this function f_1 is also an injection (since it is the composite of two injections) and so, by inductive hypothesis, $m_1 - 1 \leq k$, i.e. $m_1 \leq k + 1$, as required.

Since one or other of these cases must be true for each function f this

completes the proof of the inductive step.

Conclusion: Hence, by induction on n , if $f: \mathbb{N}_m \rightarrow \mathbb{N}_n$ is an injection then $m \leq n$. \square

We can immediately extend this lemma to general finite sets.

Corollary 11.1.1 *Suppose that X and Y are non-empty finite sets. If there exists an injection $f: X \rightarrow Y$ then $|X| \leq |Y|$.*

So for example if a group of people are all sitting in a room (on separate chairs) then the number of people is no greater than the number of chairs.

Constructing a proof. The hypothesis tells us that there are bijections $g_1: \mathbb{N}_m \rightarrow X$ and $g_2: \mathbb{N}_n \rightarrow Y$ for some positive integers m and n . Then $|X| = m$ and $|Y| = n$ and we can obtain the result by applying the lemma to the composite

$$g_2^{-1} \circ f \circ g_1: \mathbb{N}_m \rightarrow X \rightarrow Y \rightarrow \mathbb{N}_n$$

since this is an injection (because it is a composite of injections).

This is a good example of how we can deduce a result about general finite sets from the special case about the model sets \mathbb{N}_n of the same cardinality.

Proof By hypothesis $|X| = m$ and $|Y| = n$ for positive integers m and n . Hence there are bijections $g_1: \mathbb{N}_m \rightarrow X$ and $g_2: \mathbb{N}_n \rightarrow Y$. Then $g_2^{-1} \circ f \circ g_1: \mathbb{N}_m \rightarrow \mathbb{N}_n$ is an injection. Hence, by Lemma 10.1.4, $m \leq n$, i.e. $|X| \leq |Y|$, as required. \square

This result is usually stated in the following form. It was first formulated in the first half of the nineteenth century by Lejeune Dirichlet who called it the ‘drawer principle’.

Theorem 11.1.2 (The pigeonhole principle) *Suppose that $f: X \rightarrow Y$ is a function between non-empty finite sets such that $|X| > |Y|$. Then f is not an injection, i.e. there exist distinct elements x_1 and $x_2 \in X$ such that $f(x_1) = f(x_2)$.*

Proof This is the contrapositive of Corollary 11.1.1 and so follows from that result. \square

Examples 11.1.3 (a) There are many simple applications of this result. For example, in any group of more than twelve people there must be two people with birthdays in the same month.

(b) For a slightly more elaborate application consider the following. Suppose that X is a set of at least two people. Then it can be shown that within this set there are two people with the same number of friends in the set. (Here we are assuming that if x_1 is a friend of x_2 then x_2 is a friend of x_1 .)

To see this let $|X| = n$ and define a function $f: X \rightarrow \{0, 1, 2, \dots, n-1\}$ by setting $f(x)$ equal to the number of friends of x in X . Now notice that if $n-1$ is a value of f then there exists $x_0 \in X$ such that $f(x_0) = n-1$. This means that the person x_0 is a friend of everyone else and so no one is friendless, i.e. 0 is not a value of f . Hence the numbers 0 and $n-1$ (distinct since $n \geq 2$) cannot both be values of f . Hence the image $\text{Im } f$ has cardinality less than n and so by the pigeonhole principle f cannot be an injection, i.e. there exist distinct elements x_1 and x_2 such that $f(x_1) = f(x_2)$ as claimed.

Some more mathematical applications will come later.

We can mimic the proof of Lemma 10.1.4 to prove the following more general result. The details are left to the reader (see Problems III, Question 9). (A similar result appears as Exercise 11.1.)

Proposition 11.1.4 *Suppose that $f: X \rightarrow \mathbb{N}_n$ is an injection. Then X is a finite set and $|X| \leq n$.*

This has the following consequence which is intuitively completely obvious. However, a *proof* of it has to be based on our definitions.

Corollary 11.1.5 *Suppose that $X \subseteq Y$ where Y is a finite set. Then X is also a finite set and $|X| \leq |Y|$.*

Proof Suppose that $|Y| = n$ so that there is a bijection $f: \mathbb{N}_n \rightarrow Y$. Let $i: X \rightarrow Y$ be the inclusion function $i(x) = x$. This is clearly an injection and so the composite $f^{-1} \circ i: X \rightarrow Y \rightarrow \mathbb{N}_n$ is an injection. Hence, by Proposition 11.1.4, X is finite and $|X| \leq n$, as required. \square

In the above we have concentrated on the property of injectivity. It is not difficult to deduce similar results about surjectivity such as the following.

Theorem 11.1.6 Suppose that $f: X \rightarrow Y$ is a function between non-empty finite sets such that $|X| < |Y|$. Then f is not a surjection, i.e. there exists an element of Y which is not a value of the function.

This can be proved by similar methods to the pigeonhole principle. Alternatively it can be deduced from the pigeonhole principle by observing that from a surjection $X \rightarrow Y$ it is possible to construct an injection $Y \rightarrow X$ (see for example Problems II, Question 19).

If two finite sets are known to have the same size, then it becomes easier to check whether a function between them is a bijection.

Theorem 11.1.7 Suppose that X and Y are non-empty finite sets of the same cardinality. Then a function $X \rightarrow Y$ is an injection if and only if it is a surjection. Thus to prove bijectivity it is only necessary to check one of injectivity and surjectivity.

The proof of this result is left to the reader (Problems III, Question 11).

11.2 Finite sets of real numbers

One advantage of working with finite sets is that when we are seeking an object with a certain property each of the elements can be tested in turn and this task will terminate. As an example of this consider the problem of seeking the greatest element in a set of real numbers. Of course there are sets of numbers without a greatest, for example the set of integers (see Problems I, Question 10). It will now be shown that any finite non-empty set of real numbers does have a greatest element.

Definition 11.2.1 Let A be a set of real numbers, i.e. $A \subseteq \mathbb{R}$. Then b is a minimum element of A or $b = \min A$ when

- (i) b is an element of A , i.e. $b \in A$,
- (ii) b is less than or equal to every element of A , i.e. $a \in A \Rightarrow b \leq a$.

Similarly, c is a maximum element of A or $c = \max A$ when

- (i) c is an element of A , i.e. $c \in A$,
- (ii) c is greater than or equal to every element of A , i.e. $a \in A \Rightarrow c \geq a$.

Notice that if a set of real numbers, A , has a maximum then this maximum is unique so that the number $\max A$ is well-defined. Writing out a formal proof of this uniqueness is left as an exercise (Exercise 11.2). Similarly the minimum is unique if it exists.

Examples 11.2.2 (a) For $A = \{-1, 17, 12, -78, 8\}$, $\min A = -78$ and $\max A = 17$.

(b) The set \mathbb{Z}^+ of positive integers has $\min \mathbb{Z}^+ = 1$ but there is no maximum element.

(c) Any non-empty set of positive integers has a minimum element. This result is known as *the well-ordering principle* and is equivalent to the induction principle (see Exercise 11.6 and Problems III, Question 15).

(d) The set $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ of positive real numbers has no minimum element and no maximum element. Notice that, given any element $a \in \mathbb{R}^+$ there is a smaller one, for example $a/2 \in \mathbb{R}^+$ (see Problems I, Question 11).

Proposition 11.2.3 *Let A be a finite non-empty set of real numbers. Then A has a minimum element and a maximum element.*

When this result is applied it is always important to check that the set under consideration is non-empty. The empty set is finite but does not have a minimum or maximum element since it has no elements at all!

Constructing a proof. If we think why this is intuitively obvious we come up with the following ideas.

Suppose that $|A| = n \in \mathbb{Z}^+$. (This makes use of the fact that A is finite.) Then we can write $A = \{a_1, a_2, \dots, a_n\}$. To find the maximum element we try a_1 and begin successively comparing it with the other elements a_2, a_3 and so on. If we hit something greater we start using that in place of a_1 and carry on working through the list repeating the replacement process whenever we reach a greater element. When we have completed the list, the element we have is the maximum element.

To write out this argument more formally we notice that the phrase ‘and so on’ suggests that this is really an induction argument even though the statement of the proposition does not explicitly refer to a positive integer. However, there is an implicit integer, namely the cardinality of the set A .

Proof We write out the proof for ‘maximum element’ leaving the proof for ‘minimum element’ as an exercise.

We prove by induction on n that, for all positive integers n , all non-empty finite sets of real numbers with cardinality n have a maximum element. This is clearly equivalent to the proposition because any non-empty finite set has cardinality n for some positive integer n , by definition of ‘finite’.

Base case: For $n = 1$, the single element of the set is the maximum (and the minimum) element!

Inductive step: Suppose that for some $k \in \mathbb{Z}^+$ the result holds for $n = k$ so that all sets of real numbers of cardinality k have a maximum element. Let $A = \{a_1, a_2, \dots, a_k, a_{k+1}\}$ be a set of real numbers of cardinality $k + 1$. By inductive hypothesis, the set $A' = \{a_1, a_2, \dots, a_k\}$ has a maximum element, say a' . If $a' \geq a_{k+1}$, then a' is the maximum element of A . If $a' < a_{k+1}$, then a_{k+1} is the maximum element of A . In either case A has a maximum element and so we have deduced the result for $n = k + 1$, completing the inductive step.

Hence by induction the result holds for all $n \in \mathbb{Z}^+$ and the proposition is proved. \square

11.3 Two applications of finiteness

The greatest common divisor

In Definition 2.2.1 we introduced the notion of one integer dividing another. Recall that a non-zero integer d divides a when there is an integer q such that $a = dq$. In this case we say that d is a *divisor* or a *factor* of a . Alternatively we say that a is a *multiple* of d .

Every non-zero integer divides 0 (since we can take $q = 0$). However, if a is non-zero then, if $a = dq$, q is also non-zero and so, since $|q| \geq 1$, we have $|a| \geq |d|$. Thus the set of divisors of a ,

$$D(a) = \{n \in \mathbb{Z} \mid n \text{ divides } a\},$$

is finite if a is non-zero with $\min D(a) = -|a|$ and $\max D(a) = |a|$.

If now we are given two integers a and b , not both zero, then the set of *common divisors* of a and b is given by the intersection $D(a) \cap D(b)$. Notice that $1 \in D(a) \cap D(b)$ so that $D(a) \cap D(b)$ is a non-empty finite set and so must then have a maximum element: the *greatest common divisor*.

Definition 11.3.1 *Let a and b be two integers, at least one of which*

is non-zero. Then the greatest common divisor or highest common factor of a and b is the unique positive integer d such that

- (i) d is a common divisor, i.e. d divides a and d divides b ,
- (ii) d is greater than every other common divisor:

$$c \text{ divides } a \text{ and } c \text{ divides } b \Rightarrow c \leq d.$$

We denote the greatest common divisor of a and b by (a, b) [†] or in case of possible ambiguity $\gcd(a, b)$.

Definition 11.3.2 Two integers a and b , not both zero, are called coprime or relatively prime when $(a, b) = 1$, in other words their only common factors are 1 and -1 .

Example 11.3.3 The set of divisors of 30 is

$$D(30) = \{-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$$

and the set of divisors of 72 is

$$\begin{aligned} D(72) &= \{-72, -36, -24, -18, -12, -9, -8, -6, -4, \\ &\quad -3, -2, -1, 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}. \end{aligned}$$

Hence the set of common divisors is

$$D(30, 72) = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Thus the greatest common divisor $(30, 72) = 6$.

Odd and even integers

We can use these ideas to prove a result which was used in Problems I, Question 7. It is a special case of the *division theorem* which will be reached in Chapter 15.

[†] The reader should be aware (and beware) of the way in which some notation is used in a variety of ways. Here we are using (a, b) for the greatest common divisor of two integers, but we have previously used this notation to denote an element of the Cartesian product $\mathbb{Z} \times \mathbb{Z}$ and to denote the open interval $\{x \in \mathbb{R} \mid a < x < b\}$. It is usually clear from the context which of these meanings is intended. The reader just has to get used to this sort of ambiguity.

Proposition 11.3.4 *An integer a is odd if and only if $a = 2q + 1$ for some integer q .*

Recall that we have defined ‘odd’ to mean not divisible by 2 (see Definition 2.2.3). Since this result is an ‘if and only if’ statement we have two things to prove: that the condition $a = 2q + 1$ for some q is both necessary and sufficient for a to be odd. The proof of sufficiency is a generalization of the proof of Proposition 2.2.4 in Section 4.1 so let us get that out of the way.

Proof of the sufficiency of $a = 2q + 1$ Suppose that $a = 2q + 1$ where $q \in \mathbb{Z}$. To prove that a is odd, suppose for contradiction that a is even. Then $a = 2p$ for some $p \in \mathbb{Z}$. But then $2p = a = 2q + 1$ so that $1 = 2(p - q)$ which implies $1 \geq 2$ giving the required contradiction.

Hence $2q + 1$ is not even and so is odd by definition. \square

Constructing a proof of the necessity of $a = 2q + 1$. The difficulty of the proof of necessity is that we somehow have to get our hands on the element q . One common way of constructing an element in results of this type is to define it in terms of some set – in this case we define it as the maximum member of a finite set. If you think of how you would in practice find this number q you realize that you would keep doubling integers until you got as close to a as possible. When we formalize this into a mathematical argument it gives the proof. It is easier to work with positive integers first and then extend to negative ones.

Proof of the necessity of $a = 2q + 1$ (a) Suppose that a is a positive odd integer. Set

$$A = \{ k \in \mathbb{Z} \mid k \geq 0 \text{ and } a \geq 2k \}.$$

This is a non-empty set since $0 \in A$ and it is a finite set since $k \in A \Rightarrow 2k \leq a \Rightarrow k \leq a$. So we can define $q = \max A$.

To prove that $a = 2q + 1$ notice first of all that, since $q \in A$, $a \geq 2q$ and, since q is odd, $a \neq 2q$ and so $a \geq 2q + 1$. On the other hand, since $q = \max A$, $q + 1 \notin A$ so that $a < 2(q + 1) = 2q + 2$, i.e. $a \leq 2q + 1$. Thus we have proved that $a \geq 2q + 1$ and $a \leq 2q + 1$ from which it follows that $a = 2q + 1$ as required.

(b) To complete the proof suppose that a is a negative odd integer. Then $-a$ is a positive odd integer so that from what we have proved $-a = 2q_1 + 1$. But then $a = -2q_1 - 1 = 2(-q_1 - 1) + 1 = 2q + 1$ as required if we put $q = -q_1 - 1$. \square

Exercises

11.1 Suppose that $\mathbb{N}_n \rightarrow X$ is a surjection. Prove, by induction on n , that X is a finite set and that $|X| \leq n$.

[This is similar to Proposition 11.1.4.]

11.2 Use Definition 11.2.1 to prove that if a set of real numbers has a maximum element then this element is unique.

[Hint: Suppose that c_1 and c_2 are two maximum elements of a set A and use the definition to prove that $c_1 = c_2$.]

11.3 Find the greatest common divisor of 88 and 136.

11.4 Prove that, if a and b are non-zero integers with $\gcd(a, b) = d$, then the integers a/d and b/d are coprime.

11.5 Suppose that X and Y are finite sets such that $X \subseteq Y$. Prove that

- (i) $X = Y \Leftrightarrow |X| = |Y|$,
- (ii) $X \subset Y \Leftrightarrow |X| < |Y|$.

11.6 Prove by induction on n that if A is a set of positive integers without a least element then $\mathbb{N}_n \subseteq \mathbb{Z}^+ - A$ for every n so that A is the empty set.

Deduce the well-ordering principle: every non-empty set of positive integers has a least element.

12

Counting functions and subsets

Very many counting problems can be formulated in terms of counting the number of functions between two sets (possibly satisfying certain properties) or counting the number of subsets of a given set (possibly satisfying certain properties). In this chapter we give a brief introduction to these ideas. They naturally lead to the *binomial coefficients*, one of the most important families of numbers in all mathematics.

12.1 Counting sets of functions

Suppose that X and Y are finite sets. It is natural to ask how many different functions there are with domain X and codomain Y . For example, if X is a set of people and Y is a set of dishes on a menu, then each function $X \rightarrow Y$ represents a choice of (one) dish for each person, so that the number of functions represents the number of possible orders by the set of people. If S is a set of students and T is a set of tutors then a function $S \rightarrow T$ is an assignment of a tutor for each student.

There is another increased level of abstraction here. The idea of treating a set, for example the set of integers, as a single mathematical object is one stage of abstraction. A further stage is viewing a function from one set to another as a single mathematical object. But now we are forming a new set whose elements are the functions from one set to another and asking questions about this set.

Let us return to the problem we are considering to give an example.

Example 12.1.1 Let $X = \{a, b, c\}$ and $Y = \{d, e\}$. Then the eight functions $X \rightarrow Y$ are listed in Example 8.1.3. In order to define a function $f: X \rightarrow Y$, we must list the elements $f(a)$, $f(b)$ and $f(c)$. Intuitively, since $f(a)$ can be chosen in two ways (d and e), $f(b)$ can be

chosen in two ways and $f(c)$ can be chosen in two ways, f can be chosen in $2 \times 2 \times 2 = 8$ ways and so there are eight functions. This example illustrates the following general result.

Proposition 12.1.2 *Suppose that X and Y are non-empty finite sets with $|X| = m$ and $|Y| = n$. Then the number of functions $X \rightarrow Y$ is given by n^m .*

Constructing a proof. We can generalize the above argument as follows. By the hypotheses in the proposition we can list the elements of the sets: $X = \{x_1, x_2, \dots, x_m\}$ and $Y = \{y_1, y_2, \dots, y_n\}$. A function $f: X \rightarrow Y$ is determined by listing the values $f(x_1), f(x_2)$, and so on up to $f(x_m)$. There are n possibilities for $f(x_1)$, n possibilities for $f(x_2)$, and so on. Hence the number of functions is $n \times n \times \dots \times n$ (m factors) $= n^m$, as required.

The phrase ‘and so on’ in this argument indicates that it is really an argument by induction – in this case an induction on m . This is a good example of a result with a convincing informal proof, as given above, for which the formal proof is rather complicated. The reader should endeavour to see how the simple idea in the informal proof underpins the formal proof. When writing out a formal proof it is convenient to have a name for the set of functions $X \rightarrow Y$.

Definition 12.1.3 *Given sets X and Y we denote the set of functions from X to Y by $\boxed{\text{Fun}(X, Y)}$.*

Proof of Proposition 12.1.2 The proof is by induction on the positive integer m .

Base case: For $m = 1$ suppose that $X = \{x_1\}$. Then for any set Y there is a bijection $\text{Fun}(X, Y) \rightarrow Y$ given by $f \mapsto f(x_1)$. Hence $|\text{Fun}(X, Y)| = |Y| = n$ as required.

Inductive step: Suppose that, for some $k \geq 1$, the result holds for $m = k$. To deduce the result for $m = k+1$ suppose that X_1 and Y are non-empty finite sets with $|X_1| = k+1$ and $|Y| = n$. Let $X_1 = \{x_1, x_2, \dots, x_{k+1}\}$ and $Y = \{y_1, y_2, \dots, y_n\}$. Then there are n possibilities for $f(x_{k+1})$ and

$$\text{Fun}(X_1, Y) = \bigcup_{i=1}^n \{ f: X_1 \rightarrow Y \mid f(x_{k+1}) = y_i \},$$

a disjoint union. We can determine the cardinality of each of the sets in

the union using the bijection

$$\{ f: X_1 \rightarrow Y \mid f(x_{k+1}) = y_i \} \rightarrow \text{Fun}(\{x_1, x_2, \dots, x_k\}, Y)$$

defined by $f \mapsto f|(X_1 - \{x_{k+1}\})$. [Notice that if we know that $f(x_{k+1}) = y_i$ then f is determined by its values on x_1, \dots, x_k .] For then, by inductive hypothesis,

$$|\{ f: X_1 \rightarrow Y \mid f(x_{k+1}) = y_i \}| = |\text{Fun}(\{x_1, x_2, \dots, x_k\}, Y)| = n^k.$$

Hence, by the addition principle,

$$|\text{Fun}(X_1, Y)| = \sum_{i=1}^n n^k = n \times n^k = n^{k+1}$$

as required to deduce the result for $m = k + 1$ and so completing the inductive step.

Conclusion: Hence, by induction on m , the result holds for all positive integers m . \square

For certain applications we do not wish to know the total number of functions, but just the number which have some specific property. Quite commonly we want to know the number of injections.

Proposition 12.1.4 *Suppose that X and Y are non-empty sets with $|X| = m$ and $|Y| = n$. Then the number of injections $X \rightarrow Y$ is given by $n(n-1)\dots(n-m+1)$.*

The number $n(n-1)\dots(n-m+1)$ is usually called a *falling factorial* and is denoted by $(n)_m$ in books on combinatorics. When $m = n$ it is just the usual factorial denoted by $n!$. When $m > n$ the falling factorial vanishes since one of the factors is 0: this shows that Proposition 12.1.4 is a generalization of the pigeonhole principle which asserts that in this case there are no injections. If $m \leq n$, then $(n)_m = n!/(n-m)!$.

The proof of this result is almost identical to that of Proposition 12.1.2 except that as we choose the values $f(x_1), f(x_2)$ and so on we must avoid elements of the codomain Y which have already been selected. To write it out it is again useful to have a name for the set we are counting.

Definition 12.1.5 *Given sets X and Y we denote the set of injections from X to Y by $\boxed{\text{Inj}(X, Y)}$.*

Proof of Proposition 12.1.4 The proof is by induction on the positive integer m .

Base case: For $m = 1$ suppose that $X = \{x_1\}$. Then for any set Y there is a bijection $\text{Inj}(X, Y) = \text{Fun}(X, Y) \rightarrow Y$ given by $f \mapsto f(x_1)$. Hence $|\text{Inj}(X, Y)| = |Y| = n$ as required.

Inductive step: Suppose that, for some $k \geq 1$, the result holds for $m = k$. To deduce the result for $m = k + 1$ suppose that X_1 is a set of $k + 1$ elements. Let $X_1 = \{x_1, x_2, \dots, x_{k+1}\}$ and $Y = \{y_1, y_2, \dots, y_n\}$. Then

$$\text{Inj}(X_1, Y) = \bigcup_{i=1}^n \{f \in \text{Inj}(X_1, Y) \mid f(x_{k+1}) = y_i\},$$

a disjoint union. We can determine the cardinality of each of the sets in the union using the bijection

$$\{f \in \text{Inj}(X_1, Y) \mid f(x_{k+1}) = y_i\} \rightarrow \text{Inj}(\{x_1, x_2, \dots, x_k\}, Y - \{y_i\})$$

defined by $f \mapsto f|(X_1 - \{x_{k+1}\})$. [Notice that if f is an injection and $f(x_{k+1}) = y_i$ then none of the values $f(x_1), \dots, f(x_k)$ can be y_i .] For then, by inductive hypothesis,

$$\begin{aligned} |\{f \in \text{Inj}(X_1, Y) \mid f(x_{k+1}) = y_i\}| &= |\text{Inj}(\{x_1, x_2, \dots, x_k\}, Y - \{y_i\})| \\ &= (n-1)_k \\ &= (n-1)(n-2)\dots(n-k). \end{aligned}$$

Hence, by the addition principle,

$$\begin{aligned} |\text{Inj}(X_1, Y)| &= \sum_{i=1}^n (n-1)(n-2)\dots(n-k) \\ &= n \times (n-1)\dots(n-k) = (n)_{k+1} \end{aligned}$$

as required to deduce the result for $m = k + 1$ and so completing the inductive step.

Conclusion: Hence, by induction on m , the result holds for all positive integers m . \square

In the case when $m = n$, an injection is necessarily a bijection (see Theorem 11.1.7). Bijections with the same domain and codomain are of particular interest.

Definition 12.1.6 Given a set X , a bijection $X \rightarrow X$ is called a

permutation of the set X .

Corollary 12.1.7 *Given a finite non-empty set X of cardinality n , the number of permutations of X is given by the factorial $n!$.*

Proof This is just the special case of Proposition 12.1.4 when $m = n$ for in this case an injection is automatically a bijection (by Theorem 11.1.7). \square

12.2 Counting sets of subsets

Recall from Definition 6.3.1 that the *power set* of X is the set of subsets of X , i.e.

$$\mathcal{P}(X) = \{ A \mid A \subseteq X \}.$$

Proposition 12.2.1 *Suppose that X is a set of cardinality n . Then the power set $\mathcal{P}(X)$ is a finite set of cardinality 2^n :*

$$|\mathcal{P}(X)| = 2^{|X|}.$$

Constructing a proof. A subset $A \subseteq X$ is determined by deciding whether each of the n elements of X is in the subset: there are clearly two possibilities for each element x , namely $x \in A$ and $x \notin A$. Hence the total number of possibilities for the subset A is given by $2 \times 2 \times \dots \times 2 = 2^n$.

This rather informal argument can be made precise by using the idea of the *characteristic function* of a subset which appeared in Problems II, Question 15.

Definition 12.2.2 *For any set X , we can associate to each subset A of X ($A \in \mathcal{P}(X)$) a characteristic function $\chi_A: X \rightarrow \{0, 1\}$ defined by*

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \notin A, \\ 1 & \text{if } x \in A. \end{cases}$$

Lemma 12.2.3 *The function $\mathcal{P}(X) \rightarrow \text{Fun}(X, \{0, 1\})$ given by $A \mapsto \chi_A$ is a bijection.*

Proof The inverse is given by $\chi \mapsto \{x \in X \mid \chi(x) = 1\}$ ($= \overleftarrow{\chi}(\{1\})$). \square

Proof of Proposition 12.2.1 Using the result on counting functions in the last section,

$$|\mathcal{P}(X)| = |\text{Fun}(X, \{0, 1\})| = 2^{|X|},$$

as required. \square

Definition 12.2.4 Given a set X and a non-negative integer r , an r -subset of X is a subset $A \subseteq X$ of cardinality r . We denote the set of r -subsets of X by $\mathcal{P}_r(X)$, i.e.

$$\mathcal{P}_r(X) = \{ A \subseteq X \mid |A| = r \}.$$

We define the binomial coefficient or binomial number $\binom{n}{r}$ (read ' n choose r ') to be the cardinality of the set $\mathcal{P}_r(X)$ when $|X| = n$.

The reason for this name will be apparent when we come to the binomial theorem later in this chapter. Notice that given two finite sets X_1 and X_2 of the same cardinality, there is a bijection $f: X_1 \rightarrow X_2$. Such a bijection will induce a bijection $\vec{f}: \mathcal{P}_r(X_1) \rightarrow \mathcal{P}_r(X_2)$ (see Definition 9.3.1) and so the binomial coefficients are well-defined.

Example 12.2.5 Suppose that $X = \{a, b, c, d\}$; then

$$\begin{aligned}\mathcal{P}_0(X) &= \{\emptyset\}, \\ \mathcal{P}_1(X) &= \{\{a\}, \{b\}, \{c\}, \{d\}\}, \\ \mathcal{P}_2(X) &= \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}, \\ \mathcal{P}_3(X) &= \{\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}\}, \\ \mathcal{P}_4(X) &= \{X\}, \\ \mathcal{P}_r(X) &= \emptyset \quad \text{for } r > 4.\end{aligned}$$

Thus $\binom{4}{0} = 1$, $\binom{4}{1} = 4$, $\binom{4}{2} = 6$, $\binom{4}{3} = 4$, $\binom{4}{4} = 1$ and $\binom{4}{r} = 0$ for $r > 4$.

This example illustrates the following general results.

Proposition 12.2.6 For n and r non-negative integers

- (i) $\binom{n}{r} = 0$ if $r > n$,
- (ii) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$,

$$(iii) \quad \binom{n}{r} = \binom{n}{n-r} \text{ for } 0 \leq r \leq n.$$

Proof Suppose that X is a finite set with $|X| = n$.

(i) X has no subsets of cardinality greater than n and so $\binom{n}{r} = 0$ for $r > n$.

(ii) $\mathcal{P}_0(X) = \{\emptyset\}$ and so $\binom{n}{0} = 1$. $\mathcal{P}_n(X) = \{X\}$ and so $\binom{n}{n} = 1$.

If $X = \{x_1, x_2, \dots, x_n\}$ then $\mathcal{P}_1(X) = \{\{x_1\}, \{x_2\}, \dots, \{x_n\}\}$ and so $\binom{n}{1} = n$.

(iii) There is a bijection $\mathcal{P}_r(X) \rightarrow \mathcal{P}_{n-r}(X)$ given by mapping each subset to its complement $A \mapsto A^c$. Hence $\binom{n}{r} = \binom{n}{n-r}$. \square

Proposition 12.2.7

$$\sum_{i=0}^n \binom{n}{i} = 2^n.$$

Proof This is immediate from Definition 12.2.4 using Proposition 12.2.1 and Proposition 12.2.6(i). \square

Evaluating binomial coefficients

The method used in Example 12.2.5, calculating binomial coefficients by enumerating subsets, is extremely inefficient. There is an ancient inductive method for evaluating these numbers and the key to this is the following result.

Proposition 12.2.8

For positive integers n and r such that $1 \leq r \leq n$

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Proof Let X be a set of cardinality n and choose $x_1 \in X$. Then we may define a bijection $f: \mathcal{P}_r(X) \rightarrow \mathcal{P}_{r-1}(X - \{x_1\}) \cup \mathcal{P}_r(X - \{x_1\})$ as follows. Let $A \in \mathcal{P}_r(X)$. Then

$$f(A) = \begin{cases} A - \{x_1\} \in \mathcal{P}_{r-1}(X - \{x_1\}) & \text{if } x_1 \in A, \\ A \in \mathcal{P}_r(X - \{x_1\}) & \text{if } x_1 \notin A. \end{cases}$$

We can prove that this is a bijection by writing down the inverse

$$g: \mathcal{P}_{r-1}(X - \{x_1\}) \cup \mathcal{P}_r(X - \{x_1\}) \rightarrow \mathcal{P}_r(X)$$

as follows:

$$g(A) = \begin{cases} A \cup \{x_1\} & \text{if } A \in \mathcal{P}_{r-1}(X - \{x_1\}), \\ A & \text{if } A \in \mathcal{P}_r(X - \{x_1\}). \end{cases}$$

The result now follows by the addition principle (Theorem 10.2.1). \square

Remarks 12.2.9 This relation gives an inductive method for calculating binomial coefficients which appears to have been first discovered in China by the end of the eleventh century but is now known in the west as Pascal's triangle after the French mathematician Blaise Pascal (1623–1662) who connected the study of probability with the binomial coefficients and made use of this method of calculating them.

We may display the binomial coefficients in a triangle beginning as follows.

			1					
			1	2	1			
			1	3	3	1		
			1	4	6	4	1	
			1	5	10	10	5	1
			1	6	15	20	15	6
			1	7	21	35	35	21

Here the numbers in the $(n + 1)$ st row are the binomial coefficients $\binom{n}{r}$ for $r = 0, 1, 2, \dots, n$. By Proposition 12.2.6 the border consists entirely of the number 1. By Proposition 12.2.8 each number is the sum of the two adjacent numbers in the row above. This is not a very convenient method of working out a single binomial coefficient but there is an explicit formula as follows.

Theorem 12.2.10 *For non-negative integers n and r such that $r \leq n$,*

$$\binom{n}{r} = \frac{n(n-1)\dots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

Constructing a proof. The most direct proof of this formula is by induction using Proposition 12.2.8. The details of this argument are given below. However, although this is probably the simplest argument to write out clearly it is not the most enlightening argument: it gives no

indication why the result is true. Mathematicians prefer proofs which give some understanding although this is not always achieved.[†]

In this case we can find an alternative and, I would argue, a better argument based on the definition of the binomial number as the cardinality of a set of subsets of a given cardinality and intuitive ideas about how we choose such a subset.

Suppose that X is a set of n elements. Each element A of $\mathcal{P}_r(X)$ may be specified by listing the r distinct elements of X which belong to A . For $r > 0$ this amounts to constructing an injection $f: \mathbb{N}_r \rightarrow X$ so that $\text{Im}(f) = A$. Thus the function

$$\phi: \text{Inj}(\mathbb{N}_r, X) \rightarrow \mathcal{P}_r(X)$$

given by $\phi(f) = \text{Im}(f)$ is a surjection. However, it is not a bijection since different injections may have the same image: we may list the elements of a subset A in a variety of orders. Each ordering of the elements of A corresponds to an element of the set $\text{Inj}(\mathbb{N}_r, A)$ and, by Proposition 12.1.4, this set has cardinality $r!$. Hence, since the cardinality of $\text{Inj}(\mathbb{N}_r, X)$ is $n!/(n-r)!$ (also by Proposition 12.1.4), it follows that the cardinality of $\mathcal{P}_r(X)$ is $(n!/(n-r)!)/r! = n!/r!(n-r)!$ as claimed in the theorem.

Proof The proof is by induction on n .

Base case: If $n = 0$ then the only possibility for r is $r = 0$ and we know that $\binom{0}{0} = 1$ from Proposition 12.2.6. When $n = 0$ and $r = 0$, $n!/r!(n-r)! = 0!/0!0! = 1$ (recall that $0! = 1$) and so the result is true for $n = 0$.

Inductive step: Suppose as inductive hypothesis that, for some $k \geq 0$, the result is true for $n = k$. To deduce it for $n = k + 1$, first observe that, for $r = 0$ and $r = k + 1$, $\binom{k+1}{r} = 1$ (by Proposition 12.2.6) and $(k+1)!/r!(k+1-r)! = (k+1)!/0!(k+1)! = 1$ and so the result holds in these cases. Now suppose that $1 \leq r \leq k$. Then, by Proposition 12.2.8,

$$\binom{k+1}{r} = \binom{k}{r-1} + \binom{k}{r}$$

[†] The eminent mathematician Pierre Deligne once wrote at the end of a very formal proof of his own ‘I would be grateful if anyone who has understood this proof would explain it to me’, ‘Je serais reconnaissant à toute personne ayant compris cette démonstration de me l’expliquer’ (see *Théorie des topos et cohomologie étale des schémas, Tome 3*, Lecture Notes in Mathematics, 305, Springer-Verlag, 1973, page 584). This is quoted in D. Alibert and M. Thomas, ‘Research into mathematical proof’ in David Tall (editor), *Advanced mathematical thinking*, Kluwer, 1991.

$$\begin{aligned}
 &= \frac{k!}{(r-1)!(k-r+1)!} + \frac{k!}{r!(k-r)!} \\
 &\quad \text{by inductive hypothesis} \\
 &= \frac{k!r}{r!(k-r+1)!} + \frac{k!(k-r+1)}{r!(k-r+1)!} \\
 &= \frac{k!(r+k-r+1)}{r!(k-r+1)!} = \frac{(k+1)!}{r!(k+1-r)!}
 \end{aligned}$$

as required to deduce the result for $n = k + 1$. This proves the inductive step.

Hence the result is true for all positive integers n . \square

12.3 The binomial theorem

[Professor Moriarty] is . . . endowed by nature with a phenomenal mathematical faculty. At the age of twenty-one he wrote a treatise upon the binomial theorem, which has had a European vogue. On the strength of it he won the mathematical chair at one of our smaller universities, and had, to all appearances, a most brilliant career before him.

Arthur Conan Doyle, *Memoirs of Sherlock Holmes* (The final problem).

The name ‘binomial coefficients’ for the family of numbers considered in the previous section comes from its rôle in the binomial theorem. This theorem describes how to remove the brackets from an expression of the form $(a + b)^n$. A *binomial* is the sum of two terms and so $a + b$ is a binomial.

Theorem 12.3.1 (The binomial theorem) *For all real numbers a and b and non-negative integers n ,*

$$\begin{aligned}
 (a + b)^n &= \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \\
 &= a^n + \dots + \binom{n}{i} a^{n-i} b^i + \dots + b^n.
 \end{aligned}$$

This theorem is only the simplest form of the binomial theorem. There are versions of the theorem when the exponent is a negative integer or a non-integer but in these cases the finite sum is replaced by an infinite series.[†]

[†] The more general theorem was discovered by the English mathematician Isaac Newton in the seventeenth century. Details can be found in books on advanced calculus or mathematical analysis – see for example the excellent book R. Courant and F. John, *Introduction to calculus and analysis*, Volume I, Wiley, 1965. No doubt Professor Moriarty’s treatise was on this more general theorem.

Examples 12.3.2 Using the binomial theorem we can read off the following identities from Pascal's triangle:

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2; \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3; \\ &\vdots \\ (a+b)^7 &= a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7.\end{aligned}$$

Proof of the binomial theorem Recall (from Definition 5.3.3) that we have adopted the convention that $x^0 = 1$ for all non-zero real numbers x (including $x = 0$).

The proof is by induction on n . Let $P(n)$ be the statement we are required to prove.

Base case: For $n = 0$ this statement reads $(a+b)^0 = \binom{0}{0}a^0b^0$ which is true since $(a+b)^0 = a^0 = b^0 = \binom{0}{0} = 1$.

Inductive step: Suppose now as inductive hypothesis that, for some non-negative integer k , $P(n)$ holds for $n = k$. Then, for all a and b ,

$$\begin{aligned}(a+b)^{k+1} &= (a+b)^k(a+b) \\ &= \sum_{i=0}^k \binom{k}{i} a^{k-i}b^i(a+b) \quad \text{by inductive hypothesis} \\ &= \sum_{i=0}^k \binom{k}{i} a^{k-i+1}b^i + \sum_{i=0}^k \binom{k}{i} a^{k-i}b^{i+1} \\ &= \sum_{i=0}^k \binom{k}{i} a^{k-i+1}b^i + \sum_{j=1}^{k+1} \binom{k}{j-1} a^{k+1-j}b^j \quad (\text{writing } j \text{ for } i+1) \\ &= \sum_{i=0}^k \binom{k}{i} a^{k+1-i}b^i + \sum_{i=1}^{k+1} \binom{k}{i-1} a^{k+1-i}b^i \quad (\text{writing } i \text{ for } j) \\ &= a^{k+1}b^0 + \sum_{i=1}^k \binom{k}{i} a^{k+1-i}b^i + \sum_{i=1}^k \binom{k}{i-1} a^{k+1-i}b^i + a^0b^{k+1} \\ &\qquad\qquad\qquad \text{since } \binom{k}{0} = \binom{k}{k} = 1 \\ &= a^{k+1} + \sum_{i=1}^k \binom{k+1}{i} a^{k+1-i}b^i + b^{k+1} \quad \text{by Proposition 12.2.8} \\ &= \sum_{i=0}^{k+1} \binom{k+1}{i} a^{k+1-i}b^i\end{aligned}$$

as required to prove $P(k + 1)$.

Conclusion: Hence by induction $P(n)$ holds for all positive integers n . \square

This provides an alternative proof of Proposition 12.2.7.

Corollary 12.3.3

$$\sum_{i=0}^n \binom{n}{i} = 2^n.$$

Proof Simply put $a = b = 1$ in the binomial theorem. \square

Exercises

12.1 Write down the next three rows of Pascal's triangle (page 151) and hence find the coefficient of a^3b^7 in $(a + b)^{10}$.

12.2 Find the coefficient of $a^{98}b^2$ in $(a + b)^{100}$.

12.3 Three people each select a different card from a single pack of 52 distinct cards. How many choices are possible (i) if we record who selected which card, and (ii) if we forget who selected which card?

12.4 Three people each select a main dish from a menu of five items. How many choices are possible (i) if we record who selected which dish (as the waiter should), and (ii) if we ignore who selected which dish (as the chef could)?

12.5 By equating the coefficients of x^n in $(1 + x)^{2n} = (1 + x)^n(1 + x)^n$ prove that

$$\binom{2n}{n} = \sum_{i=0}^n \binom{n}{i}^2.$$

12.6 Prove that the product of any n consecutive positive integers is divisible by $n!$.

12.7 Use $(1+i)^n$ to prove that

$$\sum_{0 \leq 2r \leq n} (-1)^r \binom{n}{2r} = \begin{cases} (-4)^k & \text{if } n = 4k, \\ (-4)^k & \text{if } n = 4k+1, \\ 0 & \text{if } n = 4k+2, \\ \frac{1}{2}(-4)^{k+1} & \text{if } n = 4k+3. \end{cases}$$

Obtain a similar result for $\sum_{0 \leq 2r+1 \leq n} (-1)^r \binom{n}{2r+1}$.

[This question uses complex numbers. The binomial theorem, Theorem 12.3.1, holds also for complex numbers a and b , with the same proof.]

13

Number systems

Numbers originally arose for the purpose of counting. This makes use of the positive integers $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$, often called the natural or counting numbers. In order to write down numbers we need some system of *numerals*, a system of symbols to represent numbers. At first the notation used was simply some sort of tally or repeated mark but in time more elaborate systems of numerals were devised leading eventually to our present Hindu–Arabic decimal system of numerals which makes use of ‘cypherization’ (i.e. different symbols 1, 2, 3, 4, 5, 6, 7, 8, 9 for different numbers) and a ‘place value system’ (e.g. in 121 the first ‘1’ denotes 100, the ‘2’ denotes $2 \times 10 = 20$, and the second ‘1’ denotes 1 so that the number represented is the sum $100 + 20 + 1$).

An effective place value system requires a symbol to denote the absence of a positive digit and it is for this purpose that a symbol like ‘0’ first appeared (so that, for example, 102 and 12 represent different numbers). In due course zero was recognized as a number in its own right and then much later negative integers were introduced giving the complete system of integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ in which any two elements may be added or subtracted.

However, numbers are also used for purposes of measurement, originally of lengths but then of many other quantities. Before 1800 B.C. the Babylonians had developed a system of sexagesimal fractions rather like our modern decimals but using a base of 60 rather than 10. These were used until relatively modern times, particularly in astronomy, and indeed are still used in the measurement of angles by degrees, minutes and seconds and time by hours, minutes and seconds. For example if we state that the size of an angle is $18^\circ 15' 53''$ we are saying that it is

$$18 + \frac{15}{60} + \frac{53}{(60)^2} = 18 \frac{953}{3600} \text{ degrees. Other ancient cultures had different}$$

techniques for dealing with fractions.

The classical Greek mathematicians took the view that the *numbers* were simply the positive integers.[†] Indeed, they took the view that the essence of all things is explainable in terms of the positive integers and their ratios. The Pythagoreans (founded by Pythagoras about 500 B.C.) assumed at first that any two lengths were *commensurable*, meaning that, given any two line segments, some unit of length could be found so that the length of each of the lines is a whole number times this unit. If then the first line is m units and the second is n units for positive integers m and n , this means that the ratio of the lengths of the two lines is m/n for some positive integers m and n , i.e. it is a rational number.

A simple consequence of Pythagoras's theorem ('the square on the hypotenuse of a right-angled triangle is the sum of the squares on the other two sides') is that the length of the diagonal of a unit square is a number whose square is 2. Some time around 400 B.C. the Pythagoreans discovered that the diagonal and side of a square are *incommensurable* or, equivalently, that there is no rational number whose square is 2. This undermined their view of the place of the positive integers in the world and was kept a secret; there is a story that the person who eventually revealed this secret of the Pythagoreans was executed by drowning. In due course an elegant way round this dilemma was discovered by Eudoxus whose theory of proportion[‡] appears in Book Five of the *Elements* of Euclid (about 300 B.C.). This involved a separation of the concepts of 'number' (which meant a positive integer) and 'magnitude' (which meant the length of a line). It was not until the nineteenth century that the two concepts were satisfactorily brought back together again through the work of mathematicians such as Richard Dedekind in Germany.

This book is not the place to go into further details about these later developments. However, it is important that the reader realizes that there are real difficulties in developing a satisfactory system of numbers and numerals.

In this chapter we review what is involved in the algebra of *rational numbers* and go on to prove the classic result that there is no rational square root of 2. A numeral system sufficient to measure all lengths is

[†] To be precise, the Greeks did not regard 1 as a number. Euclid (Book Seven of the *Elements*) refers to 1 as a *unit* and then defines a *number* to be a multitude composed of units.

[‡] See, for example, C.B. Boyer and U.C. Merzbach, *A history of mathematics*, Wiley, Second edition 1989.

provided by *infinite decimals* and we conclude the chapter by discussing this system and indicating some of its subtleties.

Further extensions of the number system are possible. The reader may well be familiar with one possibility: the system of *complex numbers* which first arose in sixteenth century Italy in the solution of cubic and quartic equations (but was not explained properly until the nineteenth century). Complex numbers are not described in this book although a few problems make use of them. The reader will meet them in the course of the study of algebra or advanced calculus.

13.1 The rational numbers

The rational number system provides a set of numbers which can be added and multiplied and which satisfy all the basic algebraic properties of numbers as listed in Properties 2.3.1. The difficulty with the integers is that we cannot always do division. For integers $b \neq 0$ and a we can only find an integer solution of the equation $bx = a$ if b divides a . However, there is always a unique rational number which is a solution. Furthermore the set of rational numbers provide just enough numbers for this purpose: given a rational number q , there are integers $b \neq 0$ and a such that $bq = a$.

A satisfactory definition of rational numbers involves ideas which will be discussed later in this book – such a definition will be indicated in Chapter 22 (see Example 22.3.5). For the moment the reader is asked to accept that a system of rational numbers with the properties described above exists. We now consider how these properties lead to the description of the numbers and their properties in terms of fractions. While doing this it is convenient to make a distinction between a rational number and a fraction: each rational number is representable by a fraction but different fractions may represent the same rational number.

Definition 13.1.1 We will use the word **fraction** to denote an expression of the form a/b where a and b are integers and b is non-zero; a is the **numerator** and b the **denominator** of the fraction.

Given integers a and (non-zero) b we say that the fraction a/b represents the **rational number** q which has the property that $bq = a$.

As a temporary notation we indicate that the rational number q is

represented by the fraction a/b by writing

$$q = \langle a/b \rangle.$$

The equation $1x = a$, for a an integer, has an integer solution, namely a , and so the integers can be thought of as a subset of the rational numbers: an integer a can be represented as a fraction by $a = \langle a/1 \rangle$.

Proposition 13.1.2 *Two fractions a_1/b_1 and a_2/b_2 represent the same rational number q , $\langle a_1/b_1 \rangle = \langle a_2/b_2 \rangle = q$, if and only if $a_1b_2 = a_2b_1$.*

Proof The fraction a_1/b_1 represents the rational number q_1 such that $b_1q_1 = a_1$, and the fraction a_2/b_2 represents q_2 such that $b_2q_2 = a_2$. Using the basic properties of multiplication (commutativity, associativity and cancelling) it follows that

$$\begin{aligned} b_1q_1 = a_1 &\Leftrightarrow b_1b_2q_1 = a_1b_2, \\ b_2q_2 = a_2 &\Leftrightarrow b_1b_2q_2 = a_2b_1. \end{aligned}$$

Hence

$$q_1 = q_2 \Leftrightarrow b_1b_2q_1 = b_1b_2q_2 \Leftrightarrow a_1b_2 = a_2b_1.$$

□

Thus for example $\langle 2/3 \rangle = \langle 8/12 \rangle = \langle (-14)/(-21) \rangle$.

By multiplying numerator and denominator by -1 if necessary, we can represent any rational number by a fraction with positive denominator. Then, by dividing the numerator and denominator by their greatest common divisor, we see that every rational number may be written in the form $q = \langle a/b \rangle$, where $b > 0$ and the greatest common divisor $(a, b) = 1$ (see Exercise 11.4).

Definition 13.1.3 *The fraction a/b is in lowest terms when b is positive and a and b are coprime.*

Thus every rational number may be represented by a fraction in lowest terms.

To see how to describe the sum of two rational numbers in terms of fractions suppose that $q_1 = \langle a/b \rangle$ and $q_2 = \langle c/d \rangle$ so that $bq_1 = a$ and $dq_2 = c$ (where a, b, c and d are integers with b and d non-zero). Then $bdq_1 = ad$ and $bdq_2 = bc$ so that (using distributivity) $bd(q_1 + q_2) = ad + bc$ which means that $q_1 + q_2$ is represented by $(ad+bc)/bd$. Similarly, since

$bdq_1q_2 = ac$, q_1q_2 is represented by ac/bd . This discussion motivates the following definition.

Definition 13.1.4 We define $\boxed{\text{sum}}$ and $\boxed{\text{product}}$ of two fractions by

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b} \times \frac{c}{d} &= \frac{ac}{bd}.\end{aligned}$$

Now it is necessary to check that these definitions lead to *well-defined* definitions of addition and multiplication of rational numbers. This procedure is always necessary when we have different expressions for the same object and then make a definition using these expressions. In this case we need to check that if different fractions are used to represent the rational numbers then adding or multiplying the fractions leads to fractions representing the same rational number.

Proposition 13.1.5 *Addition and multiplication of rational numbers are well-defined by the above formulae.*

Constructing a proof. We deal simply with addition. The proof for multiplication is similar and easier. Let us look at what we have to do.

Given	Goal
$\langle a_1/b_1 \rangle = \langle a_2/b_2 \rangle$	
$\langle c_1/d_1 \rangle = \langle c_2/d_2 \rangle$	$\langle a_1/b_1 + c_1/d_1 \rangle = \langle a_2/b_2 + c_2/d_2 \rangle$

When we spell out what these various statements mean, this leads to the following.

Given	Goal
$a_1b_2 = a_2b_1$	$(a_1d_1 + b_1c_1)b_2d_2$
$c_1d_2 = c_2d_1$	$= (a_2d_2 + b_2c_2)b_1d_1$

But now we can obtain the goal from the given statements by some simple algebraic manipulation as follows:

$$\begin{aligned}(a_1d_1 + b_1c_1)b_2d_2 &= a_1b_2d_1d_2 + b_1b_2c_1d_2 \\ &= a_2b_1d_1d_2 + b_1b_2c_2d_1 \quad \text{by the given statements} \\ &= (a_2d_2 + b_2c_2)b_1d_1.\end{aligned}$$

Proof Suppose that $\langle a_1/b_1 \rangle = \langle a_2/b_2 \rangle$ and $\langle c_1/d_1 \rangle = \langle c_2/d_2 \rangle$ so that $a_1b_2 = a_2b_1$ and $c_1d_2 = c_2d_1$. Then $\langle a_1/b_1 + c_1/d_1 \rangle = \langle (a_1d_1 + b_1c_1)/b_1d_1 \rangle$ is the same as $\langle a_2/b_2 + c_2/d_2 \rangle = \langle (a_2d_2 + b_2c_2)/b_2d_2 \rangle$ since $(a_1d_1 + b_1c_1)b_2d_2 = (a_2d_2 + b_2c_2)b_1d_1$ (using the manipulation shown above). This shows that addition is well-defined.

The proof that multiplication is well-defined is similar. \square

Notice that if $q = \langle a/b \rangle$ then $bq = \langle b/1 \times a/b \rangle = \langle ab/b \rangle = \langle a/1 \rangle = a$ and so this definition of multiplication is consistent with Definition 13.1.1.

From now on we abandon the notation $\langle a/b \rangle$ and simply write a/b for the rational number represented by the fraction a/b as usual. Thus $a_1/b_1 = a_2/b_2$ if and only if $a_1b_2 = a_2b_1$. The set of rational numbers is denoted by the symbol \mathbb{Q} .

The above discussion has described how addition and multiplication are defined in \mathbb{Q} . But of course subtraction of any element and division by non-zero elements are always possible in \mathbb{Q} since

$$\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + \frac{-c}{d}$$

and, for $c \neq 0$,

$$\frac{a}{b}/\frac{c}{d} = \frac{a}{b} \times \frac{d}{c}.$$

13.2 The irrationality of $\sqrt{2}$

The previous section has described the rational numbers and their familiar arithmetic. It was suggested above that a good number system should enable us to represent the length of any line. Pythagoras's theorem tells us that the length of the diagonal of a unit square is a number whose square is 2, usually denoted by $\sqrt{2}$. The next result tells us that there is no such rational number.

Theorem 13.2.1 *There does not exist a rational number whose square is 2.*

Constructing a proof. Since every non-zero rational number can be written in the form a/b where a and b are non-zero integers we can write the result we are trying to prove as follows:

$$\exists a, b \in \mathbb{Z} - \{0\}, 2 = (a/b)^2.$$

Whenever a result takes the form of stating that something does not happen it is very difficult to envisage a direct proof and this suggests

very strongly that we need a proof by contradiction. Remember that this requires us to suppose that our goal is false and then to seek a contradiction. The negation of the goal is

$$\exists a, b \in \mathbb{Z} - \{0\}, 2 = (a/b)^2.$$

We use this existential statement by selecting elements a and b so that the predicate is true. This gives the following strategy.

Given	Goal
$a, b \in \mathbb{Z} - \{0\}$ $2 = (a/b)^2$	contradiction

We can rewrite this as follows.

Given	Goal
$a, b \in \mathbb{Z} - \{0\}$ $a^2 = 2b^2$	contradiction

Thus we see that the theorem we are trying to prove is really one about the integer solutions to an equation:

The only integer solution to the equation $m^2 = 2n^2$ is the trivial one $m = 0$, $n = 0$.

The one method we have used for proving that an equation has no integer solutions (see for example Proposition 4.1.1) is to use the idea of divisibility. So let us try that here. Given that $a^2 = 2b^2$ then we know that a^2 must be an even number. What does this tell us about a ?

We know that a is either even or odd and it follows by a proof by contradiction that in fact a must be even (see Problems I, Question 7).

Returning to our argument, we have seen that $a^2 = 2b^2$ implies that a is even. Hence we can write $a = 2a_1$. Substituting this into $a^2 = 2b^2$ we get $4a_1^2 = 2b^2$ so that $2a_1^2 = b^2$. Hence b^2 is even and so by the same argument b is even. So we have concluded that, if $a^2 = 2b^2$, then the numbers a and b must both be even.

So what? This in itself is no contradiction but it does suggest how we might get one, for if a and b are both even this means that the fraction a/b which we began with is not written in its lowest terms since a and b have the common factor 2. But we know that every rational number can be represented by a fraction in lowest terms. So had we thought to start by insisting that a/b be the lowest terms fraction representing a square root of 2 then we would now have obtained a contradiction. So we go back and place the requirement that $(a, b) = 1$ on a and b .

This gives the following effective strategy for proving the theorem by contradiction.

Given	Goal
$a, b \in \mathbb{Z} - \{0\}$	
$(a, b) = 1$	contradiction
$a^2 = 2b^2$	[i.e. $(a, b) = 1$ and $(a, b) \neq 1$]

Proof Suppose for contradiction that there is a rational number q such that $q^2 = 2$. Write q as a fraction in lowest terms, $q = a/b$, so that a and b are integers such that $(a, b) = 1$. Now $q^2 = 2 \Rightarrow a^2/b^2 = 2 \Rightarrow a^2 = 2b^2 \Rightarrow a^2$ is even $\Rightarrow a$ is even $\Rightarrow a = 2a_1$ for some $a_1 \in \mathbb{Z}$. But then $a^2 = 2b^2 \Rightarrow 4a_1^2 = 2b^2 \Rightarrow 2a_1^2 = b^2 \Rightarrow b^2$ is even $\Rightarrow b$ is even. Hence 2 divides a and 2 divides b implying that $(a, b) \neq 1$. But this contradicts the choice of a and b and so provides the required contradiction.

Hence there does not exist a rational number whose square is 2. \square

13.3 Real numbers and infinite decimals

The result in the previous section demonstrates that the rational number system is not adequate to represent all lengths in terms of some standard unit length since the square of the length of the diagonal of a unit square is 2 and there is no rational number whose square is 2. The *real numbers* provide a further extension of the number system which is adequate to represent the lengths of all line segments. A real number which is not a rational number is said to be *irrational*. So Theorem 13.2.1 can be reformulated as the statement ‘ $\sqrt{2}$ is irrational’.

The definition of a real number is beyond the scope of this book since it requires a full treatment of the theory of limits of sequences referred to briefly in Chapter 8. This material can be found in any book on infinite sequences and series or mathematical analysis.†

The notation used to describe real numbers is that of *infinite decimals*. Thus every non-negative real number may be represented by an infinite decimal

$$a_0.a_1a_2\dots a_i\dots, \quad \text{where } a_i \in \mathbb{Z}^{\geq 0} \text{ and } 0 \leq a_i \leq 9 \text{ for } i \geq 1$$

and every infinite decimal represents a real number. The aim in this sec-

† See for example R. Haggerty, *Fundamentals of mathematical analysis*, Addison-Wesley, Second edition 1993.

tion is describe how the real number represented by an infinite decimal may be specified.

First of all, notice that a finite decimal $a_0.a_1a_2\dots a_n$ (i.e. an infinite decimal with $a_i = 0$ for $i > n$) is equal to a rational number:

$$\begin{aligned} a_0.a_1a_2\dots a_n \\ = a_0 + a_1/10 + a_2/100 + \dots + a_n/(10)^n \\ = (a_0(10)^n + a_1(10)^{n-1} + a_2(10)^{n-2} + \dots + a_n)/(10)^n. \end{aligned}$$

So the set of finite decimals is a subset of the set of rational numbers.

The intuitive idea of an infinite decimal is that as we take more and more decimal places we get finite decimals which provide a better and better approximation to the number. Before we give a precise definition let us consider an example.

Example 13.3.1 We have already proved that there is no rational number whose square is 2. Let us consider how to find an infinite decimal representing the positive real number whose square is 2. We construct the integers a_0, a_1, \dots making up the decimal by an inductive process. The key observation which enables us to do this is that, for non-negative real numbers a and b , $a < b$ if and only if $a^2 < b^2$ (see Exercise 4.6).

Step 0: To find the integer part we find the largest integer whose square is less than 2. Since $1^2 = 1 < 2 < 2^2 = 4$ we know that $1 < \sqrt{2} < 2$ and so we put $a_0 = 1$.

Step 1: To find the first entry after the decimal point we square each of the numbers $1.0, 1.1 = 11/10, 1.2 = 12/10, \dots, 1.9 = 19/10$ in turn and find the largest of them whose square is less than 2. (Notice that we cannot get equality since 2 is not a rational square). Since

$$(14/10)^2 = 196/100 < 2 < (15/10)^2 = 225/100$$

we know that $1.4 < \sqrt{2} < 1.5$ and so put $a_1 = 4$.

Step 2: For the second decimal place, since

$$(141/100)^2 = 19881/10000 < 2 < (142/100)^2 = 20164/10000$$

so that $1.41 < \sqrt{2} < 1.42$ we put $a_2 = 1$.

This process continues indefinitely giving an infinite decimal whose first few decimal places are 1.41421356237309504880 – which means that

$$1.41421356237309504880 < \sqrt{2} < 1.41421356237309504881.$$

However, there is no apparent pattern to the numbers which emerge. By Step n we have found a finite decimal $a_0.a_1a_2\dots a_n$ such that

$$(a_0.a_1a_2\dots a_n)^2 < 2 < (a_0.a_1a_2\dots a_n + 1/(10)^n)^2$$

which means that

$$a_0.a_1a_2\dots a_n < \sqrt{2} < a_0.a_1a_2\dots a_n + 1/(10)^n.$$

For example, saying that the first seven decimal places of $\sqrt{2}$ are given by 1.4142135 means that

$$1.4142135 < \sqrt{2} < 1.4142136$$

and, if we do the arithmetic, we find that it is indeed the case that

$$1.4142135^2 = 1.99999982358225 < 2 < 1.4142136^2 = 2.00000010642496.$$

This example illustrates the formal definition.

Definition 13.3.2 *Given an infinite decimal $a_0.a_1a_2\dots a_i\dots$, we say that it represents a real number a , written $a = a_0.a_1a_2\dots a_i\dots$, when*

$$a_0.a_1a_2\dots a_n \leq a \leq a_0.a_1a_2\dots a_n + 1/(10)^n \text{ for each } n \in \mathbb{Z}^+.$$

Notice that we use ' \leq ' rather than ' $<$ ' in this definition. This is necessary so that all rational numbers may be represented by an infinite decimal (possibly with $a_i = 0$ for $i > n$, some n).

The statement that every infinite decimal represents *some* real number is one version of the *completeness* or *continuity axiom* for the real numbers.

To see that an infinite decimal is equal to a *unique* real number we observe that the inequalities in the definition uniquely specify the number a . Given two distinct real numbers a and a' we have $a - a' \neq 0$. Now we choose an integer n so that $1/(10)^n < |a - a'|$ by taking $n > 1/|a - a'|$ (for then $1/(10)^n < 1/n < |a - a'|$). [The fact that for each real number there is a greater integer is sometimes called the *Archimedean axiom* for the real numbers.] This means that infinite decimals representing a and a' will certainly differ by the n th decimal place.

Example 13.3.3 Let us consider which real number is represented by the infinite decimal $0.999\dots 99\dots$ each of whose entries after the decimal point is 9. An infinite decimal like this is called a *recurring* or repeating decimal, and we use the notation $0.\overline{9}$ to represent it with a

dot over the integer which recurs. Recurring decimals may have a block of digits recurring, for example $7.320008140081400814\dots$. In this case we indicate the repeating block by placing a dot over the first and last digits in the block, viz. $7.\overline{32000814}.$ [†]

The finite decimals $0.99\dots 9$ are certainly less than 1. Indeed,

$$0.\underbrace{99\dots 9}_n = \underbrace{99\dots 9}_n / (10)^n = \frac{(10)^n - 1}{(10)^n} = 1 - \frac{1}{(10)^n}.$$

Intuition may suggest that this means that the infinite decimal $0.\dot{9}$ is also less than 1 and this is a common misconception. I have known people become quite belligerent in their defence of this view. This is not an effective way of defending any point of view but emotion is particularly inappropriate in a mathematical argument! As always, if in doubt apply Humpty Dumpty's principle and examine what the words have been declared to mean. So we return to the definition. Let $a = 0.\dot{9}$. From the definition,

$$\begin{aligned} a = 0.\dot{9} &\Leftrightarrow 1 - 1/(10)^n \leq a \leq 1 \\ &\Leftrightarrow 0 \leq 1 - a \leq 1/(10)^n \end{aligned} \tag{13.1}$$

for all positive integers n .

Thus $1 - a > 0$ or $1 - a = 0$. We eliminate the first of these possibilities by contradiction. If x is a positive number then as above we can find a positive integer k such that $1/(10)^k < x$ by taking $k > 1/x$. Applying this to $x = 1 - a$ demonstrates that if $1 - a > 0$ then $1 - a$ does not satisfy the condition (13.1) for $n = k$, giving a contradiction. The conclusion must be that $1 - a$ is not positive and so $1 - a = 0$ or in other words $a = 1$. This proves that

$0.\dot{9} = 1.$

If this result still worries you (and after all why not, since it is based on Definition 13.3.2 which is rather sophisticated?) then you may feel happier when you remember the most familiar recurring decimal, $1/3 = 0.\dot{3}$, which you probably are comfortable with. Multiplying by 3 gives $1 = 0.\dot{9}$.

[†] Alternatively, we place a dot over each digit which recurs, $7.320\dot{0}\dot{8}1\dot{4}$ or a line over the repeating block, $7.\overline{32000814}$.

Recurring decimals and rationals

The arithmetic of infinite decimals is quite complicated.[†] However, multiplication by 10 is easy for

$$\begin{aligned} 10 \times a_0.a_1a_2\dots a_n &= 10(a_0 + a_1/10 + a_2/100 + \dots + a_n/(10)^n) \\ &= 10a_0 + a_1 + a_2/10 + \dots + a_n/(10)^{n-1} \\ &= (10a_0 + a_1).a_2\dots a_n. \end{aligned}$$

So multiplication of a finite decimal by 10 corresponds to moving the decimal point one place to the right. This means that the same is true of infinite decimals since

$$\begin{aligned} a_0.a_1a_2\dots a_n &\leq a \leq a_0.a_1a_2\dots a_n + 1/(10)^n \\ \Leftrightarrow (10a_0 + a_1).a_2\dots a_n &\leq 10a \leq (10a_0 + a_1).a_2\dots a_n + 1/(10)^{n-1}. \end{aligned}$$

This observation enables us to prove the following result.

Theorem 13.3.4 *A recurring infinite decimal is equal to a rational number.*

The idea of the proof of this result is very simple but writing out a general proof leads to great notational complexity. The proof consists of an algorithm (or procedure) for finding the rational number. If the length of the recurring block is k we multiply through by 10^k and subtract the number we started with. The result is a finite decimal and so a rational number. This enables us to write the recurring decimal as a rational number. Rather than writing out a general proof the method is illustrated by giving an example.

Example 13.3.5 To find the rational number $12.79317317317\dots = 12.79\dot{3}\dot{1}\dot{7}$.

Solution Let $x = 12.79\dot{3}\dot{1}\dot{7}$. Since the length of the recurring part is 3 we multiply through by 10^3 giving $1000x = 12793.\dot{1}\dot{7}\dot{3}$ (since the decimal point moves three places to the right) $= 12793.17\dot{3}\dot{1}\dot{7}$. From the definition of the value of an infinite decimal we can split off an initial finite decimal:

$$x = 12.79 + 0.00\dot{3}\dot{1}\dot{7},$$

[†] An excellent discussion of the arithmetic of infinite decimals, a topic bypassed in most treatments of infinite decimals, may be found in A. Gardiner, *Infinite processes, background to analysis*, Springer-Verlag, 1982.

$$1000x = 12793.17 + 0.00\dot{3}1\dot{7}.$$

Subtracting we obtain

$$999x = 12793.17 - 12.79 = 12780.38 = 1278038/100$$

and so $x = 1278038/99900$, a rational number as required. \square

We will see later on that the converse of this theorem is also true (see Problems IV, Question 5). This means that the rational numbers correspond precisely to the recurring decimals (a finite decimal can be thought of as a recurring infinite decimal: $a_0.a_1\dots a_n = a_0.a_1\dots a_n\dot{0}$).

Exercises

13.1 Prove that there does not exist a rational number whose square is 3.

[You may assume that a^2 is divisible by 3 if and only if a is divisible by 3 (proved later as Proposition 15.2.1).]

13.2 Find the first two decimal places of an infinite decimal representing $\sqrt{3}$.

13.3 Try to mimic the proof of Theorem 13.2.1 to show that there does not exist a rational number whose square is 4. Where does this go wrong?

13.4 Prove from Definition 13.3.2 that $1/3 = 0.\dot{3}$.

13.5 Find the rational number equal to the recurring infinite decimal 1.7782345.

14

Counting infinite sets

In Chapter 10 a non-empty set X was defined to have cardinality n , where n is a positive integer, when there is a bijection $N_n \rightarrow X$ from the standard set $N_n = \{1, 2, \dots, n\}$. Such sets, together with the empty set, were defined as *finite* and all others as *infinite*.

We saw (Exercise 10.1) that, given a finite set X , another set Y is also finite of the same cardinality if and only if there is a bijection $X \rightarrow Y$. In this case we say that X and Y are *equipotent*. A bijection $X \rightarrow Y$ guarantees that X and Y have the same cardinality.

These ideas may be extended to infinite sets. We can think of any two sets as having the same cardinality if they are equipotent so that there is a bijection between them. We can then describe this cardinality by introducing additional standard sets. For example, when we embark on counting a set X we assign a distinct element of the set to each positive integer in turn. If we exhaust the elements on reaching the integer n then we have constructed a bijection $N_n \rightarrow X$ and so the set is finite with cardinality n . If we never exhaust the elements we may nevertheless reach each element of the set eventually so that we have a bijection $\mathbb{Z}^+ \rightarrow X$. In this case the set is equipotent to the standard set \mathbb{Z}^+ and we say that the set, although infinite, is *denumerable*.

In this chapter we will explore the properties of infinite sets, considering which properties of finite sets can be extended to such sets. It will become clear that not all do so and this should help explain why such care was needed in developing the theory of finite sets. The fact that when we come to infinite sets various ‘obvious’ results are no longer true suggests that these results may not be quite so obvious after all! In particular we will see that care must be taken when comparing the ‘size’ of infinite sets but that it is possible to do this. It is even possible in certain cases to use ‘counting arguments’ with infinite sets.

The material in this chapter is somewhat harder than most of the rest of the book. It is not used subsequently in the book but is included to provide a context for the earlier material on finite sets and because the ideas are so striking and should be part of any general mathematical education.

14.1 Countable sets

Definition 14.1.1 Two sets X and Y are **equipotent** if there is a bijection $X \rightarrow Y$.

Thus X is finite of cardinality $n \in \mathbb{Z}^+$ if and only if X is equipotent to \mathbb{N}_n .

Definition 14.1.2 A set X is said to be **denumerable** or enumerable if there is a bijection $\mathbb{Z}^+ \rightarrow X$, so that it is equipotent to \mathbb{Z}^+ . A set is **countable** if either it is finite or it is denumerable. A set is **uncountable** if it is not countable.

If the set X is denumerable then it is said to have **cardinality** \aleph_0 and this is written $|X| = \aleph_0$.

The notation for the cardinality of a denumerable set uses the Hebrew letter aleph and ' \aleph_0 ' is usually read 'aleph null'.

Conventions vary a little and in some books the word 'countable' is used where we are using 'denumerable' or conversely.

If a set X is denumerable then we can list the elements of the set, but the list is infinite. Given a bijection $f: \mathbb{Z}^+ \rightarrow X$,

$$X = \{x_1, x_2, \dots, x_n, \dots\}$$

where we write $x_n = f(n)$.

Examples 14.1.3 (a) \mathbb{Z}^+ is denumerable by taking the identity function $\mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. This gives the listing $\mathbb{Z}^+ = \{1, 2, \dots, n, \dots\}$.

(b) The set of non-negative integers \mathbb{Z}^{\geq} is denumerable since a bijection $\mathbb{Z}^+ \rightarrow \mathbb{Z}^{\geq}$ is defined by $n \mapsto n - 1$. This gives the listing $\mathbb{Z}^{\geq} = \{0, 1, \dots, n - 1, \dots\}$.

(c) The set of all integers \mathbb{Z} is denumerable, for a bijection $\mathbb{Z}^+ \rightarrow \mathbb{Z}$ may be defined by

$$n \mapsto \begin{cases} -(n-1)/2 & \text{if } n \text{ is odd,} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

This gives the listing $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots, n, -n, \dots\}$.

(d) The set of positive even integers $X = \{2n \mid n \in \mathbb{Z}^+\}$ is denumerable, for a bijection $\mathbb{Z}^+ \rightarrow X$ may be given by $n \mapsto 2n$. This gives the listing $\{2, 4, \dots, 2n, \dots\}$.

(e) The set of positive perfect squares $X = \{n^2 \mid n \in \mathbb{Z}^+\}$ is denumerable, for a bijection $\mathbb{Z}^+ \rightarrow X$ may be given by $n \mapsto n^2$. This gives the listing $X = \{1, 4, \dots, n^2, \dots\}$.

'Paradoxes' of the infinite

Recall from Exercise 11.5 that a finite set can never have the same cardinality as a proper subset: the cardinality of a proper subset of a finite set is necessarily smaller. However, the above examples demonstrate that a denumerable set can have equipotent proper subsets. Example 14.1.3(d) shows that the set of positive integers and the positive even integers are equipotent and so, in that sense, there are the ‘same number’ of even integers as integers even though it appears that only half the integers are even!

The first reference to this ‘paradox’ appears in the work of Galileo Galilei.[†] He observes that, despite the fact that the further you go along the sequence of positive integers the scarcer the perfect squares become, we must say that there are as many squares as there are positive integers because of the correspondence between the positive integers and the squares given by the bijection $n \mapsto n^2$ (Example 14.1.3(e)). He suggests that the idea of one infinite quantity being greater than another has no meaning.

These ideas seem not to have been developed further until 1850 when a book by the unconventional Czech priest Bernhard Bolzano was published posthumously.[‡] He showed that there were many examples of bijections between infinite sets and proper subsets. He also suggested that

[†] In his 1638 book *Discorsi e dimostrazioni matematiche intorno à due nuove scienze* (written, remarkably for the period, in Italian rather than Latin and often referred to by its English title *The two new sciences*).

[‡] *Paradoxien des Unendlichen* published in English as *Paradoxes of the infinite* (edited by D.A. Steele) in 1950.

nevertheless certain infinite sets are in a real sense bigger than others, anticipating the work of Cantor which we will come to shortly.

In 1872 the German mathematician Richard Dedekind defined an infinite set to be one which is equipotent to a proper subset of itself.[†] We now observe that this is equivalent to our definition of infinite set.

Theorem 14.1.4 (Dedekind) *A set X is infinite if and only if it is equipotent to a proper subset of itself.*

Proof If X is equipotent to a proper set then, by Exercise 11.5, X is not finite and so must be infinite.

For the converse, first of all we prove that an infinite set X must contain a denumerable subset. We define this set $A = \{a_1, a_2, \dots, a_n, \dots\}$ inductively.

Base case: Choose any element of the set X as a_1 .

Inductive step: Suppose that, for some $k \geq 1$, a subset of k distinct elements $A_k = \{a_n \mid 1 \leq n \leq k\}$ has been defined. Choose any element of $X - A_k$ [non-empty since A_k is finite and X is infinite] as a_{k+1} .

This defines a denumerable subset $A = \{a_1, a_2, \dots, a_n, \dots\} \subseteq X$.

We may now define a bijection $f: X \rightarrow X - \{a_1\}$ onto a proper subset of X , as required, by

$$f(x) = \begin{cases} a_{n+1} & \text{if } x = a_n \in A, \\ x & \text{if } x \notin A. \end{cases}$$

Hence X and the proper subset $X - \{a_1\}$ are equipotent. □

14.2 Denumerable sets

For two finite sets, their cardinality determines whether or not they are equipotent, i.e. whether or not there is a bijection between them (Exercise 10.1). This property extends to sets of cardinality \aleph_0 , denumerable sets, as follows.

Proposition 14.2.1 *Given a denumerable set X , a set Y is also denumerable if and only if it is equipotent to X .*

Proof Since X is denumerable there is a bijection $f: \mathbb{Z}^+ \rightarrow X$.

[†] In his book *Stetigkeit und irrationale Zahlen*.

Suppose that Y is also denumerable. Then there is a bijection $g: \mathbb{Z}^+ \rightarrow Y$. Since a bijection is invertible we can now deduce that X and Y are equipotent by writing down the bijection $g \circ f^{-1}: X \rightarrow \mathbb{Z}^+ \rightarrow Y$.

Conversely, if X and Y are equipotent then there is a bijection $h: X \rightarrow Y$. We can deduce that Y is denumerable by writing down the bijection $h \circ f: \mathbb{Z}^+ \rightarrow X \rightarrow Y$. \square

When we form unions or products of finite sets we normally obtain bigger sets. One aspect of the unexpected behaviour of infinite sets is that for them this is not the case.

Proposition 14.2.2 *If A and B are denumerable sets then so is their union $A \cup B$.*

This is left as an exercise.

Proposition 14.2.3 *If A and B are denumerable sets then so is their Cartesian product, $A \times B$.*

Constructing a proof. Since A and B are denumerable we can list their elements: $A = \{a_1, a_2, \dots, a_m, \dots\}$ and $B = \{b_1, b_2, \dots, b_n, \dots\}$. Using these listings we can display the elements of $A \times B$ in a double array.

$$\begin{array}{ccccccc} & & & & & \vdots & \\ & (a_1, b_4) & & & & \vdots & \\ & (a_1, b_3) & (a_2, b_3) & & \dots & & \\ & (a_1, b_2) & (a_2, b_2) & (a_3, b_2) & & \dots & \\ (a_1, b_1) & (a_2, b_1) & (a_3, b_1) & (a_4, b_1) & & \dots & \end{array}$$

If we start to count these elements by going along the rows, which would be the normal way of counting a finite array (consider for example the solution to Exercise 10.3) then we will never get to the end of the first row and so no element in the second row will be reached. One way of ensuring† that we do eventually reach every element is to count along

† This should be contrasted with the situation for finite sets. For a finite set it doesn't matter how we start: the addition principle ensures that we will complete the count and Proposition 10.1.3 ensures that the answer will always be the same.

the diagonals in the following pattern.

:	:			
10	:			
6	9	...		
3	5	8	...	
1	2	4	7	...

If we count in this way the element (a_m, b_n) will occur as the n th element in diagonal number $m + n - 1$. So (since there are k elements in the k th diagonal) it will be element number

$$1 + 2 + \dots + (m + n - 2) + n = \frac{1}{2}(m + n - 2)(m + n - 1) + n$$

(using Proposition 5.3.1).

Proof Let $A = \{a_1, a_2, \dots, a_m, \dots\}$ and $B = \{b_1, b_2, \dots, b_n, \dots\}$. Then a bijection $A \times B \rightarrow \mathbb{Z}^+$ may be defined by

$$(a_m, b_n) \mapsto \frac{1}{2}(m + n - 2)(m + n - 1) + n.$$

□

Corollary 14.2.4 *If A is a denumerable set then so is A^n for every positive integer n .*

Proof This is an easy induction proof. The proposition gives the inductive step. □

Proposition 14.2.5 *A subset of a denumerable set is countable (i.e. either finite or denumerable).*

Constructing a proof. As with finite sets we can prove statements about general denumerable sets by first proving them for the standard denumerable set \mathbb{Z}^+ .

The conclusion of this result is an ‘or’ statement and so we use the standard strategy introduced in Chapter 4: we take a non-finite subset, A , of \mathbb{Z}^+ in other words an infinite subset, and verify that it must be denumerable. We can construct a bijection $\mathbb{Z}^+ \rightarrow A$ inductively essentially by listing the elements of A in increasing order starting with the least.

Proof (a) We begin by considering subsets of \mathbb{Z}^+ , the set of positive integers. Suppose that A is an infinite subset of \mathbb{Z}^+ . Then to prove that A is denumerable we must construct a bijection $f: \mathbb{Z}^+ \rightarrow A$. We define $f(n)$ inductively as follows.

Base case: Let $f(1)$ be the least element of the set A . [Recall that by the well-ordering principle (see Example 11.2.2(c)) any non-empty set of positive integers has a least element.]

Inductive step: Suppose that $f(k)$ has been defined for some $k \geq 1$. Let $f(k+1)$ be the least element of the set $\{a \in A \mid a > f(k)\}$. [This set is non-empty since A is infinite.]

This defines a function $f: \mathbb{Z}^+ \rightarrow A$.

This function is an injection since $f(k) < f(k+1)$ for all $k \geq 1$.

To see that f is a surjection notice that $f(n) \geq n$ (easily proved by induction). Given an element $a \in A$ then let m be the least integer such that $f(m) \geq a$ [we must have $m \leq a$ since $f(a) \geq a$]. Then by the definition of f we have $f(m) = a$.

Thus we have constructed a bijection $f: \mathbb{Z}^+ \rightarrow A$ showing that A is denumerable.

Hence each subset of \mathbb{Z}^+ is finite or denumerable.

(b) Now consider the general case. Let A be a subset of a denumerable set X . Since X is denumerable there is a bijection $g: \mathbb{Z}^+ \rightarrow X$. Then $\overleftarrow{g}(A)$ is a subset of \mathbb{Z}^+ and so finite or denumerable. But the restriction of g gives a bijection $\overleftarrow{g}(A) \rightarrow A$ and so A is finite or denumerable. \square

Theorem 14.2.6 (Cantor (1874)) *The set of rationals \mathbb{Q} is denumerable.*

Proof We may define a function

$$f: \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}^+$$

by $f(q) = (m, n)$ where m/n is the fraction representing q in its lowest terms (i.e. $q = m/n$, $n > 0$ and $\gcd(m, n) = 1$). This is clearly an injection. Its image is an infinite subset of the denumerable set $\mathbb{Z} \times \mathbb{Z}^+$ and so denumerable. Hence, since f defines a bijection onto its image, \mathbb{Q} is denumerable. \square

14.3 Uncountable sets

In the previous section we have seen that surprisingly many infinite sets are denumerable and indeed the examples there support Galileo's

suggestion that we can never say that one infinite set is larger than another. However, this is not the case. There are uncountable sets and we can give meaning to the statement that these are larger than the countable sets.

In 1874, Georg Cantor published a remarkable paper in which he proved not only that the set of rational numbers is denumerable but also that there is a hierarchy of infinite sets ordered by size (or cardinality).

Theorem 14.3.1 (Cantor (1874)) *The set of real numbers \mathbb{R} is uncountable.*

Constructing a proof. Notice that the statement that \mathbb{R} is uncountable is a non-existence statement: there does not exist a bijection $\mathbb{Z}^+ \rightarrow \mathbb{R}$. The method is to show how given any function $\mathbb{Z}^+ \rightarrow \mathbb{R}$ we can construct an element of \mathbb{R} which is not in the image of the function, not a value, so that the function is not a surjection and so not a bijection.

Each element $x \in \mathbb{R}$ may be represented as an infinite decimal

$$x = a_0.a_1a_2\dots a_n\dots$$

where $a_i \in \mathbb{Z}$ and, for $i \geq 1$, $0 \leq a_i \leq 9$. Some numbers (such as $(1.\dot{0} = 0.\dot{9})$) have two decimal expansions, one ending in recurring 0's (and so a finite decimal) and one ending in recurring 9's (see Problems III, Questions 26 and 27). For these we always use the first representation.

The method is now to start with a function $\mathbb{Z}^+ \rightarrow \mathbb{R}$ and to list the values of the function as infinite decimals. Having done this we have a beautifully simple, but ingenious, method (known as ‘Cantor’s diagonal process’) for writing down an infinite decimal not in the list and not representing the same real number as any member of the list. This infinite decimal represents a real number which is not a value of the function.

Proof Suppose that $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ is a function. Let

$$f(m) = a_{m0}.a_{m1}a_{m2}\dots a_{mn}\dots$$

as an infinite decimal (not ending in recurring 9’s).

Put $b = 0.b_1b_2\dots b_n\dots$ where

$$b_n = \begin{cases} 1 & \text{if } a_{nn} = 0, \\ 0 & \text{if } a_{nn} \neq 0. \end{cases}$$

Notice that this infinite decimal representing b certainly does not end

in recurring 9's. Furthermore, for each n , the n th decimal place of b , namely b_n , certainly differs from the n th decimal place of $f(n)$, namely a_{nn} . So $b \neq f(n)$. Since we have constructed an element of \mathbb{R} which is not a value of f this shows that f is not a surjection. Hence \mathbb{R} is not denumerable. \square

This result shows that the set of real numbers is in a real sense larger than the set of integers (or the set of rationals). We can make this precise as follows.

Definition 14.3.2 *Two sets X and Y have the same cardinality, written*

$|X| = |Y|$, if they are equipotent, i.e. there is a bijection $X \rightarrow Y$.

If there is an injection $X \rightarrow Y$ then we write $|X| \leq |Y|$. We write

$|X| < |Y|$ to mean that $|X| \leq |Y|$ and $|X| \neq |Y|$ and say that X has smaller cardinality than Y .

Thus Theorem 14.3.1 may be stated as $|\mathbb{R}| > |\mathbb{Z}^+|$ or $|\mathbb{R}| > \aleph_0$. One natural question now is whether there is a set intermediate in size between \mathbb{Z}^+ and \mathbb{R} . In 1878, Cantor conjectured that such sets did not exist, a statement which became known as the continuum hypothesis. Here the word 'continuum' is simply a name for the set of real numbers \mathbb{R} .

The continuum hypothesis. Every uncountable set of real numbers has the same cardinality as the set of all real numbers:

$$X \subseteq \mathbb{R} \text{ and } |X| > \aleph_0 \Rightarrow |X| = |\mathbb{R}|.$$

In 1963 the United States mathematician Paul Cohen proved the remarkable result that it is not possible either to prove or to disprove this hypothesis starting from the generally accepted assumptions (axioms) of set theory. This means that there are two alternative versions of set theory, one in which the continuum hypothesis is true and one in which it is false.

The other natural question arising from Theorem 14.3.1 is whether there is a set larger than \mathbb{R} . Cantor was able to show that there is such a set and indeed that, given any set, its power set is necessarily larger.

Theorem 14.3.3 For any set X , $|X| < |\mathcal{P}(X)|$.

Constructing a proof. Recall that $\mathcal{P}(X)$, the power set of X , is the set of all subsets of X (Definition 6.3.1).

It is easy to define an injection $X \rightarrow \mathcal{P}(X)$ by sending each element to the corresponding singleton subset. The interesting part is in proving that there is no bijection $X \rightarrow \mathcal{P}(X)$. The method is similar to that of Theorem 14.3.1: starting from any function $f: X \rightarrow \mathcal{P}(X)$ we construct an element of $\mathcal{P}(X)$, in other words a subset of X , which is not a value of f . It is easy to describe such an element but the reason why it is not a value is quite subtle.

Proof An injection $X \rightarrow \mathcal{P}(X)$ may be defined by $x \mapsto \{x\}$ and so $|X| \leq |\mathcal{P}(X)|$.

We prove that there is no bijection $X \rightarrow \mathcal{P}(X)$ by showing that any function $X \rightarrow \mathcal{P}(X)$ is not a surjection. Suppose that $f: X \rightarrow \mathcal{P}(X)$ is a function. We prove that this function is not a surjection and so not a bijection by exhibiting an element of $\mathcal{P}(X)$ which is not a value. Define

$$A = \{x \in X \mid x \notin f(x)\}.$$

[Notice that, for each $x \in X$, $f(x) \in \mathcal{P}(X)$ is a subset of X and so either $x \in f(x)$ or $x \notin f(x)$. Thus ' $x \notin f(x)$ ' is a predicate with a free variable taking values in X . The set of elements of X for which this predicate is true is a well-defined subset of X : this is the set A .]

To prove that A is not in the image of the function f we suppose for contradiction that it is, say $A = f(a)$ for some $a \in X$. Then A is a subset of X and a is an element of X , and so either $a \in A$ or $a \notin A$. We consider the possibilities in turn.

If $a \in A$ then, referring back to the predicate defining A , $a \notin f(a)$, which can be written $a \notin A$ contradicting our assumption that $a \in A$.

On the other hand, if $a \notin A$, then it does not satisfy the predicate defining A and so $a \in f(a)$, which can be written $a \in A$ contradicting our assumption that $a \notin A$.

So in either case we have a contradiction and so our initial assumption that A is in the image of f must be false and so f is not a surjection.

Hence, since there is no bijection $X \rightarrow \mathcal{P}(X)$ but there is an injection, $|X| < |\mathcal{P}(X)|$. \square

This is probably the most subtle proof in this book. However, once you have understood it, it appears to have the same glorious inevitability as the great Euclidean proofs by contradiction.

The most important result on finite sets was the pigeonhole principle (Theorem 11.1.2). This result does still hold for infinite sets.

Theorem 14.3.4 (Cantor–Schröder–Bernstein theorem) *Suppose that X and Y are non-empty sets such that $|X| > |Y|$. Then any function $f: X \rightarrow Y$ is not an injection, i.e. there exist distinct elements x_1 and $x_2 \in X$ such that $f(x_1) = f(x_2)$.*

The proof is omitted.†

This material on counting infinite sets may appear very abstract and obscure and indeed it was many years before it gained general acceptance. To give some idea of its power we will conclude by describing one result which Cantor obtained using his ideas.

Definition 14.3.5 *A real number is called algebraic if it satisfies a polynomial equation*

$$x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$$

with the coefficients a_i all rational. It is called transcendental if it is not algebraic.

Thus all rational numbers are algebraic (since m/n satisfies $nx - m = 0$) and $\sqrt{2}$ is algebraic (since it satisfies $x^2 = 2$). In 1844 the French mathematician Joseph Liouville gave an explicit construction of certain transcendental numbers‡ but it remained a problem to determine whether specific numbers are transcendental. In 1873, Charles Hermite (French) proved that e , the base of the natural logarithms, is transcendental, and these ideas were developed by Ferdinand Lindemann (German) to prove in 1882 that π is transcendental. This result finally proved that the ancient search for a ruler and compass construction to give a square of the same area as a given circle has no solution since it can be shown that any length which can be constructed from a given length is an algebraic multiple of the given length§. These arguments about specific numbers are quite delicate and it is still not known whether, for example, $\pi + e$ is transcendental.

† A proof may be found in D.J. Velleman, *How to prove it, a structured approach*, Cambridge University Press, 1994.

‡ A description of this construction may be found in R. Courant and H. Robbins, *What is mathematics?* Oxford University Press, 1941.

§ See R. Courant and H. Robbins, *op. cit.*

Cantor's remarkable result was that *most* real numbers are transcendental! He proved, using similar methods to the above proof of Theorem 14.2.6, that the set of algebraic numbers is denumerable (see Problems III, Question 28). It follows from Theorem 14.3.1 and Exercise 14.2 that the set of transcendental numbers is uncountable and it is in that sense that most real numbers are transcendental.

Exercises

14.1 Prove that if A is finite and B is denumerable then $A \cup B$ is denumerable.

14.2 Prove that if A and B are denumerable then $A \cup B$ is denumerable. Hence prove by contradiction that, if X is uncountable and a subset A is denumerable, then $X - A$ is uncountable.

14.3 Prove that if $\{A_n \mid n \in \mathbb{Z}^+\}$ is a denumerable set of pairwise disjoint denumerable sets then the union

$$\bigcup_{n \in \mathbb{Z}^+} A_n = \{x \mid x \in A_n \text{ for some } n \in \mathbb{Z}^+\}$$

is also denumerable.

14.4 Use the Cantor–Schröder–Bernstein theorem to prove that if $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$.

Problems III: Numbers and counting

1. Of the 182 students who are taking three first year core Mathematics modules (Reasoning, Algebra and Calculus), 129 like Reasoning, 129 like Algebra, 129 like Calculus, 85 like Reasoning and Algebra, 89 like Reasoning and Calculus, 86 like Algebra and Calculus, and 54 like all three modules. How many of the students like none of the core modules?
2. Of the 170 students who took all the first year core modules last year, 124 liked Reasoning, 124 liked Algebra, 124 liked Calculus, 10 liked only Reasoning, nobody liked only Algebra, 4 liked only Calculus and 2 liked none of the modules. How many students liked all three core modules?
3. At an international conference of 100 people, 75 speak English, 60 speak Spanish and 45 speak Swahili (and everyone present speaks at least one of these languages).
 - (i) What is the maximum possible number of these people who can speak only one language? In this case how many people speak only English, how many speak only Spanish, how many speak only Swahili, and how many speak all three?
 - (ii) What is the maximum number of people who speak only English? In this case what can be said about the number who speak only Spanish and the number who speak only Swahili?
 - (iii) Prove that the greater the number of people who speak all three languages, the greater the number of people who speak only one language.
4. Prove (by induction on n) the general inclusion–exclusion principle which may be stated as follows.

Let A_1, A_2, \dots, A_n be finite sets. For $I = \{i_1, i_2, \dots, i_r\} \subseteq \mathbb{N}_n$, write

$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_r}.$$

Then

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq I \subseteq \mathbb{N}_n} (-1)^{|I|-1} |A_I|,$$

summing over all non-empty subsets of \mathbb{N}_n .

5. Prove that a finite non-empty set of real numbers has a minimum element.

[This is the part of the proof of Proposition 11.2.3 left as an exercise.]

6. Suppose that A and B are non-empty finite sets of real numbers such that $A \subseteq B$. Prove that

$$\min B \leq \min A \leq \max A \leq \max B.$$

7. What is wrong with the following argument purporting to prove that for every non-empty finite set A of real numbers $\min A = \max A$?

Proof We prove by induction on n that if $|A| = n$ then $\min A = \max A$.

Base case: If $|A| = 1$ then A is a singleton set $A = \{a_1\}$ and $\min A = a_1 = \max A$.

Inductive step: Suppose that for some positive integer k the result is true for $n = k$. Let A be a set of real numbers with $|A| = k + 1$. Let $a_1 = \min A$ and $a_2 = \max A$. Then

$$\begin{aligned} a_1 &= \min(A - \{a_2\}) \\ &= \max(A - \{a_2\}) \quad (\text{by inductive hypothesis}) \\ &\geq \max(A - \{a_1, a_2\}) \quad (\text{by Question 6}) \\ &\geq \min(A - \{a_1, a_2\}) \quad (\text{by Question 6}) \\ &\geq \min(A - \{a_1\}) \quad (\text{by Question 6}), \\ &= \max(A - \{a_1\}) \quad (\text{by inductive hypothesis}) \\ &= a_2. \end{aligned}$$

Hence $a_1 \geq a_2$ and since clearly $a_1 \leq a_2$ this proves that $a_1 = a_2$ as required to deduce the result for $n = k + 1$ and so proving the inductive step.

Conclusion: Hence by induction on n , $\min A = \max A$ for a set of cardinality n for all positive integers n , and so for all finite sets. \square

8. Prove Lemma 10.1.4 by induction on m .

9. Prove Proposition 11.1.4: if $X \rightarrow \mathbb{N}_n$ is an injection, then X is finite and $|X| \leq n$.

10. Prove Theorem 11.1.6: given non-empty finite sets X and Y with $|X| < |Y|$ there does not exist a surjection $X \rightarrow Y$.

11. Use the pigeonhole principle and proof by contradiction to prove Theorem 11.1.7: given non-empty finite sets X and Y with $|X| = |Y|$, a function $X \rightarrow Y$ is an injection if and only if it is a surjection.

12. Suppose that there is an injection $f: \mathbb{Z}^+ \rightarrow X$. Prove by contradiction that X is an infinite set.

[Use Corollary 11.1.1 noting that, for any $n \geq 1$, f restricts to give an injection $\mathbb{N}_{n+1} \rightarrow X$.]

13. Find all the divisors of 126 and 180 and hence find the greatest common divisor (126, 180).

14. For $n \in \mathbb{Z}^+$, suppose that $A \subseteq \mathbb{N}_{2n}$ and $|A| = n + 1$. Prove that A contains a pair of distinct integers a, b such that a divides b .

[Let $f(a)$ be the greatest odd integer which divides a and apply the pigeonhole principle to f .]

15. Prove the induction principle from the well-ordering principle (see Example 11.2.2(c)).

[Prove the induction principle in the form of Axiom 7.5.1 by contradiction.]

16. Use the inclusion-exclusion principle (Question 4) to prove that the number of surjections $\mathbb{N}_m \rightarrow \mathbb{N}_n$ is given by

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \dots + (-1)^{n-1} \binom{n}{n-1} 1^m.$$

[For each $i \in \mathbb{N}_n$, let $A_i = \{ f: \mathbb{N}_m \rightarrow \mathbb{N}_n \mid i \text{ is not a value of } f \}$.]

Deduce that

$$n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \dots + (-1)^{n-1} \binom{n}{n-1} 1^n = n!$$

- 17.** A *derangement* of \mathbb{N}_n is a bijection $f: \mathbb{N}_n \rightarrow \mathbb{N}_n$ with no fixed points, i.e. $f(i) \neq i$ for all $i \in \mathbb{N}_n$. Use the inclusion-exclusion principle to prove that the number of derangements of \mathbb{N}_n is

$$n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots + (-1)^n \frac{1}{n!} \right).$$

[This means that the proportion of all permutations of \mathbb{N}_n which are derangements is $1/2! - 1/3! + 1/4! - \dots + (-1)^n 1/n! = 1 - 1/1! + 1/2! - 1/3! + 1/4! - \dots + (-1)^n 1/n!$. The reader may recognize this as the first part of the series for e^{-1} . It follows that for large values of n the probability that a permutation is a derangement is approximately $1/e$.]

- 18.** Suppose that X and Y are disjoint sets. Prove that the function

$$\bigcup_{i=0}^k \mathcal{P}_i(X) \times \mathcal{P}_{k-i}(Y) \rightarrow \mathcal{P}_k(X \cup Y)$$

defined by $(A, B) \mapsto A \cup B$ is a bijection. Deduce that

$$\binom{m+n}{k} = \sum_{i=0}^n \binom{m}{i} \binom{n}{k-i}.$$

Give an alternative proof of this result by induction on n using Proposition 12.2.8.

- 19.** Prove Leibniz's rule for higher order derivatives of products,

$$\frac{d^n(uv)}{dx^n} = \sum_{i=0}^n \binom{n}{i} \frac{d^i u}{dx^i} \frac{d^{n-i}v}{dx^{n-i}} \quad \text{for } n \in \mathbb{Z}^+,$$

by induction on n .

- 20.** Use the pigeonhole principle to prove that, given ten distinct positive integers less than 107, there exist two disjoint subsets with the same sum.

- 21.** Define the notion of inequality between two fractions by

$$\frac{a_1}{b_1} < \frac{a_2}{b_2} \Leftrightarrow \begin{cases} a_1 b_2 < a_2 b_1 & \text{if } b_1 b_2 > 0, \\ a_1 b_2 > a_2 b_1 & \text{if } b_1 b_2 < 0. \end{cases}$$

Prove that this definition leads to a well-defined notion of inequality between two rational numbers satisfying Axioms 3.1.2.

22. For a positive real number x and a rational number $q = m/n$ (where m and n are integers), define the power x^q to be $(x^{1/n})^m$. In this expression the integral power is defined in Problems I, Question 23 and $x^{1/n}$ is defined in Example 9.2.4(b).

Prove that this definition of rational powers is well-defined. With this definition prove the laws of exponents for any positive real numbers x and y and rational numbers p and q :

- (i) $x^q y^q = (xy)^q$;
- (ii) $x^{p+q} = x^p x^q$;
- (iii) $(x^p)^q = x^{pq}$.

23. Prove that there does not exist a rational number whose square is 10.

24. Find the first four decimal places of the infinite decimal representing $\sqrt{10}$ (without using a calculator!).

25. Find the rational number equal to the recurring infinite decimal 2.10012097̇.

26. Prove that each finite decimal may be written as an infinite decimal in two distinct ways:

$$\begin{aligned} a_0.a_1a_2\dots a_{n-1}a_n &= a_0.a_1a_2\dots a_{n-1}a_n\dot{0} \\ &= a_0.a_1a_2\dots a_{n-1}(a_n - 1)\dot{9}, \end{aligned}$$

where $a_n > 0$ if $n > 0$.

27. Prove that each real number is represented by a unique infinite decimal unless it is representable by a finite decimal, in which case it is representable by precisely two infinite decimals as described in the previous problem.

[Hint: Suppose that two infinite decimals represent the same number: $a_0.a_1a_2\dots a_n\dots = b_0.b_1b_2\dots b_n\dots$. Attempt to prove by induction that $a_n = b_n$ for all $n \geq 0$.]

- 28.** Prove that the number of polynomials of degree n with rational coefficients is denumerable. Deduce that the set of algebraic numbers (see Definition 14.3.5) is denumerable.

[Recall that a polynomial equation $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$ has at most n real roots.]

Part IV

Arithmetic

15

The division theorem

The remainder of this book illustrates how the methods of proof and the language of sets and functions introduced so far are applied in arithmetic, the theory of numbers. We begin in this chapter by discussing the elementary ideas of division and remainders which we all met at an early stage of our schooling. The formal treatment of this generalizes the discussion of odd and even integers in Section 11.3.

15.1 The division theorem

The main result of this chapter is the following.

Theorem 15.1.1 (The division theorem) *Let a and b be integers with $b > 0$. Then there are unique integers q and r such that*

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

This result should be very familiar from early school days. There, in the case of positive a , we meet the idea of ‘sharing’ a objects equally amongst b people: they each receive q objects with r ‘left over’. The number q is called the *quotient* and the number r is called the *remainder*.

In practice when we are given two numbers a and b we can find q either by division using various tricks we learnt at school or more commonly these days by means of a calculator. The calculator will give us a finite decimal which approximates the rational number a/b . The quotient q is then the greatest integer less than or equal to a/b which is given by the integer part of a/b when a is positive. We can then find r as $a - bq$.

Example 15.1.2 To find the quotient and remainder when $a = 1781293$ and $b = 1481$.

For these numbers a calculator gives $a/b \approx 1202.7637$ (or possibly 1202.7636 depending on the rounding system). Thus $q = 1202$ and so $r = 1781293 - 1481 \times 1202 = 1131$.

Example 15.1.3 To find the quotient and the remainder when $a = -7856123$ and $b = 9812$.

For these numbers a calculator gives $a/b \approx -800.66480$. Thus $q = -801$ (notice that we *increase* the absolute value of a negative number when we round *down* to the next integer) and so $r = a - bq = -7856123 + 9812 \times 801 = 3289$.

These examples demonstrate only that the division theorem is true in these specific numerical examples. We cannot base a general proof on this method since the construction of a decimal corresponding to a rational number depends in general on repeated use of the division theorem, the result we are trying to prove (see Exercise 15.6)! The proof of the theorem requires some care, if only because the result seems so obvious. It is not necessary to have a complete understanding of the proof in order to apply the theorem. It is common in learning mathematics to gain experience in how a theorem is used before fully understanding the proof; seeing how the theorem is used can help to clarify the full meaning of the theorem and so help in exploring the proof.

In the case of $b = 2$ we have already proved Theorem 15.1.1 as Proposition 11.3.4 for we proved there that a number a is odd if and only if $a = 2q + 1$ for some integer q . Since by definition a is even if and only if $a = 2q$ for some integer q and ‘odd’ is defined to mean ‘not even’, this result means that each integer a can be written uniquely in the form $a = 2q + r$ where $r = 0$ or $r = 1$. The number is even if and only if $r = 0$ and the number is odd if and only if $r = 1$.

The method of proof of the division theorem is a direct generalization of the proof of Proposition 11.3.4.

Constructing a proof. Notice that there are really two separate things to prove: that the numbers q and r exist (this is an example of an *existence theorem*) and that they are unique (a *uniqueness theorem*). It is common for students to omit the uniqueness part when asked to state the division theorem but as will be seen this is a very important part of the result for many applications.

But let us start with existence: it is necessary to show that given a and b as in the theorem there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

First of all notice that q and r determine each other and in particular $r = a - bq$. So we can remove all reference to r by restating the condition $0 \leq r < b$ as $0 \leq a - bq < b$ or equivalently $bq \leq a < b(q + 1)$. Thus we can describe what we need as follows.

Given	Goal
$a, b \in \mathbb{Z}$	
$b > 0$	$\exists q \in \mathbb{Z}, bq \leq a < b(q + 1)$

As in the proof of Proposition 11.3.4 it is convenient to deal first with the case of a non-negative. In this case as in the earlier proof we can get hold of the element q by defining it to be the maximum element of a certain finite set.

Observe that, if a is non-negative, then there is no difficulty in finding an integer k such that $bk \leq a$ for we can simply take $k = 0$. In fact if $a < b$ then we can simply take $q = 0$ giving $r = a$. Otherwise, we try the non-negative integers, $0, 1, 2, \dots$, in turn until we reach the first integer q such that $a < b(q + 1)$. (This is more or less what we do in practice when performing division although the long division methods we learnt at school give some tricks so that we do not have to try every number.) The point of the existence part of the theorem is that this process will eventually succeed.

To see this we introduce the set

$$A = \{ k \in \mathbb{Z} \mid k \geq 0 \text{ and } bk \leq a \}.$$

This is a non-empty set since $0 \in A$ and it is a finite set since $k \in A \Rightarrow bk \leq a \Rightarrow k \leq a/b$. Hence A will have a maximum element so that we can define $q = \max A$.

To ensure that this q is the number we want we must prove that $bq \leq a < b(q + 1)$. Let us sum up where we have got to.

Given	Goal
$q = \max A$	$bq \leq a$ $a < b(q + 1)$

The first goal is immediate since $q = \max A$ implies that $q \in A$. The second goal is a little more elusive. However, when we rewrite it in the form $b(q + 1) \not\leq a$ we see that it is actually the statement that $q + 1 \notin A$. So we can rewrite our strategy for this second goal as follows.

Given	Goal
$q = \max A$	$q + 1 \notin A$

This is really obvious from the definition of what is meant by the maximum element of a set and this is normally all that would be said to complete the proof. For a formal proof notice that the negative reformulation of the goal strongly suggests trying a proof by contradiction giving the following strategy.

Given	Goal
$q = \max A$ $q + 1 \in A$	contradiction

Now observe that if $q + 1 \in A$ then $q + 1 \leq \max A = q$, providing the required contradiction since we know that $q + 1 > q$.

To complete the proof it is necessary to consider the case when a is a negative integer.[†] As in the case of $b = 2$ in Proposition 11.3.4 we can prove the result for negative a by using the result for $-a$ which is positive.

We now write this proof out formally.

Proof of existence Suppose that $a \geq 0$. Consider the set

$$A = \{ k \in \mathbb{Z} \mid k \geq 0 \text{ and } bk \leq a \}.$$

This set is non-empty since $0 \in A$ and is finite since $k \in A \Rightarrow 0 \leq k \leq a$. So it contains a maximum element, $q = \max A$.

Now put $r = a - bq$ so that $a = bq + r$. To prove that q and r are as claimed in the theorem it remains to prove that $0 \leq r < b$. It is clear that $r \geq 0$ since, by the definition of q , $bq \leq a$. To prove that $r < b$ suppose for contradiction that $r \geq b$. Then $a - bq \geq b$ so that $b(q + 1) \leq a$, i.e. $q + 1 \in A$ contradicting the maximality of q . Hence $r < b$ as required to complete the proof of existence.

To complete the proof suppose that a is a negative integer. Then $-a$ is positive so that from what we have proved $-a = bq_1 + r_1$ for integers q_1 and r_1 with $0 \leq r_1 < b$. Thus $a = b(-q_1) - r_1$. We now consider two cases.

(i) If $r_1 = 0$, then $a = b(-q_1)$ and so we have an expression of the

[†] The argument given for non-negative a can be amended to include the case of negative a by replacing A by $A' = \{ k \in \mathbb{Z} \mid bk \leq a \}$, in other words allowing negative integers in the set A' . We can then define $q = \max A'$ once we are clear that A' has a maximum element. In this case the set A' is not a finite set for it contains all large negative integers but it can still be shown to have a maximum using the well-ordering principle. It seems simpler in this book to deal only with maximum values of finite sets and to prove this result for negative a by making use of the result for $-a$ since in practice this would be the way in which q and r would be found, as illustrated in Example 15.1.3.

required form with $q = -q_1$ and $r = 0$.

(ii) If $r_1 > 0$, then $a = b(-q_1) - r_1 = b(-q_1 - 1) + (b - r_1)$ and so we have an expression of the required form with $q = -q_1 - 1$ and $r = b - r_1$. Notice that, since $0 < r_1 < b$, we also have $0 < b - r_1 < b$. \square

Constructing a proof of uniqueness. The other part of the theorem is uniqueness. This says that if we have integers q_1, q_2, r_1, r_2 such that

$$a = bq_1 + r_1 = bq_2 + r_2, \quad 0 \leq r_1 < b \quad \text{and} \quad 0 \leq r_2 < b$$

then $q_1 = q_2$ and $r_1 = r_2$. As before, q_i determines r_i and so $q_1 = q_2 \Rightarrow r_1 = r_2$ which means that it is sufficient to prove that $q_1 = q_2$. We can reorder the pairs if necessary so that $q_1 \geq q_2$ which means that $r_1 = a - bq_1 \leq r_2 = a - bq_2$. This leaves us with the following strategy.

Given	Goal
$q_1, q_2 \in \mathbb{Z}$ $0 \leq a - bq_1 \leq a - bq_2 < b$	$q_1 = q_2$

But this is easy since $a - bq_1$ and $a - bq_2$ differ by a multiple of b and there isn't room for two distinct non-negative integers differing by a multiple of b within the set of non-negative integers less than b . Let us write the proof out properly straight away.

Proof of uniqueness Suppose that $a = bq_1 + r_1 = bq_2 + r_2$ with $0 \leq r_1, r_2 < b$. We must prove that $q_1 = q_2, r_1 = r_2$. To do this suppose, without loss of generality, that $q_1 \geq q_2$. Then $0 \leq r_1 = a - bq_1 \leq r_2 = a - bq_2 < b$. This means that $0 \leq (a - bq_2) - (a - bq_1) < b$ so that $0 \leq b(q_1 - q_2) < b$ which implies that $0 \leq q_1 - q_2 < 1$. But since $q_1 - q_2$ is an integer it follows that $q_1 - q_2 = 0$, i.e. $q_1 = q_2$ from which it follows also that $r_1 (= a - bq_1) = r_2 (= a - bq_2)$. \square

15.2 Some applications

The division theorem will be fundamental for the number theory in the remainder of this book. In this chapter we content ourselves with a couple of applications concerning squares.

First of all we prove a result which was asserted without proof in Exercise 13.1.

Proposition 15.2.1 *Let a be an integer. Then a^2 is divisible by 3 if and only if a is divisible by 3.*

Constructing a proof. The proof of ‘3 divides $a \Rightarrow 3$ divides a^2 ’ is easy.

What is required for the converse can be summarized as follows.

Given	Goal
$a \in \mathbb{Z}$ 3 divides a^2	3 divides a

If we try a direct argument we get something like: since 3 divides a^2 , $a^2 = 3q$ for some integer q so that $a = 3(q/a)$. To complete the proof we need to know that a divides q which seems to be no easier than what we are trying to prove. The problem is that it is difficult to get back to a from a^2 and this suggests trying a proof by contradiction. This gives the following strategy.

Given	Goal
$a \in \mathbb{Z}$ 3 divides a^2 3 does not divide a	contradiction

Now the uniqueness part of the division theorem enables us to reformulate the negative statement that 3 does not divide a as the positive statement that the remainder after dividing a by 3 is 1 or 2, i.e. $a = 3q+1$ or $a = 3q+2$ for some $q \in \mathbb{Z}$. From this it easily follows that a^2 is not divisible by 3 giving the required contradiction.

It may be useful to formulate the way in which we are using the uniqueness part of the division theorem as an explicit corollary.

Corollary 15.2.2 *Let a and b be integers with $b > 0$ and suppose that $a = bq + r$ for integers q and r with $0 \leq q < r$. Then b divides a if and only if $r = 0$ (or equivalently, b does not divide a if and only if $r > 0$).*

Constructing a proof. The point here is that if b divides a then, for some integer q_1 , $a = bq_1 = bq_1 + r_1$ with $r_1 = 0$. So if $a = bq + r$ with $0 < r < q$ then (q, r) and $(q_1, 0)$ would be two distinct solutions to the division problem, contradicting the uniqueness part of the division theorem.

Proof This follows immediately from the uniqueness part of the division theorem, for b divides a if and only if $a = bq$ for some integer q if and only if $r = 0$. □

Proof of Proposition 15.2.1 First of all notice that, if a is divisible by 3, then $a = 3q$ and so $a^2 = 9q^2 = 3(3q^2)$ is divisible by 3.

For the converse suppose that a^2 is divisible by 3 and, for contradiction, that a is not divisible by 3. Then, by the division theorem, $a = 3q + 1$ or $a = 3q + 2$. However,

$$a = 3q + 1 \Rightarrow a^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1,$$

and similarly

$$a = 3q + 2 \Rightarrow a^2 = 3(3q^2 + 4q + 1) + 1.$$

Hence in either case the remainder is non-zero and so, by the division theorem, a^2 is not divisible by 3, giving the required contradiction. Hence, if a^2 is divisible by 3 then so is a as required. \square

If we examine the above proof we see that it contains the demonstration that, for all integers a , the integer a^2 has remainder 0 or 1 after division by 3, i.e. it never has remainder 2. We can use this fact to recognize that an integer is not a square.

Proposition 15.2.3 *If $n \in \mathbb{Z}^+$ is a perfect square (i.e. the square of an integer) then $n = 3q$ or $n = 3q + 1$ for some $q \in \mathbb{Z}$.*

Proof If n is a perfect square then $n = a^2$ for some $a \in \mathbb{Z}$. By the division theorem $a = 3q_0$ or $a = 3q_0 + 1$ or $a = 3q_0 + 2$ for some $q_0 \in \mathbb{Z}$. Hence $a^2 = 3(3q_0^2)$ or $a^2 = 3(3q_0^2 + 2q_0) + 1$ or $a^2 = 3(3q_0^2 + 4q_0 + 1) + 1$ so that $n = 3q$ or $n = 3q + 1$ as required. \square

Example 15.2.4 The integer 1111111111 is not the square of an integer. For $1111111111 = 3 \times 3703703703 + 2$ so that 1111111111 has remainder 2 after division by 3. Hence by the proposition it is not a perfect square.

Exercises

15.1 For a and b as follows write down q and r such that $a = bq + r$ and $0 \leq r < b$.

- (i) $a = 100, b = 3;$
- (ii) $a = 3, b = 100;$
- (iii) $a = 100, b = 7;$
- (iv) $a = -100, b = 7;$

- (v) $a = -105, b = 7;$
- (vi) $a = -3, b = 105;$
- (vii) $a = 7684, b = 4148;$
- (viii) $a = -7684, b = 4148;$
- (ix) $a = 1234567, b = 1357;$
- (x) $a = 0, b = 17.$

15.2 Prove that an integer a is divisible by 5 if and only if a^2 is divisible by 5.

15.3 Prove that, for integers a , a^2 is divisible by 3 if and only if it is divisible by 9.

15.4 Prove that 98765432 is not the square of an integer.

15.5 Prove that if n is a perfect square then $n = 4q$ or $n = 4q + 1$ for some $q \in \mathbb{Z}$. Deduce that 1234567 is not a perfect square.

15.6 By repeated use of the division theorem find the infinite decimal representing the rational number $5/7$.

16

The Euclidean algorithm

In this chapter we return to the idea of the greatest common divisor introduced in Chapter 11, introducing an extremely efficient way of calculating this number known as the Euclidean algorithm. As well as being an efficient method of calculation this method has quite far-reaching consequences some of which will be considered in subsequent chapters. This approach can be applied in several other situations in algebra and number theory which the reader will meet if these areas are explored further.

16.1 Finding the greatest common divisor

First of all recall the following definition.

Definition 11.3.1 Let a and b be two integers, at least one of which is non-zero. Then the greatest common divisor of a and b is the unique positive integer d such that

- (i) d is a common divisor, i.e. d divides a and d divides b ,
- (ii) d is greater than every other common divisor:

$$c \text{ divides } a \text{ and } c \text{ divides } b \Rightarrow c \leq d.$$

We denote the greatest common divisor of a and b by $\gcd(a, b)$ or simply by (a, b) .

In Chapter 11 we showed how to find the greatest common divisor by finding all the common divisors. This method is extremely tedious if the numbers are at all large. A more efficient process, involving repeated

application of the division theorem, is given in Book Seven of the *Elements* of Euclid and was discovered independently in China. It is now known as *the Euclidean algorithm*.

To begin with notice that d divides a if and only if d divides $-a$ and so it is sufficient to deal with the greatest common factor of two non-negative integers. Furthermore, if a is positive then $\gcd(a, 0) = a$ and so we may as well restrict attention to strictly positive integers. Thus we consider how to find the greatest common divisor of two positive integers a and b .

The method is based on two key observations. The first of these is very simple.

Lemma 16.1.1 *If a positive integer b divides a then b must be the greatest common divisor of a and b , i.e. $\gcd(a, b) = b$.*

Proof If b divides a , then b is a common divisor since it clearly also divides b . However, nothing larger than b can divide b and so it must be the greatest common divisor. \square

On the other hand, if b does not divide a , then the division theorem enables us to write

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

The second key observation is the following result.

Lemma 16.1.2 *For non-zero integers a and b suppose that*

$$a = bq + r \quad \text{where } q, r \in \mathbb{Z}.$$

Then $\gcd(a, b) = \gcd(b, r)$.

Before considering the proof of this result let us consider an example of how these two observations may be used to find greatest common divisors.

Example 16.1.3 To find the greatest common divisor of 72 and 30 (Example 11.3.3 again).

We begin by dividing 30 into 72 which gives

$$72 = 30 \times 2 + 12$$

and so, by Lemma 16.1.2, $\boxed{\gcd(72, 30) = \gcd(30, 12)}$.

Now we can repeat the process dividing 12 into 30:

$$30 = 12 \times 2 + 6$$

giving $(30, 12) = (12, 6)$.

Finally, since 6 divides 12, we have $(12, 6) = 6$ by Lemma 16.1.1.

Putting all this together we get

$$(72, 30) = (30, 12) = (12, 6) = 6$$

and so the greatest common divisor of 72 and 30 is 6.

This calculation is an example of the Euclidean algorithm in action. The Euclidean algorithm is stated below as Theorem 16.2.1. But before coming to this we prove Lemma 16.1.2.

Constructing a proof of Lemma 16.1.2.

Given	Goal
$a = bq + r$	$\gcd(a, b) = \gcd(b, r)$

The difficulty here is that the definition of greatest common divisor is quite complicated and does not give (a, b) as a simple formula in terms of a and b . In fact this is one of those cases when it easier to prove something slightly stronger than needed. Recall that

$$D(a, b) = \{ c \in \mathbb{Z} \mid c \text{ divides } a \text{ and } c \text{ divides } b \},$$

the set of common divisors of a and b , and similarly

$$D(b, r) = \{ c \in \mathbb{Z} \mid c \text{ divides } b \text{ and } c \text{ divides } r \},$$

the set of common divisors of b and r . If we can prove that $D(a, b) = D(b, r)$ then we are home because $\gcd(a, b)$ is the greatest element of the first set and $\gcd(b, r)$ is the greatest element of the second set.

But this is easy. Recall that proving two sets equal amounts to proving that each is a subset of the other, in this case $D(a, b) \subseteq D(b, r)$ and $D(b, r) \subseteq D(a, b)$. To show that $D(a, b) \subseteq D(b, r)$ we need to prove that $c \in D(a, b) \Rightarrow c \in D(b, r)$. We can summarize what this involves as follows.

Given	Goal
$a = bq + r$	
$c \in \mathbb{Z}$	
$c \text{ divides } a$	$c \text{ divides } b$
$c \text{ divides } b$	$c \text{ divides } r$

One of the goals, c divides b , is already given. For the other we need to remember the definition of ‘divides’.

Given	Goal
$a = bq + r$	
$a = q_1 c$	
$b = q_2 c$	$\exists k \in \mathbb{Z}, r = kc$

This is immediate since $r = a - bq = q_1 c - q_2 cq = (q_1 - q_2 q)c$ and so we can take $k = q_1 - q_2 q$.

The proof that $D(b, r) \subseteq D(a, b)$ is almost identical (see Exercise 16.4). When we come to write out a formal proof it is quite short.

Proof If c divides a and c divides b then $a = cq_1$ and $b = cq_2$ for some integers q_1 and q_2 . In this case $r = a - bq = q_1 c - cq_2 q = c(q_1 - q_2 q)$ so that c divides r . Thus c is a common divisor of a and b implies that c is a common divisor of b and r . Conversely, if c is a common divisor of b and r then c is a common divisor of a and b . Hence the common divisors of a and b are the same as the common divisors of b and r and so their greatest common divisors are the same. \square

We have now justified the calculation in Example 16.1.3. So we go on to describe the method in general as an algorithm.

16.2 The Euclidean algorithm

Theorem 16.2.1 (The Euclidean algorithm) Suppose that a and b are positive integers. The following procedure defines a finite sequence of positive integers a_0, a_1, \dots, a_n such that $a_n = (a, b)$, the greatest common divisor of a and b .

Put $a_0 = a, a_1 = b$.

Step k : For $k \geq 1$, suppose that a_0, a_1, \dots, a_k have been defined. Using the division theorem write

$$a_{k-1} = a_k q_k + r_k \quad \text{where } q_k, r_k \in \mathbb{Z} \text{ and } 0 \leq r_k < a_k.$$

If $r_k = 0$, stop.

Otherwise, put $a_{k+1} = r_k$ and continue with step $k + 1$.

Remarks 16.2.2 An *algorithm*† is a sequence of steps necessarily leading to a desired conclusion. Notice that since $b = a_1 > a_2 > \dots > a_n > 0$ the Euclidean algorithm necessarily terminates after at most b steps. If there were examples where the number of steps was as many as this then it would be a poor algorithm. However, it is known‡ that the number of steps required to find the greatest common divisor of a and b using the Euclidean algorithm does not exceed five times the number of decimal digits in the smaller of a and b .

Numerical algorithms are very well suited to being programmed on a computer. We can formulate the Euclidean algorithm as a BASIC program as follows.

```

10      INPUT "FIRST NUMBER =", A
20      INPUT "SECOND NUMBER =", B
30      Q=INT(A/B)
40      R=A-B*Q
50      IF R > 0 THEN GOTO 60 ELSE GOTO 90
60      A=B
70      B=R
80      GOTO 30
90      PRINT "GCD =" B

```

Notice that BASIC has within it a command INT which gives the quotient in the division theorem. If we did not have this command then it would be easy to write a subprogram to achieve that (see Problems IV, Question 9). Even if you are unfamiliar with programming you should be able to work through this program. When you run it the first two lines ask you to input the two numbers whose greatest common divisor is sought. Then lines 30 to 50 describe a single step of the algorithm. Line 50 examines whether the last remainder is zero in order to decide whether the algorithm is complete: if it is then the program goes to line 90 and prints out the answer; if it is not then lines 70 and 80 redefine the numbers A and B before applying the division algorithm again in order to

† This word derives from the name of the ninth century arabic scholar Mohammed ibn-Musa al-Khowarizmi whose two books on arithmetic and algebra were very influential in the spread of the Hindu–Arabic numeral system to Europe. The word ‘algebra’ also comes from this same source, from the title of his book *Al-jabr wa'l muqâbalah* through which arabic algebra passed to Europe (see C.B. Boyer and U.C. Merzbach, *A history of mathematics*, Wiley, Second edition 1989).

‡ This result was proved by Gabriel Lamé in 1845 (see Problems IV, Question 8).

obtain the next remainder. Rather than using all those subscripts that appear in the statement of the theorem we change the meaning of A, B, Q and R with each step of the algorithm. For example, in line 60 'A=B' means 'define A to be the number B'. As a result the previous meaning of A is forgotten – this is a special use of the symbol '=' in computer programs†.

In terms of this program the theorem states simply that if the program is run then on inputting any two positive numbers the program will terminate by printing the greatest common divisor.

Notice that Example 11.3.3 illustrates an alternative algorithm for the greatest common divisor: simply try all the positive integers less than or equal to the smaller of a and b in turn. However, this is essentially useless for all but the smallest numbers: imagine using it for two six figure numbers. The Euclidean algorithm can deal with six figure numbers quite easily by hand (see Exercise 16.2).

Example 16.2.3 To find the greatest common divisor of 232 and 136.

The Euclidean algorithm gives the following.

$$\begin{aligned} \text{Step 1: } 232 &= 136 \times 1 + 96 \\ \text{Step 2: } 136 &= 96 \times 1 + 40 \\ \text{Step 3: } 96 &= 40 \times 2 + 16 \\ \text{Step 4: } 40 &= 16 \times 2 + 8 \\ \text{Step 5: } 16 &= 8 \times 2 + 0 \end{aligned}$$

Hence $(232, 136) = 8$.

In this case $a_0 = 232$, $a_1 = 136$, $a_2 = 96$, $a_3 = 40$, $a_4 = 16$, $a_5 = 8$.

In practice when we are applying the division theorem in these calculations we can use a calculator to find an approximate value for a/b . Then the quotient q is the greatest integer less than or equal to a/b and $r = a - bq$ as illustrated in Examples 15.1.2 and 15.1.3.

Observe that it is sufficient to write down simply the numbers a_k in a column. At each stage we simply subtract enough multiples of the last number written down from the previous one in order to get a smaller number. Thus for the above example we could write the following (where the information in brackets is there simply to indicate what has been

† It is even correct to write 'A=A+1' in a computer program, meaning that the value of A should be increased by 1. It is not correct to write 'put $a = a + 1$ ' when writing mathematics – although such barbarisms are sometimes used.

done).

$$\begin{array}{r}
 232 \\
 136 \\
 96 \quad (= 232 - 136 \times 1) \\
 40 \quad (= 136 - 96 \times 1) \\
 16 \quad (= 96 - 40 \times 2) \\
 8 \quad (= 40 - 16 \times 2) \\
 0 \quad (= 16 - 8 \times 2)
 \end{array}$$

Or more briefly we could write

$$\begin{array}{r}
 232 \\
 136 \quad (-1) \\
 96 \quad (-1) \\
 40 \quad (-2) \\
 16 \quad (-2) \\
 8 \quad (-2) \\
 0
 \end{array}$$

where the numbers in brackets indicate what multiple of each number is subtracted from the one above in order to obtain the next number – namely the quotient when you divide that number into the one above.

If we do write out the calculation in this way, as we will in this book, it is important to realize that it may be meaningless to a reader who has not had the conventions explained. In almost all mathematical writing there is a lot of convention, if only about the meanings of symbols, and Humpty Dumpty's principle applies here. In a case like this it is useful to at least indicate what we are doing, say by prefacing the calculation by stating 'Applying the Euclidean algorithm gives the following sequence of remainders.'

Constructing a proof of Theorem 16.2.1. The above example illustrates the general proof. Notice how repeated use of Lemma 16.1.2 implies that 8 is the greatest common divisor:

$$(232, 136) = (136, 96) = (96, 40) = (40, 16) = (16, 8) = 8.$$

Turning to the general case, first of all notice that repeating the steps in the theorem does lead to a *finite* sequence of positive integers a_0, a_1, \dots, a_n where $n \leq b$ since $a_{k+1} < a_k$.

Now, for $1 \leq k < n$, $a_{k-1} = a_k q_k + a_{k+1}$. Hence, just as in the example, by Lemma 16.1.2, $(a_{k-1}, a_k) = (a_k, a_{k+1})$. Furthermore, since

$a_{n-1} = a_n q_n$, it follows (Lemma 16.1.1) that $(a_{n-1}, a_n) = a_n$. Hence $(a, b) = (a_0, a_1) = (a_1, a_2) = \dots = (a_{n-1}, a_n) = a_n$.

The dots in this proof indicating ‘and so on’ should alert us to the fact that strictly speaking this proof is making use of the induction principle. The style of presentation used in the above paragraph is normally considered acceptable but we could write this out as a formal proof by induction as follows.

Proof of Theorem 16.2.1. Let $P(n)$ be the statement that, given any sequence of positive integers numbers a_0, a_1, \dots, a_n generated by $n - 1$ steps of the Euclidean algorithm (but not necessarily terminating after n steps), $(a_0, a_1) = (a_{n-1}, a_n)$.

We prove that $P(n)$ is true for all positive integers n by induction on n . Base case: $P(1)$ simply says $(a_0, a_1) = (a_0, a_1)$ which is certainly true! Inductive step: Suppose now that for some $k \geq 1$ the result is true for $n = k$. Then, given a sequence of numbers a_0, a_1, \dots, a_{k+1} generated by k steps of the Euclidean algorithm, $a_{k-1} = a_k q_k + a_{k+1}$ and so by Lemma 16.1.2 $(a_{k-1}, a_k) = (a_k, a_{k+1})$. But, by inductive hypothesis, $(a_{k-1}, a_k) = (a_0, a_1)$ and so $(a_k, a_{k+1}) = (a_0, a_1)$ as required to prove the result for $n = k + 1$.

Hence, by induction the statement $P(n)$ is true for all positive integers n .

Now to complete the proof, using the notation of the theorem it follows that $(a, b) = (a_0, a_1) = (a_{n-1}, a_n)$. But since $r_n = 0$ it follows that a_n divides a_{n-1} and so $(a_{n-1}, a_n) = a_n$, i.e. $(a, b) = a_n$. \square

Exercises

16.1 Use the Euclidean algorithm to find the greatest common divisor of 7684 and 4148.

16.2 Use the Euclidean algorithm to find the greatest common divisor of 110233442 and 1102246.

16.3 What difference does the order of the two numbers a and b make when we calculate their greatest common divisor using the Euclidean algorithm?

16.4 Suppose that a, b, q and r are integers such that $a = bq + r$. Prove that $D(b, r) \subseteq D(a, b)$.

17

Consequences of the Euclidean algorithm

In the previous chapter it was explained how the Euclidean algorithm provides an extremely efficient method for calculating the greatest common divisor of two integers. However, it does much more than this. In particular it enables us to see how to write the greatest common divisor in terms of the numbers we started with as an *integral linear combination*. We will see that this result is of both numerical and theoretical interest.

17.1 Integral linear combinations

Theorem 17.1.1 *Let a, b be integers at least one of which is non-zero with greatest common divisor $\gcd(a, b)$. Then there exist integers m and n such that*

$$\gcd(a, b) = am + bn.$$

Definition 17.1.2 *Given integers a and b , we say that an integer c is an integral linear combination of a and b if there exist integers m and n such that*

$$c = am + bn.$$

Thus Theorem 17.1.1 asserts that the greatest common divisor of two integers is an integral linear combination of the two integers.

Before giving the general proof we illustrate the result by considering an example.

Example 17.1.3 Consider Example 16.2.3 in which it was shown that $\gcd(232, 136) = 8$. The full details of the Euclidean algorithm were as follows.

$$\begin{aligned} \text{Step 1: } 232 &= 136 \times 1 + 96 \\ \text{Step 2: } 136 &= 96 \times 1 + 40 \\ \text{Step 3: } 96 &= 40 \times 2 + 16 \\ \text{Step 4: } 40 &= 16 \times 2 + 8 \\ \text{Step 5: } 16 &= 8 \times 2 + 0 \end{aligned}$$

If we examine these equations we see that we can use them to provide an expressions for each term in the sequence of remainders generated by the algorithm as a linear combination of the previous two terms.

$$\begin{aligned} \text{Step 1: } 96 &= 232 \times 1 - 136 \times 1 \\ \text{Step 2: } 40 &= 136 \times 1 - 96 \times 1 \\ \text{Step 3: } 16 &= 96 \times 1 - 40 \times 2 \\ \text{Step 4: } 8 &= 40 \times 1 - 16 \times 2 \end{aligned}$$

Now if we substitute each of these equations in the next we get an expression for 8 as a linear combination of 232 and 136.

There are two ways of organizing this calculation.

Method 1: The usual method is to work up through the equations as follows.

$$\begin{aligned} 8 &= 40 \times 1 - 16 \times 2 \text{ (by Step 4)} \\ &= 40 \times 1 - (96 \times 1 - 40 \times 2) \times 2 \text{ (by Step 3)} \\ &= 96 \times (-2) + 40 \times 5 \text{ (collecting up terms)} \\ &= 96 \times (-2) + (136 \times 1 - 96 \times 1) \times 5 \text{ (by Step 2)} \\ &= 136 \times 5 + 96 \times (-7) \\ &= 136 \times 5 + (232 \times 1 - 136 \times 1) \times (-7) \text{ (by Step 1)} \\ &= 232 \times (-7) + 136 \times 12 \end{aligned}$$

Personally I find this method rather cumbersome. Whatever method is used care with signs is required but I find that slips are less likely using a second method.

Method 2: This method is to write each of the numbers generated by the Euclidean algorithm in turn as an integral linear combination of the

Chapter 17: Consequences of the Euclidean algorithm 209

required form working down through the above equations. The numbers we start with, in this case 232 and 136, are easy to deal with since

$$232 = 232 \times 1 + 136 \times 0$$

and

$$136 = 232 \times 0 + 136 \times 1.$$

Step 1 of the Euclidean algorithm gives the following.

$$\begin{aligned} 96 &= 232 - 136 \\ &= 232 \times 1 + 136 \times (-1). \end{aligned}$$

Step 2 gives the following.

$$\begin{aligned} 40 &= 136 - 96 \\ &= (232 \times 0 + 136 \times 1) - (232 \times 1 + 136 \times (-1)) \\ &= 232 \times (0 - 1) + 136(1 - (-1)) \\ &= 232 \times (-1) + 136 \times 2. \end{aligned}$$

And continuing in this way we obtain the following sequence of equations.

$$\begin{array}{llll} 232 &= 232 \times 1 &+ 136 \times 0 \\ 136 &= 232 \times 0 &+ 136 \times 1 &(-1) \\ \text{Step 1: } 96 &= 232 \times 1 &+ 136 \times (-1) &(-1) \\ \text{Step 2: } 40 &= 232 \times (-1) + 136 \times 2 &&(-2) \\ \text{Step 3: } 16 &= 232 \times 3 &+ 136 \times (-5) &(-2) \\ \text{Step 4: } 8 &= 232 \times (-7) + 136 \times 12 &&(-2) \\ \text{Step 5: } 0 &&& \end{array}$$

Hence, an expression as required is $8 = 232 \times (-7) + 136 \times 12$. We stop the calculation at Step 4 because we have obtained what we want.

Remember that the numbers in brackets tell what multiple of each line must be subtracted from the previous line in order to get the next. If we set out the calculation in this way then at each step we do just the same calculation with the multipliers of 232 and 136. So for example, for Step 2, we simply get $0 - 1 = -1$ as the multiplier of 232 and $1 - (-1) = 2$ as the multiplier of 136; and, for Step 3, $1 - (-1) \times 2 = 3$ and $-1 - 2 \times 2 = -5$.

Just as the first column of figures was all that it was necessary to write down when finding the greatest common divisor, this list of equations is all that is needed when finding the integral linear combination coefficients.

Notice that you can readily check whether you have successfully manoeuvred yourself through the calculation by checking that the values you have obtained for m and n actually work. In this case $232 \times (-7) + 136 \times 12 = -1624 + 1632 = 8$. This illustrates the fact that the best way of proving that you have a solution to an equation is by substituting in the values you have found and confirming that they do satisfy the equation.

In this book I will use the second method. Whatever method you use it is important when doing numerical examples always to check that your solutions work since numerical slips are so easy.

Constructing a proof of Theorem 17.1.1 The second method of organizing the above calculation can be used to prove that each of the numbers in the sequence a_0, a_1, \dots, a_n generated by the Euclidean algorithm (and in particular the greatest common divisor) is an integral linear combination of a and b .

As in the proof of the Euclidean algorithm itself the proof is by induction on the length of a sequence of numbers generated by the Euclidean algorithm.

Proof of Theorem 17.1.1 We first of all prove the result in the case when a and b are non-negative.

We prove by induction on n that a sequence of positive integers a_0, a_1, \dots, a_n generated by the first $n - 1$ steps of the Euclidean algorithm are integral linear combinations of a and b .

Base case: The numbers a_0 and a_1 have this form since $a_0 = a = a \times 1 + b \times 0$ and $a_1 = b = a \times 0 + b \times 1$.

Inductive step: Now suppose as inductive hypothesis that, for some $k \geq 1$, the result holds for $n = k$ so that, for $0 \leq i \leq k$, $a_i = am_i + bn_i$ where $m_i, n_i \in \mathbb{Z}$. To prove the result for $n = k + 1$ observe that

$$\begin{aligned} a_{k+1} &= a_{k-1} - a_k q_k \quad \text{using the notation of Theorem 16.2.1} \\ &= (am_{k-1} + bn_{k-1}) - (am_k + bn_k)q_k \\ &\quad \text{by inductive hypothesis} \\ &= a(m_{k-1} - m_k q_k) + b(n_{k-1} - n_k q_k) \end{aligned}$$

expressing a_{k+1} as an integral linear combination of a and b and completing the inductive step.

Hence by induction the result is true for all positive integers n .

In particular the greatest common divisor, the final term in the com-

plete sequence of numbers generated by the Euclidean algorithm, is an integral linear combination of a and b .

To obtain the general result observe for example that if a is negative and b non-negative then by the above argument, since $-a$ is positive, there are integers m_1 and n_1 such that

$$(-a)m_1 + bn_1 = \gcd(-a, b) = \gcd(a, b).$$

This means that the required integers are given by $m = -m_1$, $n = n_1$. Similar methods work for b negative or a and b both negative. \square

17.2 An alternative definition of the greatest common divisor

The definition of greatest common factor which was introduced in Chapter 11 is not entirely standard. It reads (essentially) as follows.

Definition 11.3.1 *Let a and b be two integers, at least one of which is non-zero. Then the greatest common divisor of a and b is the unique positive integer d such that*

- (i) *d is a common divisor, i.e. d divides a and d divides b ,*
- (ii) *d is greater than every other common divisor:*

$$c \text{ divides } a \text{ and } c \text{ divides } b \Rightarrow c \leq d.$$

We denote the greatest common divisor of a and b by $\gcd(a, b)$ or sometimes $\gcd(a, b)$.

It is usual to have the following stronger condition in place of (ii) in the above:

- (ii)' *d is a multiple of any other common divisor:*

$$c \text{ divides } a \text{ and } c \text{ divides } b \Rightarrow c \text{ divides } d.$$

This definition is not used in this book because it is not immediately obvious from it that two integers will have a greatest common divisor. It also seems simplest to have a definition which reflects as closely as possible what the words ‘greatest common divisor’ might reasonably be expected to mean!

In fact these two definitions are equivalent since the apparently more stringent condition (ii)' is automatically satisfied by a number d which satisfies our definition of a greatest common divisor. This is a simple consequence of Theorem 17.1.1 as follows.

Corollary 17.2.1 Let $d = \gcd(a, b)$ be the greatest common divisor of the integers a and b . Then c is a common divisor of a and b if and only if c divides d , i.e. $D(a, b) = D(d)$.

Example 17.2.2 Recall from Example 11.3.3 that the set of common divisors of 30 and 72 is

$$D(30, 72) = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

This is precisely $D(6)$, the set of divisors of the greatest common divisor $(30, 72) = 6$.

Proof of Corollary 17.2.1 Notice that the statement ‘if and only if’ indicates that two separate results must be proved.

Proof of ‘if’: Suppose that c divides d . By definition d divides a and d divides b . But c divides d which divides a immediately implies from the definition of ‘divides’ that c divides a (see Exercise 3.2) and in the same way c divides b so that c is a common divisor as required.

Proof of ‘only if’: By Theorem 17.1.1, $d = am + bn$ for some $m, n \in \mathbb{Z}$. Now if c is a common divisor of a and b then c divides a and c divides b so that $a = cq_1$ and $b = cq_2$ for some integers q_1 and q_2 . In this case $d = (cq_1)m + (cq_2)n = c(q_1m + q_2n)$ so that c divides d as required. \square

17.3 Coprime pairs

Recall the following definition.

Definition 11.3.2 Two integers a and b , not both zero, are called coprime when $(a, b) = 1$, in other words their only common factors are 1 and -1 .

Proposition 17.3.1 Two non-zero integers a and b are coprime if and only if there exist integers m and n such that

$$am + bn = 1.$$

Constructing a proof. The necessity of the existence of m and n is a special case of Theorem 17.1.1.

In the other direction we are starting from an existence statement. The simplest way to use such a statement is to take particular elements which satisfy the predicate. So in this case we use integers m_0 and n_0

Chapter 17: Consequences of the Euclidean algorithm 213

such that $am_0 + bn_0 = 1$ – we are supposing that such integers exist. It was explained in Chapter 7 that it is usual to use the same symbols as in the existence statement for specific elements for which the predicate is true, in this case m and n rather than the new symbols m_0 and n_0 , but here it seems clearer to use different symbols for specific elements.

This leads to the following summary of what is required.

Given	Goal
integers m_0, n_0 $am_0 + bn_0 = 1$	$(a, b) = 1$

To proceed we need to unpack the definition of coprime. To show that $(a, b) = 1$ we must show that the only common divisors of a and b are ± 1 , i.e.

$$c \text{ divides } a \text{ and } c \text{ divides } b \Rightarrow c = \pm 1 \text{ for integers } c.$$

If we now try the direct method of proof this gives the following strategy.

Given	Goal
$m_0, n_0 \in \mathbb{Z}$ $am_0 + bn_0 = 1$ $c \in \mathbb{Z}$ $c \text{ divides } a$ $c \text{ divides } b$	$c = \pm 1$

Having got this far we can move on to the formal proof which is constructed easily by spelling out the definition of ‘divides’.

Proof If a and b are coprime then the existence of integers m and n as required is a special case of Theorem 17.1.1.

For the converse suppose that m_0 and n_0 are integers such that $am_0 + bn_0 = 1$. Suppose that c is a common divisor of a and b . Then, since c divides a , $a = cq_1$ for some $q_1 \in \mathbb{Z}$ and, since c divides b , $b = cq_2$ for some $q_2 \in \mathbb{Z}$. Hence

$$1 = am_0 + bn_0 = cq_1m_0 + cq_2n_0 = c(q_1m_0 + q_2n_0).$$

Thus c divides 1 which implies that $c = \pm 1$. Thus the only common divisors of a and b are ± 1 and so the greatest common divisor is 1, as required to prove that a and b are coprime. \square

Theorem 17.3.2 Suppose that a, b and c are positive integers with a

and b coprime. Then

$$a \text{ divides } bc \Rightarrow a \text{ divides } c.$$

Constructing a proof. This innocuous appearing result is the key to many basic results in number theory. It is surprisingly difficult to prove. Although in this book I am attempting to demonstrate that many proofs arise naturally from the definitions, this is not the case with all proofs: some proofs are just clever and although we can suggest that the steps arise naturally this is only with the benefit of hindsight. Although this particular proof is not difficult to understand it is rather ingenious: an example of a proof which we might be surprised that anyone was able to think of in the first place!

What we are looking for can be summarized as follows.

Given	Goal
$(a, b) = 1$ $a \text{ divides } bc$	$a \text{ divides } c$

It is not clear how to proceed. So, as always in such a situation, we go back to the definitions to simplify the statements involved. The ‘divides’ statements are simple enough but, as we have noted before, the definition of the greatest common divisor is rather complicated and difficult to use. It turns out (and this is the first clever step) that a good way to proceed which gives us a logically much simpler statement is to use the previous result which characterized coprime integers. Since a and b are coprime, $am_0 + bn_0 = 1$ for some $m_0, n_0 \in \mathbb{Z}$. This gives us the following strategy.

Given	Goal
$am_0 + bn_0 = 1$ $bc = aq$	$c = ak$ for some $k \in \mathbb{Z}$

Even now it is not absolutely obvious what to do. The second clever step is to multiply the first given statement by c which, if you think about it, is the only way of getting c out of the given statements using addition or multiplication (division is no use because it may not lead to integers). This gives the following steps:

$$\begin{aligned} c &= (am_0 + bn_0)c \quad (\text{using the first given statement}) \\ &= acm_0 + bcn_0 \\ &= acm_0 + aqn_0 \quad (\text{using the second given statement}) \\ &= a(cm_0 + qn_0). \end{aligned}$$

Thus $k = cm_0 + qn_0$ gives us the integer we need.

This remarkable proof is very short when written out formally.

Proof Suppose that a divides bc so that $bc = aq$ for some $q \in \mathbb{Z}$. Since $(a, b) = 1$, by Proposition 17.3.1 there are integers m_0 and n_0 such that $1 = am_0 + bn_0$. But then $c = (am_0 + bn_0)c = acm_0 + bcn_0 = acm_0 + aqn_0 = a(cm_0 + qn_0)$ so that a divides c as required. \square

Exercises

17.1 From Exercise 16.1, $\gcd(7684, 4148) = 68$. Find integers m and n such that $68 = 7648m + 4148n$.

17.2 Find integers m and n such that $68 = 7648m - 4148n$.

17.3 From Exercise 16.2, $\gcd(11033442, 1102246) = 578$. Find integers m and n such that $11033442m + 1102246n = 578$.

17.4 Let $\gcd(a, b, c)$ denote the greatest common divisor of the three non-zero integers a , b and c . Use Corollary 17.2.1 to prove that

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c).$$

Hence find the greatest common divisor of 11033442, 1102246 and 6035.

17.5 Find integers m , n and p such that

$$11033442m + 1102246n + 6035p = \gcd(11033442, 1102246, 6035).$$

17.6 Suppose that a_1, a_2, b_1, b_2 are positive integers such that a_1 and b_1 are coprime and a_2 and b_2 are coprime. Prove that

$$a_1b_2 = a_2b_1 \Rightarrow a_1 = a_2 \text{ and } b_1 = b_2.$$

18

Linear diophantine equations

In this chapter we present a striking application of the Euclidean algorithm. The following very ancient problem will be solved.

Problem 18.0.1 *Given integers a , b and c , find all integers m and n such that*

$$am + bn = c.$$

Notice that Proposition 4.1.1 shows that for certain choices of a , b and c there are no solutions at all since it was proved there that there are no solutions for $a = 14$, $b = 20$, $c = 101$. The first part of the solution to the problem is to give a necessary and sufficient condition for a solution to exist. It turns out that the idea used in proving Proposition 4.1.1 gives such a condition although the proof that this condition is sufficient makes use of the material on the Euclidean algorithm. The second part of the solution is to describe all the solutions when the condition is satisfied.

18.1 Diophantine equations

Problem 18.0.1 is an example of a *diophantine equation*. This term refers to an equation in one or more unknowns which is to be solved in the integers. The study of such problems is one of the oldest branches of mathematics and examples are to be found in extremely ancient documents. They are named after the Greek mathematician Diophantus†

† Exercise (from the fourth century): Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh as a bachelor. Five years after his marriage was born a son who died four years before his father, living half as long as his father. How long did Diophantus live for?

who lived in the third century A.D.; his book the *Arithmetica* is usually considered to be the high point of classical Greek number theory. Diophantus was usually content to find only one solution and did not allow negative solutions. A complete solution to Problem 18.0.1 was apparently first obtained by the Indian mathematician Brahmagupta in the seventh century.[†]

One of the most famous of all problems in mathematics takes the form of a diophantine equation. It was when reading Diophantus's *Arithmetica* (which had been recently rediscovered and translated into Latin by Bachet) in 1637 that Pierre de Fermat (1601–1665) made the following note (in Latin) in the margin of his copy.

On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any power which is a power greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition which this margin is too narrow to contain.[‡]

To understand this assertion recall that, by Pythagoras's theorem, the lengths of the sides of a right-angled triangle satisfy the equation $x^2 + y^2 = z^2$. It is easy to find integers which satisfy this equation, for example $x = 3$, $y = 4$, $z = 5$, or $x = 5$, $y = 12$, $z = 13$, and a complete description of all the solutions, known as Pythagorean triples, has been known since the time of Euclid. Fermat's note was written next to Book II, Problem 5 the *Arithmetica* which asks which squares can be written as the sum of two squares and so can be solved using knowledge of Pythagorean triples.

Fermat considered the equation $x^n + y^n = z^n$ for integers $n \geq 3$ and his note asserts that in this case there are no positive integers[§] which satisfy the equation. Fermat himself did provide elsewhere a proof of

[†] See C.B. Boyer and U.C. Merzbach, *A history of mathematics*, Wiley, Second edition 1989.

[‡] Various versions of this note appear in the literature. This one comes from H.M. Edwards, *Fermat's last theorem, a genetic introduction to algebraic number theory*, Springer-Verlag, 1977. The actual book containing the margin note has been lost. When Fermat's son, Samuel de Fermat, went through his father's papers he found the annotated copy of Diophantus's book and in 1670 published a new edition of the Bachet translation with Fermat's marginal notes as an appendix of 48 Observations. The 'last theorem' was Observation 2.

Another excellent and less advanced source of information about the problem is D.M. Burton, *Elementary number theory*, Allyn and Bacon, 1976.

[§] Actually, Diophantus worked entirely with rational numbers and so, strictly speaking, Fermat was asserting that there are no positive rational solutions. However, it is sufficient to consider only integer solutions because if one had a rational solution then an appropriate multiple of it would be an integer solution (see Problems IV, Question 19).

this result in the case that $n = 4$. A proof for $n = 3$ was first given by the Swiss mathematician Leonhard Euler in 1770 (by which time at the age of 63 he had already been blind for four years); this was incomplete but Adrien-Marie Legendre (French) plugged the gap. A proof for $n = 5$ was found around 1825 by Lejeune Dirichlet (also of French descent) and by Legendre. Since then, much modern algebra has been developed in attempting to prove Fermat's last theorem and many mathematicians have worked on it. Recently computer calculations have been used and by these means the theorem was shown to be true for values of n less than 25000. But there is no hope of proving the general theorem by checking integers n one by one.

However, in 1993 the British mathematician Andrew Wiles of Princeton University announced a proof of Fermat's last theorem. There was intense interest in this work and at the end of the year a gap was found in the proof. By October 1994 this gap had been bridged and the proof is now published.[†] It appears that this most famous mathematical problem has at last been solved.

Notice that Theorem 13.2.1, which asserted that there is no rational number whose square is 2, is a statement about a diophantine equation: it is equivalent to the assertion that the only solution to the diophantine equation $m^2 = 2n^2$ is the trivial one $m = 0, n = 0$.

18.2 A condition for the existence of solutions

We now begin the discussion of Problem 18.0.1 stated at the beginning of the chapter.

For simplicity we suppose that a, b, c are positive. It is easy to extend the methods to the general case (see Exercise 18.2).

Theorem 18.2.1 *For positive integers a, b and c , there exist integers m and n such that*

$$am + bn = c$$

[†] The proof appears in Andrew Wiles, Modular elliptic curves and Fermat's last theorem, *Annals of Mathematics*, second series, volume 141, Princeton University Press, 1995 (pages 443–551). This is a highly technical paper beyond the reach even of most professional mathematicians, but books have now appeared attempting to make the background to the proof and some of its ideas more widely available: A.D. Aczel, *Fermat's last theorem, unlocking the secret of an ancient mathematical problem*, Viking, 1997, and S. Singh, *Fermat's last theorem, the story of a riddle that confounded the world's greatest minds for 358 years*, Fourth Estate, 1997.

if and only if the greatest common divisor $\gcd(a, b)$ divides c .

Constructing a proof of the necessity of the divisibility condition. It is always a good idea to think about a specific numerical example. In Proposition 4.1.1 we showed that there are no integers m and n such that $14m + 20n = 101$ by observing that, since 2 divides 14 and 2 divides 20, for any integers m and n , 2 divides $14m + 20n$. In just the same way, in the general case, if d divides a and d divides b then d divides $am + bn$ and in particular $\gcd(a, b)$ divides $am + bn$. The details follow.

Proof of the necessity of the divisibility condition Suppose that m_0 and n_0 are integers such that $am_0 + bn_0 = c$. Let $d = \gcd(a, b)$. Since d divides a and d divides b , $a = dq_1$ and $b = dq_2$ for some natural numbers q_1 and q_2 . Therefore $c = (dq_1)m_0 + (dq_2)n_0 = d(q_1m_0 + q_2n_0)$ so that d divides c as required. \square

Constructing a proof of the sufficiency of the divisibility condition. This is the interesting part. It is often helpful to think about one particular simple case. For this problem the easiest case of $\gcd(a, b)$ dividing c is when $c = \gcd(a, b)$. In this case we need to show that there are integers m and n such that

$$am + bn = (a, b).$$

But Theorem 17.1.1 is precisely the statement that such integers exist.

Now in the general case of $\gcd(a, b)$ dividing c we have $c = (a, b)q$ for some $q \in \mathbb{Z}$. But if $am_0 + bn_0 = (a, b)$ then $a(m_0q) + b(n_0q) = (a, b)q = c$ and so we have the required integer solution of $am + bn = c$.

Proof of the sufficiency of the divisibility condition If (a, b) divides c then $c = (a, b)q$ for some $q \in \mathbb{Z}$. By Theorem 17.1.1 we can choose integers m_0 and n_0 such that

$$am_0 + bn_0 = (a, b).$$

Hence

$$a(m_0q) + b(n_0q) = (a, b)q = c.$$

Thus we see that a solution is provided by $m = m_0q$, $n = n_0q$. \square

Example 18.2.2 Prove that the diophantine equation

$$140m + 63n = 35$$

has a solution and write down one such solution.

Solution We apply the Euclidean algorithm to the numbers $a = 140$, $b = 63$, obtaining the following sequence of remainders.

$$\begin{array}{rcl} 140 & & \\ 63 & (-2) & \\ 14 & (-4) & \\ 7 & (-2) & \\ 0 & & \end{array}$$

This shows that $(140, 63) = 7$. Since 7 divides 35 the equation has a solution.

To find a solution we write the sequence of remainders as integral linear combinations.

$$\begin{array}{rcl} 140 & = & 140 \times 1 & + 63 \times 0 \\ 63 & = & 140 \times 0 & + 63 \times 1 & (-2) \\ 14 & = & 140 \times 1 & + 63 \times (-2) & (-4) \\ 7 & = & 140 \times (-4) & + 63 \times 9 & (-2) \\ 0 & & & & \end{array}$$

This gives $140 \times (-4) + 63 \times 9 = 7$ and so multiplying through by $35/7 = 5$ we obtain $140 \times (-20) + 63 \times 45 = 35$. Thus a solution is given by $m = -20$, $n = 45$. \square

18.3 Finding all the solutions – the homogeneous case

So far we have seen how to decide whether the diophantine equation

$$am + bn = c \tag{18.1}$$

has a solution and, if it has, how the Euclidean algorithm enables us to find one solution. However, there is no reason to believe that there is only one solution and we now consider how we can find all the solutions to the equation. We will see that if the equation has one solution then it has infinitely many.

We start with the special case of $c = 0$ for which the equation certainly does have a solution, namely $m = 0$, $n = 0$.

The diophantine equation

$$am + bn = 0 \tag{18.2}$$

is called a *homogeneous* equation. Equation (18.2) is said to be the homogeneous equation *associated with* the equation (18.1) (which is called *inhomogeneous* if $c \neq 0$).

The method of finding all the solutions to a homogeneous linear diophantine equation is best illustrated by means of an example. We take the homogeneous equation associated with the equation of Example 18.2.2.

Example 18.3.1 Find all the solutions to the diophantine equation

$$140m + 63n = 0. \quad (18.3)$$

Solution Recall from Example 18.2.2 that $\gcd(140, 63) = 7$. So we can begin by dividing through by 7. Then, for $m, n \in \mathbb{Z}$,

$$\begin{aligned} 140m + 63n = 0 &\Leftrightarrow 20m + 9n = 0 \\ &\Leftrightarrow 20m = -9n \\ &\Rightarrow 9 \text{ divides } 20m \end{aligned}$$

since it is clear that $-9n = 9(-n)$ is divisible by 9. From this we can deduce that 9 divides m using Proposition 17.3.2 since 9 and 20 are coprime. [Notice that, by Exercise 11.4, it is always the case that dividing $am + bn = 0$ by $\gcd(a, b)$ leads to an equation with coprime coefficients.]

It now follows that $m = 9q$ for some $q \in \mathbb{Z}$. Substituting this back into equation (18.3) we get $20 \times 9q = -9n$ which gives $n = -20q$. So we see that the solutions to the diophantine equation are given by

$$m = 9q, \quad n = -20q \quad \text{for } q \in \mathbb{Z}.$$

There is one solution for each integer q . Notice that a solution is a pair of integers (m, n) , in other words an element of the set $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$.

The following table gives some examples.

q	(m, n)
-2	(-18, 40)
-1	(-9, 20)
0	(0, 0)
1	(9, -20)
2	(18, -40)
3	(27, -60)

□

The key part of this argument can be abstracted into the following result.

Proposition 18.3.2 *Suppose that a and b are coprime non-zero integers. Then, for $(m, n) \in \mathbb{Z}^2$,*

$$am + bn = 0 \Leftrightarrow (m, n) = (bq, -aq) \text{ for some } q \in \mathbb{Z}.$$

Proof We use the same argument as in the example.

The proof of ' \Leftarrow ' is simply by substitution:

$$(m, n) = (bq, -aq) \Rightarrow am + bn = a(bq) + b(-aq) = 0.$$

To prove ' \Rightarrow ' observe that $am + bn = 0$ implies that $am = -bn$ so that b divides am . By invoking Proposition 17.3.2 it follows that b divides m since a and b are coprime. Hence $m = bq$ for some integer q and substituting this back into the equation gives $n = -aq$, as required. \square

Example 18.3.3 Using this result we could write out the solution to Example 18.3.1 as follows.

Solution For $m, n \in \mathbb{Z}$,

$$\begin{aligned} 140m + 63n = 0 &\Leftrightarrow 20m + 9n = 0 \\ &\Leftrightarrow (m, n) = (9q, -20q) \text{ for } q \in \mathbb{Z}, \end{aligned}$$

since 9 and 20 are coprime. \square

However, when using Proposition 18.3.2, care must be taken to get the numbers a and b the correct way round and the signs correct. It is usually best to check that the solutions you are claiming actually are solutions – simply by substituting into the equation.

18.4 Finding all the solutions – the general case

Now we return to the general case of equation (18.1). Once we know that such an equation has a single solution then we can write down all the solutions by solving the associated homogeneous equation (18.2). The following result sums up why this is the case.

Proposition 18.4.1 *Suppose that $(m, n) = (m_0, n_0) \in \mathbb{Z}^2$ is a solution to the diophantine equation $am + bn = c$, i.e. $am_0 + bn_0 = c$. Then, for*

$(m, n) \in \mathbb{Z}^2$,

$$am + bn = c \Leftrightarrow a(m - m_0) + b(n - n_0) = 0.$$

Proof

$$\begin{aligned} am + bn = c &\Leftrightarrow am + bn = am_0 + bn_0 \\ &\Leftrightarrow a(m - m_0) + b(n - n_0) = 0. \end{aligned}$$

□

Let us illustrate how this is used by considering an example.

Example 18.4.2 Find all the solutions to the diophantine equation

$$140m + 63n = 35.$$

Solution In Example 18.2.2 we found the particular solution $m = -20$, $n = 45$. Thus

$$\begin{aligned} 140m + 63n = 35 &\Leftrightarrow 140(m + 20) + 63(n - 45) = 0 \\ &\quad \text{by Proposition 18.4.1} \\ &\Leftrightarrow (m + 20, n - 45) = (9q, -20q) \text{ for some } q \in \mathbb{Z} \\ &\quad \text{by Example 18.3.1} \\ &\Leftrightarrow (m, n) = (-20 + 9q, 45 - 20q) \text{ for some } q \in \mathbb{Z}. \end{aligned}$$

The following table gives some solutions.

q	m	n
-2	-38	85
-1	-29	65
0	-20	45
1	-11	25
2	-2	5
3	7	-15

Notice that had we started with a different particular solution, say $m = -2$, $n = 5$, then we would have obtained that the solutions are $(m, n) = (-2 + 9q, 5 - 20q)$ for $q \in \mathbb{Z}$. But putting in some values for q illustrates that we get just the same solution set.

q	m	n
-4	-38	85
-3	-29	65
-2	-20	45
-1	-11	25
0	-2	5
1	7	-15

This problem is considered again as Example 20.2.4 where an alternative method is explained. \square

Exercises

18.1 Solve the diophantine equation

$$7684m + 4148n = 272.$$

18.2 Solve the diophantine equation

$$7684m - 4148n = 272.$$

18.3 Solve the diophantine equation

$$516m + 564n = 6432.$$

Prove that there are unique positive integers satisfying this equation and find these integers.

Problems IV: Arithmetic

1. Prove that if an integer n is the sum of two squares ($n = a^2 + b^2$ for $a, b \in \mathbb{Z}$) then $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ for some $q \in \mathbb{Z}$. Deduce that 1234567 cannot be written as the sum of two squares.
2. Let a be an integer. Prove that a^2 is divisible by 5 if and only if a is divisible by 5.
3. Use the result of Question 2 to prove that there does not exist a rational number whose square is 5.
4. Prove that there is no rational number whose square is 98.
5. Prove that every infinite decimal representing a rational number is recurring (the converse of Theorem 13.3.4) and furthermore that if the fraction in lowest terms representing a fraction is a/b then the number of recurring digits in its decimal representation is less than b .

[See Exercise 15.6.]

6. Use the Euclidean algorithm to find the greatest common divisors of (i) 165 and 252, (ii) 4284 and 3480.
7. Let u_n be the n th Fibonacci number (for the definition see Definition 5.4.2). Prove that the Euclidean algorithm takes precisely n steps to prove that $\gcd(u_{n+1}, u_n) = 1$.

- 8.** Suppose that a and b are two positive integers with $a \geq b$. Let a_0, a_1, \dots, a_n be the sequence of integers generated by the Euclidean algorithm so that $a_n = \gcd(a, b)$. Prove by induction on k that $a_{n-k} \geq u_{k+2}$ where u_m is the m th Fibonacci number. Deduce that $b \geq u_{n+1}$.

Hence prove Lamé's theorem: if b has r decimal digits then $n \leq 5r$.

[Prove that $\log_{10} \alpha > 1/5$ where $\alpha = (1 + \sqrt{5})/2$.]

- 9.** Describe an algorithm to output the numbers q and r in the division theorem (Theorem 15.1.1) given positive integers a and b .

[The discussion on page 193 may help.]

- 10.** In each case of Question 6 write the greatest common divisor as an integral linear combination of the two numbers.

- 11.** Given positive integers a and b , suppose that applying the Euclidean algorithm leads to a sequence of positive integers a_0, a_1, \dots, a_N . Suppose that the procedure of the proof of Theorem 17.1.1 leads to expressions of the form

$$a_k = am_k + bn_k$$

for integers m_k and n_k . Prove that $m_k n_{k-1} - m_{k-1} n_k = (-1)^k$ for $1 \leq k \leq N$. Deduce that the numbers m_k and n_k are coprime.

- 12.** With the same data as in the previous question suppose that the procedure of the proof of Theorem 17.1.1 is continued for one more step to give

$$0 = am_{N+1} + bn_{N+1}.$$

Prove that the integers m_{N+1} and n_{N+1} determine the solution set of the diophantine equation $am + bn = 0$:

$$am + bn = 0 \Leftrightarrow (m, n) = (m_{N+1}q, n_{N+1}q) \text{ for some } q \in \mathbb{Z}.$$

- 13.** The *least common multiple* of two non-zero integers a and b is the unique positive integer m such that

- (i) m is a common multiple, i.e. a divides m and b divides m ,
- (ii) m is less than any other common multiple:

$$a \text{ divides } n \text{ and } b \text{ divides } n \Rightarrow m \leq n.$$

We denote the least common multiple of a and b by $[a, b]$ or $\text{lcm}[a, b]$.

Give a proof by contradiction that if a positive integer n is a common multiple of a and b then $[a, b]$ divides n .

[Use the division theorem. If $[a, b]$ does not divide n then $n = [a, b]q + r$ where $0 < r < [a, b]$. Now prove that r is a common multiple of a and b .]

This means that $ab/[a, b]$ is an integer. Prove that this integer is a common divisor of a and b . Deduce that $ab/[a, b] \leq (a, b)$, the greatest common divisor of a and b .

Prove that $ab/(a, b)$ is a common multiple of a and b . Deduce that $(a, b)[a, b] = ab$ if a and b are positive.

Hence find $\text{lcm}[612, 696]$.

14. Let a and b be positive integers. By the well-ordering principle the non-empty set of positive integers

$$\{ am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0 \}$$

has a minimum element c . Prove by contradiction that c is a common divisor of a and b and hence give an alternative proof of Theorem 17.1.1.

15. Solve the linear diophantine equations

- (i) $165m + 252n = 15$,
- (ii) $165m + 252n = 20$,
- (iii) $4284m + 3480n = 60$,
- (iv) $4284m - 3480n = 36$.

16. Solve the linear diophantine equation

$$336m + 238n = 5558.$$

Prove that there is a unique pair of *positive* integers m and n satisfying this equation and find this solution.

17. Find all positive integers which satisfy the diophantine equation

$$12563m + 6052n = 9922169.$$

18. Solve the linear diophantine equation

$$6m + 10n + 15p = 1.$$

- 19.** Prove that if there are no non-zero integer solutions to the equation $x^n + y^n = z^n$ then there are no non-zero rational solutions.

[Prove the contrapositive: show how a rational solution leads to an integer solution.]

Part V

Modular arithmetic

19

Congruence of integers

Throughout this chapter m will denote a fixed positive integer.

One of the most useful distinctions amongst the integers is that between even and odd numbers. We have already seen a number of mathematical arguments which make use of this. The distinction between these two types of number can be expressed in terms of the remainder when the number is divided by 2: the remainder is 0 in the case of an even number and 1 for an odd number. The idea of congruence is a generalization of this: we classify integers according to the remainder after division by some fixed positive integer, not necessarily 2.

To be more precise, suppose that m is a positive integer. Two integers a and b are *congruent modulo m* if they have the same remainder after division by m . This divides the integers into m different subsets each consisting of the set of integers having a certain remainder. These subsets are called *congruence classes* of integers and they will be investigated more fully in Chapter 21.

This idea is familiar to everyone in the measurement of time. For example when we use the days of the week we are counting days modulo 7. Most calendars list days in columns with the Sundays in the first column, the Mondays in the second and so on up to the Saturdays in the seventh column. This means that two days are in the same column if and only if they are on the same day of the week so that when we count the days successively from some fixed starting point then the numbers of the two days are congruent modulo 7. Thus the columns form the congruence classes. Many of our activities are determined by which column a day lies in, by the day of the week: think of timetables (of trains or lectures) and shop opening hours.

As an illustration, 1 January 1998 is a Thursday. If we want to find the day of the week of 6 September 1998 then we calculate what day of the year it is: $31 \times 5 + 30 \times 2 + 28 \times 1 + 6 = 155 + 60 + 28 + 6 = 249$. Applying the division theorem, $249 = 7 \times 35 + 4$. Hence 249 is congruent modulo 7 to 4 so that 6 September 1998 is the same day of the week as the fourth day of the year, 4 January 1998, namely Sunday. We will see shortly how to simplify this calculation.

19.1 Basic definitions

It is convenient to phrase the formal definition of congruence in a slightly different way from that described above. This formulation of the definition uses only the idea of divisibility and does not rely on the division theorem.

Definition 19.1.1 Two integers a and b are congruent modulo m when $a - b$ is divisible by m , i.e. there exists an integer q such that $a - b = mq$. We write $a \equiv b \pmod{m}$. If the modulus m is clear we may sometimes omit it and just write $a \equiv b$.

This definition (and the notation \equiv) was introduced by the German mathematician Carl Friedrich Gauss in his book *Disquisitiones arithmeticae* published in 1801 when he was only 24. This book is considered to have laid the foundations of modern number theory. It is available in an English translation† and is beautifully written and readily understood by a modern reader.

To illustrate the definition observe that $14 \equiv 2 \pmod{3}$ since $14 - 2 = 12 = 3 \times 4$, and $14 \equiv -10 \pmod{3}$ since $14 - (-10) = 24 = 3 \times 8$. On the other hand, $14 \not\equiv 1 \pmod{3}$ since $14 - 1 = 13$ is not a multiple of 3. Given any two integers they are congruent modulo 1 since every integer is divisible by 1. Because of this it is usual to take $m > 1$.

Notice that $a \equiv 0 \pmod{m}$ is another way of saying that m divides a , or equivalently a is a multiple of m .

The relation of congruence has many properties which are similar to those of equality.

† C.F. Gauss, *Disquisitiones arithmeticae* (translated by A.A. Clarke), Springer-Verlag, 1986.

Proposition 19.1.2

- (i) Reflexive property. *For all integers a , $a \equiv a \pmod{m}$.*
- (ii) Symmetric property. *If a and b are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.*
- (iii) Transitive property. *If a , b and c are integers such that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*

We usually use these properties without comment.

Proof (i) This is immediate since $a - a = 0 = m \times 0$.

(ii) If $a \equiv b \pmod{m}$, then m divides $(a - b)$ and so $a - b = mq$ for some $q \in \mathbb{Z}$. But then $b - a = -mq = m \times (-q)$ so that m divides $(b - a)$, i.e. $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ then $a - b = mq_1$ for some $q_1 \in \mathbb{Z}$. Similarly $b \equiv c \pmod{m} \Rightarrow b - c = mq_2$ for some $q_2 \in \mathbb{Z}$. But then $a - c = (a - b) + (b - c) = mq_1 + mq_2 = m(q_1 + q_2)$ and so, since $q_1 + q_2 \in \mathbb{Z}$, m divides $a - c$, i.e. $a \equiv c \pmod{m}$. \square

The real power of the notion of congruence arises from the fact that it respects the basic operations of arithmetic, addition, subtraction and multiplication, as follows.

Proposition 19.1.3 (Modular arithmetic) *Suppose that a_1 , a_2 , b_1 and b_2 are integers such that $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$. Then*

- (i) $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$,
- (ii) $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$,
- (iii) $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.

Proof Suppose that $a_1 - a_2 = mq_1$ and $b_1 - b_2 = mq_2$. Then we have the following.

(i) $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = mq_1 + mq_2 = m(q_1 + q_2)$. Therefore m divides $[(a_1 + b_1) - (a_2 + b_2)]$, i.e. $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ as required.

(ii) Left as an exercise (Exercise 19.2).

(iii) Since $a_1 = a_2 + mq_1$ and $b_1 = b_2 + mq_2$, $a_1 b_1 = (a_2 + mq_1)(b_2 + mq_2) = a_2 b_2 + a_2 mq_2 + mq_1 b_2 + m^2 q_1 q_2 = a_2 b_2 + m(a_2 q_2 + q_1 b_2 + mq_1 q_2)$. Hence $a_1 b_1 - a_2 b_2 = m(a_2 q_2 + q_1 b_2 + mq_1 q_2)$ so that $a_1 b_1 - a_2 b_2$ is divisible by m , i.e. $a_1 b_1 \equiv a_2 b_2 \pmod{m}$. \square

This result means that if we consider two integers to be interchangeable if they are congruent then as far as addition, subtraction and multiplication are concerned no problems will arise. Division is more complicated and we will begin to look at this at the end of this chapter.

Modular arithmetic leads to chains of congruences just as ordinary arithmetic leads to chains of equalities.

Examples 19.1.4 (a) Working modulo 5, $97 \equiv 2$ since $97 - 2 = 95 = 5 \times 19$ and $144 \equiv 4$ since $144 - 4 = 140 = 5 \times 28$. Hence $97^3 + 144^2 \equiv 2^3 + 4^2 \equiv 8 + 16$. But now $8 \equiv 3$ and $16 \equiv 1$ and so $8 + 16 \equiv 3 + 1 \equiv 4$. The conclusion is that $97^3 + 144^2 \equiv 4 \pmod{5}$.

(b) For all $n \geq 1$, $4^n + 5 \equiv 1^n + 2 \equiv 1 + 2 \equiv 0 \pmod{3}$ so that 3 divides $4^n + 5$. This provides a much simpler proof of the result of Problems I, Question 12.

(c) The calculation in the introduction to this chapter leading to the day of the week of 6 September 1998 can be much simplified using modular arithmetic. The day of the year of 6 September 1998 is $31 \times 5 + 30 \times 2 + 28 \times 1 + 6 \equiv 3 \times 5 + 2 \times 2 + 0 \times 1 + 6 = 15 + 4 + 6 = 25 \equiv 4 \pmod{7}$. Hence the day of the week is the same as that of 4 January 1998, namely Sunday.

19.2 The remainder map

We had better now confirm that the idea used to motivate the concept of congruence in the introduction to this chapter does agree with the formal definition. There we stated that two integers are congruent modulo m if they lead to the same remainder after division by m .

Definition 19.2.1 *The set of integers*

$$R_m = \{0, 1, 2, \dots, m-1\} = \{i \in \mathbb{Z} \mid 0 \leq i < m\}$$

is called the set of (least, non-negative) remainders modulo m *or, alternatively, the set of residues modulo m .*

Proposition 19.2.2 *Given an integer a , there is a unique $r \in R_m$ such that $a \equiv r \pmod{m}$.*

Proof This is an immediate consequence of the division theorem (Theorem 15.1.1) since $a \equiv r \pmod{m}$ if and only if $a = mq + r$ for some integer q . \square

Definition 19.2.3 We define the remainder map $r_m: \mathbb{Z} \rightarrow R_m$ by

$$r_m(a) = r \Leftrightarrow a \equiv r \pmod{m} \text{ and } r \in R_m.$$

This is well-defined by Proposition 19.2.2.

Notice that since we are here giving a conditional definition of the values of a function it is necessary to confirm that the condition determines a unique element of the codomain for each element of the domain. This is what is meant by the assertion that the function is ‘well-defined’.

In terms of this notation we can state the equivalence of the definition of congruence in Definition 19.1.1 and the idea of congruence discussed in the introduction as follows.

Proposition 19.2.4 Two integers a and b are congruent modulo m if and only if $r_m(a) = r_m(b)$.

Proof Suppose that $r_m(a) = r'$ and $r_m(b) = r''$.

\Leftarrow : By definition of r_m , $a \equiv r' \pmod{m}$ and $b \equiv r'' \pmod{m}$. Hence if $r' = r''$ then $a \equiv r' \equiv r'' \equiv b \pmod{m}$ so that $a \equiv b \pmod{m}$.

\Rightarrow : Similarly, if $a \equiv b \pmod{m}$ then $r' \equiv a \equiv b \equiv r'' \pmod{m}$ so that $r' \equiv r'' \pmod{m}$. But clearly $r' \equiv r' \pmod{m}$. Hence, by the uniqueness part of Proposition 19.2.2, $r' = r''$. \square

The last step in this proof is an example of how uniqueness results are often used: given that there is only one object with some property, if you know that two objects have this property then they must be equal.

We now illustrate how the language of congruence can simplify the presentation of some earlier proofs.

Example 19.2.5 Prove that, for an integer a , a is even if and only if a^2 is even. [Exercise 3.3 and Problems I, Question 7]

Solution An integer n is even if and only if $n \equiv 0 \pmod{2}$. The set of least non-negative remainders modulo 2 is just $R_2 = \{0, 1\}$ and so

$n \equiv 0 \pmod{2}$ if and only if $n \not\equiv 1 \pmod{2}$. From modular arithmetic,

$$\begin{aligned} a \equiv 0 \pmod{2} &\Rightarrow a^2 \equiv 0 \pmod{2}, \\ a \equiv 1 \pmod{2} &\Rightarrow a^2 \equiv 1 \pmod{2}. \end{aligned}$$

The contrapositive of the second statement is

$$a^2 \equiv 0 \pmod{2} \Rightarrow a \equiv 0 \pmod{2}.$$

Hence $a \equiv 0 \pmod{2} \Leftrightarrow a^2 \equiv 0 \pmod{2}$, i.e. a is even if and only if a^2 is even. \square

Example 19.2.6 Prove that there do not exist integers a and b such that $a^2 + b^2 = 1234567$. [Problems IV, Question 1]

Solution The set of remainders modulo 4, R_4 , is $\{0, 1, 2, 3\}$ and so working modulo 4 we have four possibilities to consider. From modular arithmetic,

$$\begin{aligned} a \equiv 0 \pmod{4} &\Rightarrow a^2 \equiv 0 \pmod{4}, \\ a \equiv 1 \pmod{4} &\Rightarrow a^2 \equiv 1 \pmod{4}, \\ a \equiv 2 \pmod{4} &\Rightarrow a^2 \equiv 4 \equiv 0 \pmod{4}, \\ a \equiv 3 \pmod{4} &\Rightarrow a^2 \equiv 9 \equiv 1 \pmod{4}. \end{aligned}$$

Thus for any $a \in \mathbb{Z}$, $a^2 \equiv 0$ or $1 \pmod{4}$. Therefore given two integers a and b , $a^2 + b^2 \equiv 0$ or 1 or $2 \pmod{4}$, i.e. $a^2 + b^2 \not\equiv 3 \pmod{4}$.

Suppose now for contradiction that a and b are integers such that $a^2 + b^2 = 1234567$. Then, since $1234567 \equiv 3 \pmod{4}$, we have $a^2 + b^2 \equiv 3 \pmod{4}$ giving the required contradiction. Hence such integers cannot exist. \square

In neither case is this essentially a new proof. It is just that the congruence notation simplifies the presentation of the old proof. This demonstrates one way in which introducing a new concept like congruence is useful: it helps to simplify and unify earlier arguments. However, even more importantly, when we become familiar with the new concept it can then lead to new ideas; the final chapter of the book will include some proofs which seem to arise from a good understanding of the concept of congruence.

19.3 Division in congruences

In stating Proposition 19.1.3 we observed that congruences work well with respect to addition, subtraction and multiplication. However, more care is needed with division.

As an illustration observe that $30 \equiv 2 \pmod{4}$. If now we divide both sides by 2 we obtain 15 and 1, which are not congruent modulo 4; $15 \not\equiv 1 \pmod{4}$ since $15 - 1 = 14$ is not divisible by 4. Let us look for what has gone wrong. We have the congruence $30 \equiv 2 \pmod{4}$ because $30 - 2 = 4 \times 7$. If we divide this equation by 2 we obtain $15 - 1 = 4 \times (7/2)$ and we do not get a congruence modulo 4 between 15 and 1 because $7/2$ is not an integer. We can, however, write $15 - 1 = (4/2) \times 7 = 2 \times 7$ which shows that we do have a congruence modulo 2: $15 \equiv 1 \pmod{2}$.

This example shows how we do division when the divisor also divides the modulus. The general result is as follows.

Proposition 19.3.1 *Suppose that a is an integer which divides m (i.e. m/a is an integer). Then*

$$ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow b_1 \equiv b_2 \pmod{m/a}.$$

Proof From the definition of congruence, $ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow a(b_1 - b_2) = mq$ for some $q \in \mathbb{Z} \Leftrightarrow b_1 - b_2 = (m/a)q$ for some $q \in \mathbb{Z} \Leftrightarrow b_1 \equiv b_2 \pmod{m/a}$.

[Notice that we make use of the fact that m/a is an integer when we write ‘mod (m/a) ’.] \square

At the other extreme, division by numbers which are coprime to the modulus is also easy.

Proposition 19.3.2 *Suppose that a is an integer such that a and m are coprime (i.e. the greatest common divisor $(a, m) = 1$). Then*

$$ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow b_1 \equiv b_2 \pmod{m}.$$

Proof ‘ \Rightarrow ’: $ab_1 \equiv ab_2 \pmod{m} \Rightarrow m$ divides $a(b_1 - b_2) \Rightarrow m$ divides $(b_1 - b_2)$ [by Theorem 17.3.2 using the fact that $(a, m) = 1$] $\Rightarrow b_1 \equiv b_2 \pmod{m}$.

‘ \Leftarrow ’: This is a special case of Proposition 19.1.3(iii). \square

Division in ordinary arithmetic first arises when we try to solve the linear equation $ax = b$. Division in modular arithmetic arises when we

try to solve the linear congruence $ax \equiv b \pmod{m}$, in other words seek all integers which satisfy this congruence.

We can go quite a long way by simply using the above results in turn. We use the first until we run out of divisors of m and then move on to the second.

Example 19.3.3 Solve the congruence $4x \equiv 12 \pmod{14}$, i.e. find all integers x such that $4x \equiv 12 \pmod{14}$.

Solution We simply say

$$\begin{aligned} 4x \equiv 12 \pmod{14} &\Leftrightarrow 2x \equiv 6 \pmod{7} \text{ (by Proposition 19.3.1)} \\ &\Leftrightarrow x \equiv 3 \pmod{7} \text{ (by Proposition 19.3.2).} \end{aligned}$$

Thus $4x \equiv 12 \pmod{14} \Leftrightarrow x \equiv 3 \pmod{7}$. \square

Notice that as in solving equations it is important to have ' \Leftrightarrow ' in the conclusion. In this case the predicate $x \equiv 3 \pmod{7}$ provides a necessary and sufficient condition for an integer x to satisfy the congruence.

We normally leave the solution in this form which provides a conditional description of the solution set, $S = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{7}\}$. As an alternative we could give a constructive description of the set by spelling out the notion of congruence which gives $4x \equiv 12 \pmod{14} \Leftrightarrow x = 3 + 7q$ for some $q \in \mathbb{Z}$; this shows that the solution set $S = \{3 + 7q \mid q \in \mathbb{Z}\}$.

However, the question was couched in terms of the modulus 14 and so it might be appropriate to give the solution in terms of this modulus. If we consider the elements of the modulo 14 remainder set, R_{14} , we see that for $r \in R_{14}$, $r \equiv 3 \pmod{7}$ if and only if $r = 3$ or $r = 10$. So we conclude that $x \equiv 3 \pmod{7}$ if and only if $x \equiv 3 \pmod{14}$ or $x \equiv 10 \pmod{14}$. Thus $4x \equiv 12 \pmod{14} \Leftrightarrow x \equiv 3 \text{ or } 10 \pmod{14}$.

Example 19.3.4 Solve the congruence $6x \equiv 15 \pmod{21}$.

Solution This time we obtain

$$\begin{aligned} 6x \equiv 15 \pmod{21} &\Leftrightarrow 2x \equiv 5 \pmod{7} \text{ (by Proposition 19.3.1)} \\ &\Leftrightarrow 2x \equiv 12 \pmod{7} \\ &\quad (\text{using } 5 \equiv 12 \pmod{7} \text{ to get an even number}) \\ &\Leftrightarrow x \equiv 6 \pmod{7} \text{ (by Proposition 19.3.2).} \end{aligned}$$

Hence $6x \equiv 15 \pmod{21} \Leftrightarrow x \equiv 6 \pmod{7}$. \square

Since for $r \in R_{21}$, $r \equiv 6 \pmod{7} \Leftrightarrow r = 6, 13 \text{ or } 20$, we can state this solution as $6x \equiv 15 \pmod{21} \Leftrightarrow x \equiv 6, 13 \text{ or } 20 \pmod{21}$.

The *ad hoc* methods used in these two examples are adequate for problems of this type involving only small numbers but if the numbers are large then something more systematic is needed. In the next chapter we will consider a general method for solving linear congruences.

Exercises

19.1 What day of the week is 6 September 2045?

19.2 Prove that $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$.

19.3 Suppose that a positive integer is written in decimal notation as $n = a_k a_{k-1} \dots a_2 a_1 a_0$ where $0 \leq a_i \leq 9$. Prove that n is divisible by 3 if and only if the sum of its digits $a_k + a_{k-1} + \dots + a_1 + a_0$ is divisible by 3.

19.4 Solve the following congruences:

- (i) $6x \equiv 24 \pmod{45}$;
- (ii) $10x \equiv 15 \pmod{45}$.

State the results in terms of the modulus 45.

Describe the solution sets without using the notion of congruence.

19.5 Prove that

$$ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow b_1 \equiv b_2 \pmod{(m/(a, m))}.$$

[Here (a, m) denotes the greatest common divisor of a and m which necessarily divides m so that $m/(a, m)$ is an integer.]

20

Linear congruences

Throughout this chapter m will denote a fixed positive integer.

In this chapter we discuss the following problem.

Problem 20.0.1 Given a positive integer m and integers a and b , solve the congruence

$$ax \equiv b \pmod{m},$$

i.e. find all integers x which satisfy this congruence.

Such a problem is called a *linear congruence* and examples have already been considered in the previous chapter. In this chapter we will discuss the general solution. We will make use of a close relationship between this problem and the linear diophantine equation problem discussed in Chapter 18.

20.1 A criterion for the existence of solutions

We considered some examples of linear congruences in the previous chapter. The results we used there were as follows.

Proposition 19.3.1 If a divides m , then

$$ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow b_1 \equiv b_2 \pmod{m/a}.$$

Proposition 19.3.2 If $(a, m) = 1$, then

$$ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow b_1 \equiv b_2 \pmod{m}.$$

These results enable us to divide through the linear congruence $ax \equiv b \pmod{m}$ by common factors of a and b . Examples of this were given in Example 19.3.3 and Example 19.3.4. The first result tells us what to do if this common factor is also a factor of the modulus m . A natural question which arises is what happens if a and m have a common factor which does not divide b . In fact this tells us that the congruence has no solutions at all as we will now explain beginning with an example.

Example 20.1.1 Prove that the linear congruence $6x \equiv 14 \pmod{21}$ has no solutions.

Constructing a proof. We can summarize what is required as follows.

Given	Goal
$x \in \mathbb{Z}$	$6x \not\equiv 14 \pmod{21}$

Since the goal here is negative a proof by contradiction is suggested.

Given	Goal
$x \in \mathbb{Z}$ $6x \equiv 14 \pmod{21}$	contradiction

This is not a difficult argument to construct once we make use of the definition of congruence. If $6x \equiv 14 \pmod{21}$ then $6x - 14 = 21q$ for some integer q . Hence $14 = 6x - 21q$. But now our work on linear diophantine equations enables us to see immediately how to obtain a contradiction using divisibility by 3 for we can rewrite this equation as $14 = 3(2x - 7q)$ implying that 3 divides 14 which is certainly not the case and so gives the necessary contradiction.

The reader should write out this argument as a formal proof by contradiction using the template of Chapter 4.

The idea used in this example may be stated generally as follows.

Proposition 20.1.2 *Let a and b be integers. If there exists a common divisor of a and m which does not divide b , then the linear congruence $ax \equiv b \pmod{m}$ has no solutions.*

The proof of this result is by contradiction following the pattern of the previous example.

Proof Suppose that c is a common divisor of a and m which does not

divide b . Suppose for contradiction that there is an integer x_0 which is a solution to the congruence, i.e. $ax_0 \equiv b \pmod{m}$. Then $ax_0 - b = mq$ for some $q \in \mathbb{Z}$. Hence $b = ax_0 - mq$. But c divides a so that $a = ca_1$ for some $a_1 \in \mathbb{Z}$ and, since c divides m , $m = cm_1$ for some $m_1 \in \mathbb{Z}$. Hence $b = ax_0 - mq = ca_1x_0 - cm_1q = c(a_1x_0 - m_1q)$ so that c divides b contradicting the given statement that c does not divide b . Hence our assumption must be false and so there is no integer solution to $ax \equiv b \pmod{m}$. \square

Example 20.1.3 Prove that the linear congruence

$$12468x \equiv 34567 \pmod{48732}$$

has no solutions.

Solution There are no solutions because 3 is a common divisor of 12468 and 48732 but does not divide 34567. [Use Exercise 19.3.] \square

We would like a criterion for the existence of solutions, in other words a necessary and sufficient condition. Proposition 20.1.2 provides us with a necessary condition: if there is a solution then every common divisor of a and m must divide b . This is in fact a necessary and sufficient condition but in order to state an efficient criterion it is useful to restate the proposition in a more specific way: the reference to ‘every common divisor’ suggests that there is a lot to check. Recall that by Corollary 17.2.1 all the common divisors of a and m divide the greatest common divisor $\gcd(a, m)$. So the necessary condition for solutions given in Proposition 20.1.2 can be entirely captured by considering divisibility by the greatest common divisor.

Corollary 20.1.4 *A necessary condition for the existence of solutions of the linear congruence $ax \equiv b \pmod{m}$ is that the greatest common divisor $\gcd(a, m)$ divides b .*

Proof This is just a special case of the proposition for, by definition of the greatest common divisor, (a, m) divides a and (a, m) divides m . \square

The condition in Corollary 20.1.4 is also sufficient for the existence of solutions. The key to proving this is the special case when a and m are coprime, in which case, since $\gcd(a, m) = 1$, the condition is automatically satisfied.

Theorem 20.1.5 Let m be a positive integer. Suppose that a and b are integers such that a and m are coprime. Then the linear congruence

$$ax \equiv b \pmod{m}$$

has a solution. This solution is unique up to congruence modulo m .

We will defer the proof of this result to the next section. To see the significance of the uniqueness part of this theorem observe that if x_0 is a solution of the linear congruence then so is any integer congruent to x_0 for, by modular arithmetic, if $x \equiv x_0 \pmod{m}$ then $ax \equiv ax_0 \pmod{m}$. The meaning of the statement that the solution is unique modulo m is that these are the only solutions: given any solution, x_0 , an integer x is a solution if and only if it is congruent to x_0 . This is illustrated in the following examples.

Examples 20.1.6 (a) In Example 19.3.4 it was observed that $2x \equiv 5 \pmod{7} \Leftrightarrow x \equiv 6 \pmod{7}$.

(b) In Solution 19.4(ii) it was observed that $2x \equiv 3 \pmod{9} \Leftrightarrow x \equiv 6 \pmod{9}$.

(c) The linear congruence $3x \equiv 8 \pmod{11}$ has a unique solution modulo 11 by the theorem. To find the solution we may simply try in turn the elements R_{11} . The following table lists the values of $r_{11}(3x)$.

$r_{11}(x)$	0	1	2	3	4	5	6	7	8	9	10
$r_{11}(3x)$	0	3	6	9	1	4	7	10	2	5	8

From this we see that $3x \equiv 8 \pmod{11} \Leftrightarrow x \equiv 10 \pmod{11}$.

In this case it might have been quicker to observe that $8 \equiv -3 \pmod{11}$ so that $3x \equiv 8 \pmod{11} \Leftrightarrow 3x \equiv -3 \pmod{11} \Leftrightarrow x \equiv -1 \pmod{11}$ (since 3 and 11 are coprime) $\Leftrightarrow x \equiv 10 \pmod{11}$.

(d) Consider the linear congruence $290x \equiv 5 \pmod{357}$.

Applying the Euclidean algorithm we discover that 290 and 357 are coprime and so according to Theorem 20.1.5 this congruence has a unique solution modulo 357. It is a bit daunting to go through all the possibilities and it is also harder to see any tricks with these larger numbers. For this sort of example we need something which is systematic but is more efficient. Such a method will be considered in the next section and will provide a method for proving Theorem 20.1.5.

(e) In Example 19.3.3 it was proved that $4x \equiv 12 \pmod{14} \Leftrightarrow x \equiv 3$ or $x \equiv 10 \pmod{14}$. In this case $a = 4$ and $m = 14$ are not coprime and

the solution is not unique modulo 14: there are two solutions modulo 14.

If we put together Theorem 20.1.5, Proposition 19.3.1 and Corollary 20.1.4 we obtain the following result which provides the desired criterion for the existence of solutions to a linear congruence and also a measure of how many solutions there are.

Theorem 20.1.7 *The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if the greatest common divisor (a, m) divides b . In this case the number of different solutions modulo m is $\gcd(a, m)$.*

Constructing a proof. The proof that the divisibility criterion is necessary and sufficient follows easily from previously stated results.

In order to understand the result about the number of solutions the reader may find it useful to look back to Example 19.3.4 which illustrates it. There we found that the congruence $6x \equiv 15 \pmod{21}$ has a unique solution modulo 7, namely $x \equiv 6 \pmod{7}$. To obtain a result formulated in terms of the modulus 21 we observed that the remainders modulo 21 which are congruent to 6 modulo 7 are $6 + 7q$ for $q = 0, 1$ and 2 , i.e. 6, 13 and 20. The same idea works in general.

Proof The necessity of the divisibility condition is Corollary 20.1.4.

For sufficiency suppose that $\gcd(a, m)$ divides b . Then since (a, m) divides a and m

$$ax \equiv b \pmod{m} \Leftrightarrow \frac{a}{(a, m)}x \equiv \frac{b}{(a, m)} \pmod{\frac{m}{(a, m)}},$$

by Proposition 19.3.1. Now the numbers $a/(a, m)$ and $m/(a, m)$ are coprime (Exercise 11.4) and so by Theorem 20.1.5 this congruence has a (unique) solution modulo $m/(a, m)$ and so certainly a solution.

Now we determine the number of incongruent solutions. Put $m_1 = m/(a, m)$, an integer since (a, m) divides m . Suppose that the unique solution to the linear congruence modulo m_1 is represented by $r_1 \in R_{m_1}$ so that an integer x is a solution if and only if $x \equiv r_1 \pmod{m_1}$. Suppose that an integer x is congruent modulo m to $r \in R_m$. Then x is a solution if and only if $r \equiv r_1 \pmod{m_1}$. This means that $r = r_1 + m_1q$. Now $r \in R_m \Leftrightarrow 0 \leq r < m \Leftrightarrow 0 \leq r_1 + m_1q < m_1(a, m) \Leftrightarrow 0 \leq q < (a, m)$. So x is a solution if and only if $x \equiv r_1 + m_1q \pmod{m}$ for $0 \leq q < (a, m)$, giving the required (a, m) solutions modulo m . \square

20.2 Linear congruences and diophantine equations

We now present a systematic method of finding the solutions of a linear congruence which will enable us to prove Theorem 20.1.5. The key idea is to relate linear congruences to linear diophantine equations.

Let us go back to the definition of congruence modulo m . Recall that $ax \equiv b \pmod{m}$ if and only if $b - ax$ is a multiple of m which means that there is some integer, say y , such that $b - ax = my$, i.e. $ax + my = b$. This means that solving the linear congruence $ax \equiv b \pmod{m}$ is equivalent to solving the diophantine equation $ax + my = b$.

We can make this more precise in the following way. Notice that a solution to the diophantine equation $ax + my = b$ consists of an ordered pair of integers (x_0, y_0) such that $x = x_0$, $y = y_0$ satisfies the equation. So we can think of a solution as being an element of the Cartesian product $\mathbb{Z} \times \mathbb{Z}$ or \mathbb{Z}^2 . The *solution set* of the diophantine equation is then the subset of \mathbb{Z}^2 given by $\{(x, y) \in \mathbb{Z}^2 \mid ax + my = b\}$. Of course, if there are no solutions, then this is the empty set.

Similarly, the solution set of the linear congruence $ax \equiv b \pmod{m}$ is the subset $\{x \in \mathbb{Z} \mid ax \equiv b \pmod{m}\}$ of the integers.

Proposition 20.2.1 *For integers a , b , and positive integers m , there is a bijection*

$$f: \{(x, y) \in \mathbb{Z}^2 \mid ax + my = b\} \rightarrow \{x \in \mathbb{Z} \mid ax \equiv b \pmod{m}\}$$

given by $f(x, y) = x$.

Proof Suppose that $ax_0 \equiv b \pmod{m}$. Then, for $(x, y) \in \mathbb{Z}^2$ such that $ax + my = b$, $f(x, y) = x_0$ if and only if $x = x_0$ which means that $y = (b - ax_0)/m$. [Notice that $(b - ax_0)/m \in \mathbb{Z}$ since $ax_0 \equiv b \pmod{m}$.] This means that x_0 has the unique pre-image $(x_0, (b - ax_0)/m)$ and so f is a bijection with inverse map given by $g(x) = (x, (b - ax)/m)$. \square

In Chapter 18 a systematic way of finding solutions to linear diophantine equations using the Euclidean algorithm was described. Using the above correspondence this can be used to solve linear congruences.

Example 20.2.2 Solve the linear congruence $290x \equiv 5 \pmod{357}$.

Solution We solve the diophantine equation $290x + 357y = 5$. Applying

the Euclidean algorithm we get the following sequence of remainders.

$$\begin{array}{r}
 357 \\
 290 \quad (-1) \\
 67 \quad (-4) \\
 22 \quad (-3) \\
 1 \quad (-22) \\
 0
 \end{array}$$

Thus 290 and 357 are coprime so that the diophantine equation has a solution. To find a solution we use the Euclidean algorithm to write 1 as an integral linear combination of 290 and 357.

$$\begin{array}{rcl}
 357 & = & 357 \times 1 + 290 \times 0 \\
 290 & = & 357 \times 0 + 290 \times 1 \quad (-1) \\
 67 & = & 357 \times 1 + 290 \times (-1) \quad (-4) \\
 22 & = & 357 \times (-4) + 290 \times 5 \quad (-3) \\
 1 & = & 357 \times 13 + 290 \times (-16) \quad (-22) \\
 0
 \end{array}$$

Thus a solution to the diophantine equation is given by $x = (-16) \times 5 = -80$, $y = 13 \times 5 = 65$. Hence $x = -80$ is a solution to the linear congruence.

Finally, to see that this is the unique solution modulo 357 observe that

$$\begin{aligned}
 290x \equiv 5 \pmod{357} &\Leftrightarrow 290x \equiv 290 \times (-80) \pmod{357} \\
 &\Leftrightarrow x \equiv -80 \pmod{357},
 \end{aligned}$$

since 290 and 357 are coprime (using Proposition 19.3.2).

Now since $-80 \equiv 277 \pmod{357}$ we conclude that $290x \equiv 5 \pmod{357}$ if and only if $x \equiv 277 \pmod{357}$. (It is customary to express the solution in terms of the least non-negative remainders.) \square

If we are only interested in solving the congruence we can work with congruences throughout in the Euclidean algorithm. For example we could set out the calculation in the above proof as follows working modulo 357.

$$\begin{array}{rcl}
 357 & \equiv & 290 \times 0 \\
 290 & \equiv & 290 \times 1 \quad (-1) \\
 67 & \equiv & 290 \times (-1) \quad (-4) \\
 22 & \equiv & 290 \times 5 \quad (-3) \\
 1 & \equiv & 290 \times (-16) \quad (-22) \\
 0
 \end{array}$$

Thus $290x \equiv 5 \pmod{357}$ if $x \equiv (-16) \times 5 = -80 \equiv 277 \pmod{357}$. The proof of uniqueness now goes as before.

Example 20.2.3 Solve the linear congruence $255x \equiv 15 \pmod{621}$.

This is an example where a and m are not coprime. However, the method of working is very similar to the previous example.

Solution Applying the Euclidean algorithm to 255 and 621 gives the following sequence of remainders.

$$\begin{array}{r} 621 \\ 255 \quad (-2) \\ 111 \quad (-2) \\ 33 \quad (-3) \\ 12 \quad (-2) \\ 9 \quad (-1) \\ 3 \quad (-3) \\ 0 \end{array}$$

So $\gcd(255, 621) = 3$ and, since this divides 15, solutions to the linear congruence will exist according to Theorem 20.1.7. To find them we write each element in the Euclidean algorithm in turn as a multiple of 255 modulo 621.

$$\begin{array}{rcl} 621 & \equiv & 255 \times 0 \\ 255 & \equiv & 255 \times 1 \quad (-2) \\ 111 & \equiv & 255 \times (-2) \quad (-2) \\ 33 & \equiv & 255 \times 5 \quad (-3) \\ 12 & \equiv & 255 \times (-17) \quad (-2) \\ 9 & \equiv & 255 \times 39 \quad (-1) \\ 3 & \equiv & 255 \times (-56) \quad (-3) \\ 0 & & \end{array}$$

Thus $255x \equiv 15 \pmod{621}$ if $x \equiv -56 \times 5 = -280 \equiv 341 \pmod{621}$.

To find all the solutions observe that

$$\begin{aligned} 255x \equiv 15 \pmod{621} &\Leftrightarrow 255x \equiv 255 \times 341 \pmod{621} \\ &\Leftrightarrow 85x \equiv 85 \times 341 \pmod{207} \\ &\Leftrightarrow x \equiv 341 \equiv 134 \pmod{207}, \end{aligned}$$

since 85 and 207 are coprime (as we have divided through by 3, the

greatest common divisor of 255 and 621). If desired we can write the solutions modulo 621 as

$$255x \equiv 15 \pmod{621} \Leftrightarrow x \equiv 134 \text{ or } 341 \text{ or } 548 \pmod{621}.$$

□

This process can be reversed and we can use techniques for solving linear congruences to solve linear diophantine equations.

Example 20.2.4 Solve the diophantine equation $140x + 63y = 35$. [This was considered in Example 18.4.2.]

Solution From Proposition 20.2.1 there is a bijection

$$\{(x, y) \in \mathbb{Z}^2 \mid 140x + 63y = 35\} \rightarrow \{x \in \mathbb{Z} \mid 140x \equiv 35 \pmod{63}\}$$

given by $(x, y) \mapsto x$. However,

$$\begin{aligned} 140x \equiv 35 \pmod{63} &\Leftrightarrow 14x \equiv 35 \pmod{63} \\ &\quad (\text{since } 140 \equiv 14 \pmod{63}) \\ &\Leftrightarrow 2x \equiv 5 \pmod{9} \\ &\Leftrightarrow 2x \equiv 14 \pmod{9} \\ &\Leftrightarrow x \equiv 7 \pmod{9} \\ &\Leftrightarrow x = 7 + 9q \text{ (for some } q \in \mathbb{Z}). \end{aligned}$$

Substituting back into the equation we see that $x = 7 + 9q \Leftrightarrow y = -15 - 20q$ and so the solutions to the diophantine equation are given by $(x, y) = (7 + 9q, -15 - 20q)$ for $q \in \mathbb{Z}$, the same solution set as was obtained in Example 18.4.2, but expressed differently. □

If the numbers are small this is usually the best method of solving linear congruences and linear diophantine equations. When they are larger the Euclidean algorithm method is usually best.

Using the ideas of these examples it is now easy to derive Theorem 20.1.5 from previous results on linear diophantine equations.

Proof of Theorem 20.1.5 Suppose that a and m are coprime integers. Then by Theorem 18.2.1 the diophantine equation $ax + my = b$ has a solution. It follows that the congruence $ax \equiv b \pmod{m}$ has a solution.

For uniqueness modulo m , suppose that a solution is given by $x = x_0$. Then $ax \equiv b \pmod{m} \Leftrightarrow ax \equiv ax_0 \pmod{m} \Leftrightarrow x \equiv x_0 \pmod{m}$ since a and m are coprime (Proposition 19.3.2). □

The next chapter will include an alternative and very different proof of this result.

Exercises

20.1 Solve the following linear congruences:

- (i) $3x \equiv 5 \pmod{11}$;
- (ii) $10x \equiv 16 \pmod{35}$;
- (iii) $10x \equiv 5 \pmod{35}$;
- (iv) $10x \equiv 13 \pmod{21}$.

20.2 Solve the following linear congruences:

- (i) $341x \equiv 15 \pmod{912}$;
- (ii) $341x \equiv 15 \pmod{913}$;
- (iii) $345x \equiv 15 \pmod{912}$.

20.3 Interpret Theorem 20.1.7 in the case when $a = 0$.

21

Congruence classes and the arithmetic of remainders

Throughout this chapter m will denote a fixed positive integer.

The reader will be familiar with the idea that the set of integers is the disjoint union of two subsets: the set of even integers and the set of odd integers. In this case two integers lie in the same subset if and only if they are congruent modulo 2. In the same way, given any positive integer m we can divide the set of integers into m disjoint subsets, called the *congruence classes modulo m* : two integers lie in the same class if and only if they are congruent modulo m .

For some purposes, rather than using congruence of integers it is more convenient to use equality of congruence classes of integers. This is a typical process of mathematical abstraction: the set of all even integers is a more abstract notion than an even integer. In principle everything that is said about congruence classes can be reformulated in terms of congruent integers. However, as so often in mathematics the process of abstraction is enormously powerful because of the way in which it liberates our thinking. In this case one benefit of working with congruence classes is that they are finite in number so that we can make use of counting arguments like the pigeonhole principle introduced in Chapter 11. The power of this approach will be illustrated by giving an alternative proof of Theorem 20.1.5 which demonstrates that from an appropriate point of view the result is essentially ‘obvious’. A further application with far-reaching results known as Fermat’s little theorem will be described in Chapter 24.

A necessary ingredient of this proof is the idea of adding and multiplying congruence classes which can be thought of as describing an arithmetic of remainders. The idea of working in this way using con-

gruence classes arose in the work of Richard Dedekind (whose work on infinite sets was referred to in Chapter 14) in 1857.

21.1 Congruence classes

Definition 21.1.1 Given an integer a , the congruence class of a modulo m is the set of integers which are congruent to a modulo m . We denote this congruence class by $[a]_m$. Thus

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

Examples 21.1.2 (a) In the case when $m = 2$,

$$\begin{aligned}[0]_2 &= \{\dots, -4, -2, 0, 2, 4, \dots\} = \{2q \mid q \in \mathbb{Z}\} = [2]_2 = [-16]_2, \\ [1]_2 &= \{\dots, -3, -1, 1, 3, 5, \dots\} = \{2q + 1 \mid q \in \mathbb{Z}\} = [3]_2 = [-53]_2.\end{aligned}$$

Thus there are just two congruence classes modulo 2: the set of all even integers and the set of all odd integers; the congruence class of an even number is the set of all even numbers, and the congruence class of an odd number is the set of all odd numbers.

(b) In the case when $m = 6$, there are six congruence classes:

$$\begin{aligned}[0]_6 &= \{\dots, -12, -6, 0, 6, 12, \dots\} = \{6q \mid q \in \mathbb{Z}\} = [36]_6 = [-594]_6, \\ [1]_6 &= \{6q + 1 \mid q \in \mathbb{Z}\} = [49]_6, \\ [2]_6 &= \{6q + 2 \mid q \in \mathbb{Z}\}, \\ [3]_6 &= \{6q + 3 \mid q \in \mathbb{Z}\}, \\ [4]_6 &= \{6q + 4 \mid q \in \mathbb{Z}\}, \\ [5]_6 &= \{6q + 5 \mid q \in \mathbb{Z}\}.\end{aligned}$$

If we list the integers in order in rows of six –

			...	-9	-8	-7
-6	-5	-4	-3	-2	-1	
0	1	2	3	4	5	
6	7	8	...			

– then we see that the six columns form the six congruence classes modulo 6.

These examples demonstrate that the m congruence classes of integers modulo m provide a *partition* of the set of integers. This is formulated precisely in the next result. The significance of this result is that, given two integers a and b , the congruence classes $[a]_m$ and $[b]_m$ are either equal or disjoint. Hence the set of integers is the disjoint union of the m congruence classes modulo m .

Proposition 21.1.3 *For integers a, b ,*

- (i) $a \equiv b \pmod{m} \Leftrightarrow [a]_m = [b]_m$,
- (ii) $a \not\equiv b \pmod{m} \Leftrightarrow [a]_m \cap [b]_m = \emptyset$.

Thus two congruence classes modulo m are either equal or disjoint.

Constructing a proof. Notice that, since the congruence classes $[a]_m$ and $[b]_m$ are subsets of the set of integers, the statement that $[a]_m = [b]_m$ is the assertion that two subsets are equal:

$$x \in [a]_m \Leftrightarrow x \in [b]_m$$

or equivalently

$$x \equiv a \pmod{m} \Leftrightarrow x \equiv b \pmod{m}.$$

The statement that $[a]_m \cap [b]_m = \emptyset$ is a non-existence statement and $a \not\equiv b \pmod{m}$ is a negative statement and therefore it is natural to attempt proofs by contradiction for both implications in part (ii) of the proposition.

Proof (i) ‘ \Rightarrow ’: Suppose that $a \equiv b \pmod{m}$. Then $x \in [a]_m \Rightarrow x \equiv a \pmod{m} \Rightarrow x \equiv b \pmod{m}$ (by Proposition 19.1.2(iii)) $\Rightarrow x \in [b]_m$ so that $[a]_m \subseteq [b]_m$. Similarly, $[b]_m \subseteq [a]_m$ and so $[a]_m = [b]_m$.

‘ \Leftarrow ’: Suppose that $[a]_m = [b]_m$. Then, since $a \in [a]_m$, we have $a \in [b]_m$ so that $a \equiv b \pmod{m}$.

(ii) ‘ \Rightarrow ’ Suppose that $a \not\equiv b \pmod{m}$. Suppose also, for contradiction, that $[a]_m \cap [b]_m \neq \emptyset$. Then we can choose $x_0 \in [a]_m \cap [b]_m$. But then $a \equiv x_0 \equiv b \pmod{m}$ so that $a \equiv b \pmod{m}$ contradicting our hypothesis. Hence our assumption must be false and $[a]_m \cap [b]_m = \emptyset$.

‘ \Leftarrow ’: Suppose that $[a]_m \cap [b]_m = \emptyset$ and, for contradiction, that $a \equiv b \pmod{m}$. Then $a \in [a]_m \cap [b]_m$ and so $[a]_m \cap [b]_m \neq \emptyset$ giving the required contradiction. Hence $a \not\equiv b \pmod{m}$. \square

The reader may find an alternative picture of the congruence classes modulo m useful. Recall from page 90 the box model of a function. The

box model of the remainder map $r_m: \mathbb{Z} \rightarrow R_m$ (Definition 19.2.3) may be pictured as follows.

Table 21.1.4

0	1	2	3	...	$m - 1$
\vdots	\vdots	\vdots	\vdots		\vdots
$-m$					-1
0	1	2	3	...	$m - 1$
m	$m + 1$	$m + 2$	$m + 3$...	$2m - 1$
$2m$	$2m + 1$				$3m - 1$
\vdots	\vdots	\vdots	\vdots		\vdots

Here the boxes are labelled by the m remainders $0, 1, 2, \dots, m-1$. The contents of the box $r \in R_m$ form the set $\overline{r}_m(\{r\}) = \{x \in \mathbb{Z} \mid r_m(x) = r\}$ which is just the congruence class $[r]_m$. Thus this picture shows the partition of the set of integers \mathbb{Z} into the m congruence classes modulo m , generalizing the picture for $m = 6$ at the end of Example 21.1.2(b) or the layout of a calendar in the case $m = 7$. For a general integer a , the congruence class $[a]_m$ is equal to $[r]_m$ if and only if $r_m(a) = r$.

Definition 21.1.5 We write $\boxed{\mathbb{Z}_m}$ for the set of congruence classes modulo m .

Notice that an *element* of the set \mathbb{Z}_m is a *subset* of the set of integers.

Proposition 21.1.6 The set of congruence classes modulo m , \mathbb{Z}_m , is a finite set of cardinality m . The m elements are given by $[r]_m$ for integers r such that $0 \leq r < m$.

Constructing a proof. We can simply count the boxes in the above picture. If we work from left to right then we get the function given in the following proof.

Proof We may define a bijection $f: \mathbb{N}_m \rightarrow \mathbb{Z}_m$ by $f(i) = [i-1]_m$. This is a bijection because it has an inverse given by $g([a]_m) = r_m(a) + 1$.

This means that

$$\begin{aligned}\mathbb{Z}_m &= \{f(1), f(2), \dots, f(m)\} \\ &= \{[0]_m, [1]_m, \dots, [m-1]_m\}.\end{aligned}$$

□

The reader should consider what is involved in the assertions that this function g is well-defined and is an inverse to f – see Exercise 21.6.

21.2 The arithmetic of congruence classes

The reader is probably familiar with the following properties of the addition and multiplication of even and odd integers.

$+$	even	odd	\times	even	odd
even	even	odd	even	even	even
odd	odd	even	odd	even	odd

These tables describe the way odd and even integers behave under addition and multiplication. We can see them as a way of adding and multiplying congruence classes modulo 2, a description of arithmetic in the set \mathbb{Z}_2 as follows.

$+$	[0] ₂	[1] ₂	\times	[0] ₂	[1] ₂
[0] ₂	[0] ₂	[1] ₂	[0] ₂	[0] ₂	[0] ₂
[1] ₂	[1] ₂	[0] ₂	[1] ₂	[0] ₂	[1] ₂

The first table describes how the parity (congruence class modulo 2) of integers a and b determines the parity of their sum $a + b$ and the second gives the same information for the product. We can think of this as defining addition and multiplication in the set \mathbb{Z}_2 .

We are now going to consider arithmetic in the set of congruence classes \mathbb{Z}_m . Remember that the elements of this set are subsets of the integers, the m subsets forming the columns in Table 21.1.4. To do arithmetic we need to know how to add and multiply two columns together. The method used to add two columns is to choose any element from each column, add the elements and look which column the result lies in. It turns out that whatever choices are made their sum will lie in the same column and so we can define the resulting column as the sum of the two columns to be added. The definition of subtraction and multiplication is similar. Here is the formal definition.

Definition 21.2.1 Addition, subtraction and multiplication of elements of \mathbb{Z}_m are defined by

$$[a]_m + [b]_m = [a + b]_m,$$

$$[a]_m - [b]_m = [a - b]_m,$$

$$[a]_m \times [b]_m = [ab]_m.$$

Proposition 21.2.2 *Addition, subtraction and multiplication in \mathbb{Z}_m are well-defined.*

Let us illustrate this in the case of multiplication in \mathbb{Z}_8 . The eight congruence classes modulo 8 are given by the columns in the following picture.

:	:	:	:	:	:	:	:
-8	-7						-1
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17						23
:	:	:	:	:	:	:	:

We can describe the third column as $[2]_8$ or as $[10]_8$. We can describe the eighth column as $[7]_8$ or as $[31]_8$. Multiplying the first representatives gives $2 \times 7 = 14$ which lies in the seventh column. Multiplying the second representatives gives $10 \times 31 = 310 = 8 \times 38 + 6$ which also lies in the seventh column. The reader might like to experiment a little more: whatever elements are chosen from the third column and the eighth column their product will lie in the seventh column. This is what is meant in this case by asserting that the definition of multiplication is well-defined.

This procedure leads to the following multiplication table in which as usual congruence classes are represented by the least non-negative remainders modulo 8.

\times	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[1]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[2]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[3]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$
$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[5]_8$	$[0]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$
$[6]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$
$[7]_8$	$[0]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$

Constructing a proof of Proposition 21.2.2. Whenever a definition involves choices it is necessary to check that the outcome is independent of the choice. We indicate the proof for multiplication and leave the proofs for addition and subtraction as exercises (see Exercise 21.1). To prove that multiplication is well-defined it is necessary to demonstrate that

$$[a_1]_m = [a_2]_m \text{ and } [b_1]_m = [b_2]_m \Rightarrow [a_1 b_1]_m = [a_2 b_2]_m.$$

Using Proposition 21.1.3 this can be rewritten

$$a_1 \equiv a_2 \pmod{m} \text{ and } b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

This is one of the parts of Proposition 19.1.3 and so the result holds.

Notice that addition and multiplication in \mathbb{Z}_m inherit the good properties of addition and multiplication in the integers described in Properties 2.3.1: they are commutative, associative and multiplication is distributive over addition. Notice also that the element $[0]_m$ plays the rôle of 0 in this arithmetic since it is an additive identity:

$$[a]_m + [0]_m = [a]_m \text{ for all } [a]_m \in \mathbb{Z}_m.$$

In the same way the element $[1]_m$ plays the rôle of 1 since it is a multiplicative identity:

$$[a]_m \times [1]_m = [a]_m \text{ for all } [a]_m \in \mathbb{Z}_m.$$

21.3 The arithmetic of remainders

It is possible to view the arithmetic of congruence classes in a slightly different way which the reader may find more acceptable – as the arithmetic of remainders. Consider the following definitions.

Definition 21.3.1 Addition, subtraction and multiplication of elements of R_m are defined by

$$\begin{aligned} a +_m b &= r_m(a + b), \\ a -_m b &= r_m(a - b), \\ a \times_m b &= r_m(ab) \end{aligned}$$

for $a, b \in R_m$.

Thus to perform addition of remainders, for example, we simply perform ordinary addition and then take the remainder modulo m .

We can then write out addition and multiplication tables for R_m . For example in the case of $m = 10$ we get the following multiplication table.

\times_{10}	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Arithmetic modulo 10 is very familiar since the remainder of a positive integer modulo 10 is simply the last (right-hand) digit when it is written in the usual decimal notation.

It is easy to see the relationship between this remainder arithmetic and the arithmetic of congruences. If we represent the congruence classes modulo m as $[a]_m$ for $a \in R_m$ as described in Proposition 21.1.6 then there is a complete correspondence.

Proposition 21.3.2 For a and $b \in R_m$,

$$\begin{aligned} [a]_m + [b]_m &= [a +_m b]_m, \\ [a]_m - [b]_m &= [a -_m b]_m, \\ [a]_m \times [b]_m &= [a \times_m b]_m. \end{aligned}$$

This shows that the tables for addition, subtraction and multiplication in \mathbb{Z}_m can be obtained from those for R_m simply by replacing $a \in R_m$ by $[a]_m \in \mathbb{Z}_m$. This provides an example of two *isomorphic* algebraic structures. The reader will meet the general concept of isomorphism (meaning ‘same form’) when going on to study abstract algebra.

Proof The addition result follows immediately from the fact that $a + b \equiv a +_m b \text{ mod } m$ and similarly for subtraction and multiplication. (See Exercise 21.2.) \square

21.4 Linear diophantine equations

There are two big differences between arithmetic in \mathbb{Z}_m or R_m and arithmetic in \mathbb{Z} . Firstly, the set R_m is finite and so we can always find all the solutions to equations simply by trying out the possibilities. Secondly, division is rather different. In the integers, the only numbers by which we can always divide are 1 and -1 . But in R_m there are other numbers which we can always divide by. These differences may be illustrated by revisiting the linear diophantine equation problem.

Recall the main result guaranteeing the existence of solutions.

Theorem 20.1.5 *Suppose that a and b are integers such that a and m are coprime. Then the linear congruence*

$$ax \equiv b \pmod{m} \quad (21.1)$$

has a solution. This solution is unique up to congruence modulo m .

This result can be reformulated in the language of congruence classes as follows since $ax \equiv b \pmod{m}$ if and only if $[ax]_m = [b]_m$.

Theorem 21.4.1 *Suppose that a and b are integers such that a and m are coprime. Then the equation*

$$[a]_m \times [x]_m = [b]_m \quad (21.2)$$

has a solution in \mathbb{Z}_m . This solution is unique.

This reformulation enables us to illustrate the power of the congruence class approach for, in this formulation, since the set of congruence classes is finite it is possible to give a proof using a counting argument.

Constructing a proof. Let $\text{Row}(a)$ be the set of elements in the row corresponding to $[a]_m$ in the multiplication table for \mathbb{Z}_m . Notice the following.

- Equation (21.2) has a solution if and only if the congruence class $[b]_m$ occurs in $\text{Row}(a)$.
- If the elements in $\text{Row}(a)$ are all distinct (so that there are m of them) then $\text{Row}(a) = \mathbb{Z}_m$ (and so certainly $[b]_m \in \text{Row}(a)$). [This is a consequence of the pigeonhole principle – see Exercise 11.5.]
- The elements in $\text{Row}(a)$ are all distinct if $(a, m) = 1$ (by Proposition 19.3.2).

These three statements taken together prove that equation (21.2) has a

solution if a and m are coprime. The distinctness of the elements in the row implies that the solution is unique.

In writing out the formal proof we go back to the pigeonhole principle (Theorem 11.1.2). To use this we need a function between finite sets.

Proof Define a function $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ by $f([x]_m) = [a]_m \times [x]_m$.

Now, by Proposition 19.3.2, since $(a, m) = 1$, the function f is an injection, for

$$\begin{aligned} f([x_1]_m) = f([x_2]_m) &\Rightarrow [ax_1]_m = [ax_2]_m \\ &\Rightarrow ax_1 \equiv ax_2 \pmod{m} \\ &\Rightarrow x_1 \equiv x_2 \pmod{m} \\ &\Rightarrow [x_1]_m = [x_2]_m. \end{aligned}$$

We can now see that it is a surjection using the pigeonhole principle (as in Theorem 11.1.7). For suppose for contradiction that it is not a surjection. Then there is some element $[y_0]_m \in \mathbb{Z}_m$ which is not a value of f and so f is an injection $\mathbb{Z}_m \rightarrow \mathbb{Z}_m - \{[y_0]_m\}$ from a set of cardinality m to a set of cardinality $m-1$ which contradicts the pigeonhole principle. Hence f is a surjection and so a bijection.

Thus there is a unique element $[x_0]_m \in \mathbb{Z}_m$ such that $f([x_0]_m) = [b]_m$, i.e. such that $[a]_m \times [x_0]_m = [b]_m$. \square

Notice that this proof is non-constructive, in other words it does not give a means of finding the solutions to the congruence but simply guarantees that these exist. This is a common feature of proofs involving counting arguments. Of course since there are only m congruence classes modulo m we can try them in turn and this will inevitably lead to the solution. However, if m is large this may not be very efficient; then the Euclidean algorithm method described in the previous chapter can be used.

The reader may feel that the proof based on the Euclidean algorithm is preferable, particularly since it does give an algorithm for finding the solution. However, it can be argued that the proof using congruence classes makes it clearer why the result is true. In the end both proofs have something to offer in the exploration of the idea of congruence. This illustrates the way in which a proof is not simply a logical argument demonstrating that a claim is true: a good proof illuminates the relationships between the mathematical ideas involved and different proofs can provide different illumination.

Example 21.4.2 If we look at the row corresponding to 7 in the multiplication table for R_{10} then we see that every remainder modulo 10 occurs precisely once in this row. This means that we can always divide by 7: the equation $7 \times_{10} x = b$ for $b \in R_{10}$, or equivalently the equation $[7]_{10} \times [x]_{10} = [b]_{10}$, always has a unique solution. If we examine for which rows this is true we find that it is the rows corresponding to 1, 3, 7, 9 and these are precisely the elements of R_{10} which are coprime to 10.

Furthermore these are the only rows containing the element 1. We now show that this is always the case. An element is called invertible when the corresponding row in the multiplication table contains 1.

Definition 21.4.3 The element $[a]_m \in \mathbb{Z}_m$ is called invertible (or $a \in \mathbb{Z}$ is invertible modulo m) if there is an integer $a' \in \mathbb{Z}$ such that $[a]_m \times [a']_m = [1]_m$ (or equivalently $aa' \equiv 1 \pmod{m}$). $[a']_m \in \mathbb{Z}_m$ is called the inverse of $[a]_m$ and we write $[a']_m = ([a]_m)^{-1}$. Alternatively, we say that a' is an inverse of a modulo m .

For example, in \mathbb{Z}_{10} the invertible elements are $[1]_{10}$, $[3]_{10}$, $[7]_{10}$ and $[9]_{10}$ and the inverses are given by $([1]_{10})^{-1} = [1]_{10}$, $([3]_{10})^{-1} = [7]_{10}$, $([7]_{10})^{-1} = [3]_{10}$ and $([9]_{10})^{-1} = [9]_{10}$.

Proposition 21.4.4 The integer a is invertible modulo m if and only if every linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m .

Notice that this means that $\text{Row}(a) = \mathbb{Z}_m$ in the multiplication table for \mathbb{Z}_m : each congruence class occurs precisely once in the row. This result is an immediate consequence of the next result.

Proposition 21.4.5 Suppose that a' is an inverse of a modulo m . Then

$$ax \equiv b \pmod{m} \Leftrightarrow x \equiv a'b \pmod{m}.$$

Proof Since a' is an inverse modulo m of a , $aa' \equiv 1 \pmod{m}$. Thus

$$ax \equiv b \pmod{m} \Rightarrow a'ax \equiv a'b \pmod{m} \Rightarrow x \equiv a'b \pmod{m}$$

and

$$x \equiv a'b \pmod{m} \Rightarrow ax \equiv aa'b \pmod{m} \Rightarrow ax \equiv b \pmod{m}$$

as required. \square

Notice that this means that once we have found an inverse modulo m to a then we can compute the solution to any linear congruence $ax \equiv b \pmod{m}$ by multiplication. This is illustrated in Exercise 21.5.

Exercises

21.1 Use Proposition 19.1.3 to confirm that addition and subtraction in \mathbb{Z}_m are well-defined by Definition 21.3.2.

21.2 Prove that $a +_m b \equiv a + b \pmod{m}$, $a -_m b \equiv a - b \pmod{m}$ and $a \times_m b \equiv ab \pmod{m}$. [This was used in the proof of Proposition 21.3.2.]

21.3 Write down the multiplication table for R_{12} . From the table identify the invertible elements modulo 12 and their inverses.

21.4 Prove that a is invertible modulo m if and only if a and m are coprime.

21.5 Prove that 290 is invertible modulo 357 and find its inverse. Hence solve the linear congruences:

- (i) $290x \equiv 2 \pmod{357}$;
- (ii) $290x \equiv 5 \pmod{357}$;
- (iii) $290x \equiv 355 \pmod{357}$.

21.6 Prove that the function $g: \mathbb{Z}_m \rightarrow N_m$ used in the proof of Proposition 21.1.6 is well-defined and an inverse to the function f .

22

Partitions and equivalence relations

In the previous chapter we saw that congruence of integers can be viewed in two ways: as a relation between certain integers and as a partition of the set of integers. This is an example of a very general concept, known as an equivalence relation, which the reader will encounter frequently in more advanced pure mathematics.

An equivalence relation on a set corresponds to a partition of the set. In this chapter this correspondence is explained and a number of examples discussed.

22.1 Partitions

We saw in Chapter 21 that the relation of congruence modulo m partitions the set of integers \mathbb{Z} into m disjoint *congruence classes* (see Proposition 21.1.3). Let us make the notion of a partition of a set precise.

Definition 22.1.1 *Let X be a set. Recall that the power set of X , denoted $\mathcal{P}(X)$, is the set of all subsets of X . A partition of the set X is a subset Π of $\mathcal{P}(X)$, i.e. a set of subsets of X , such that*

- (i) *the subsets in Π are non-empty, i.e. $A \in \Pi \Rightarrow A \neq \emptyset$,*
- (ii) *the subsets in Π are disjoint, i.e.*
 $\forall A_1, A_2 \in \Pi, (A_1 \neq A_2 \Rightarrow A_1 \cap A_2 = \emptyset),$
- (iii) *the subsets in Π cover X : $\forall x \in X, \exists A \in \Pi, x \in A$.*

Examples 22.1.2 (a) By Proposition 21.1.3, the set of congruence classes modulo m ,

$$\mathbb{Z}_m = \{ [a]_m \mid a \in \mathbb{Z} \} = \{ [a]_m \mid a \in R_m \},$$

is a partition of \mathbb{Z} into m subsets.

(b) A set of people may be partitioned according to the year of their birth.

(c) A partition of the set N_{10} is given by

$$\Pi = \{\{1, 3, 7, 8\}, \{2, 9, 10\}, \{4\}, \{5, 6\}\}.$$

(d) A partition of the set \mathbb{Z} is given by

$$\Pi = \{\mathbb{Z}^+, \{0\}, \mathbb{Z}^- = \{n \in \mathbb{Z} \mid n < 0\}\}.$$

(e) The set of subsets

$$\{\{1, 2, 3, 4, 5\}, \{5, 6, 7, 8, 9\}\}$$

is not a partition of N_9 since the element 5 lies in both subsets.

(f) The set of subsets

$$\{\{1, 2, 3, 4\}, \{6, 7, 8, 9\}\}$$

is not a partition of N_9 since the element 5 lies in neither subset.

We have already seen that congruence classes modulo m are obtained by partitioning the integers according to the remainder after division by m . It is common to describe a partition by means of some property of the elements such as the remainder after division by m which can be used for Example 22.1.2(a), or the date of birth used in Example 22.1.2(b). This amounts to partitioning according to the value of some function at each point.

Proposition 22.1.3 *Let $f: X \rightarrow Y$ be a surjection. Then X may be partitioned according to the value of the function f giving the partition*

$$\Pi = \{\overleftarrow{f}(\{y\}) \mid y \in Y\}.$$

Recall from Definition 9.3.1 that $\overleftarrow{f}(\{y_0\}) = \{x \in X \mid f(x) = y_0\}$.

Proof The proof of this result is immediate from the definitions: the sets of the partition are non-empty since f is a surjection, they are disjoint because the function f is well-defined, and they cover X because f has a value in Y at each point of X . \square

Examples 22.1.4 (a) The partition of the integers by congruence classes modulo m corresponds to the remainder map $r_m: \mathbb{Z} \rightarrow R_m$ discussed in

Chapter 19.

(b) The partition of the integers of Example 22.1.2(d) corresponds to the function

$$f: \mathbb{Z} \rightarrow \{-1, 0, 1\}$$

defined by

$$f(x) = \begin{cases} x/|x| & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

22.2 Equivalence relations

The idea of a partition takes as its starting point the set to be partitioned or divided up. We can view the same idea from the point of view of the elements. If a set of people is physically partitioned into subsets with possibly each subset put in a separate room, each person may not have a good idea of the overall picture but they are able to see who is in the same subset as themselves by looking round the room. A partition of a set X determines a *relation* on the set: two elements are related if they are in the same subset of the partition.

A *relation* on a set X is determined by a property which may or may not be satisfied by each ordered pair of elements of the set. If an ordered pair of elements a and b satisfies the property then we say that the elements are related and write $a \sim b$ to indicate this. We write $a \not\sim b$ to denote the fact that the ordered pair (a, b) does not satisfy the property and so the elements are not related.

Proposition 22.2.1 *Suppose that Π is a partition of the set X . Then we may define a relation on the set X as follows. For elements a and b of X , a is related to b , written $a \sim_{\Pi} b$, if and only if a and b belong to the same subset of the partition. Then this relation has the following properties.*

- (i) Reflexive property. *For all $a \in X$, $a \sim_{\Pi} a$.*
- (ii) Symmetric property. *If a and b are elements of X such that $a \sim_{\Pi} b$, then $b \sim_{\Pi} a$.*
- (iii) Transitive property. *If a , b and c are elements of X such that $a \sim_{\Pi} b$ and $b \sim_{\Pi} c$, then $a \sim_{\Pi} c$.*

This result should be compared with Proposition 19.1.2. Starting from the partition of the integers into congruence classes modulo m we obtain the relation of congruence modulo m .

Proof The relation is clearly reflexive and symmetric. For transitivity, suppose that $a \sim_{\Pi} b$ and $b \sim_{\Pi} c$. Then a and b belong to some $A_1 \in \Pi$ and b and c belong to some $A_2 \in \Pi$. Now $b \in A_1 \cap A_2$ and so these two subsets are not disjoint. Thus $A_1 = A_2$ and so $a \sim_{\Pi} c$. \square

A relation with these three properties is called an *equivalence relation*. In order to clarify the significance of the properties we consider a variety of relations.

Examples 22.2.2 (a) The relation ' \leq ' on \mathbb{Z} the set of integers.

- (b) The relation ' $<$ ' on \mathbb{Z} .
- (c) The relation ' $=$ ' on \mathbb{Z} .
- (d) We can define a relation on \mathbb{Z} by $a \sim b \Leftrightarrow ab > 0$.
- (e) We can define a relation on \mathbb{Z} by $a \sim b \Leftrightarrow ab = 0$.
- (f) We can define a relation on the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1$.
- (g) For each positive integer m , congruence modulo m defines a relation on the set \mathbb{Z} .

We now consider the particular features of relations arising from a partition of a set described in Proposition 22.2.1.

Definition 22.2.3 Suppose that \sim is a relation on a set X .

- (i) The relation is said to be reflexive when, for all $x \in X$, $x \sim x$.
- (ii) The relation is said to be symmetric when, for all elements x, y of X , $x \sim y \Rightarrow y \sim x$.
- (iii) The relation is said to be transitive when, for all elements x, y, z of X , $x \sim y$ and $y \sim z \Rightarrow x \sim z$.

An equivalence relation on the set X is a relation which is reflexive, symmetric and transitive.

Let us look at the above examples.

Examples 22.2.4 (a) The relation ' \leq ' on \mathbb{Z} is reflexive (since $\forall a \in \mathbb{Z}, a \leq a$), is not symmetric (since $1 \leq 2$ but $2 \not\leq 1$) and is transitive (since $a \leq b$ and $b \leq c \Rightarrow a \leq c$).

- (b) The relation ' $<$ ' on \mathbb{Z} is not reflexive (since $1 \not< 1$), is not symmetric (since $1 < 2$ but $2 \not< 1$), and is transitive ($a < b$ and $b < c \Rightarrow a < c$).
- (c) The relation '=' on \mathbb{Z} is reflexive ($\forall a \in \mathbb{Z}, a = a$), is symmetric ($\forall a, b \in \mathbb{Z}, a = b \Rightarrow b = a$) and is transitive ($\forall a, b, c \in \mathbb{Z}, a = b$ and $b = c \Rightarrow a = c$). This is an equivalence relation.
- (d) The relation $a \sim b \Leftrightarrow ab > 0$ on \mathbb{Z} is not reflexive ($0 \not\sim 0$ since $0^2 = 0 \not> 0$), is symmetric ($ab > 0 \Rightarrow ba > 0$) and is transitive (since $ab > 0$ and $bc > 0 \Rightarrow ab^2c > 0 \Rightarrow ac > 0$).
- (e) The relation $a \sim b \Leftrightarrow ab = 0$ on \mathbb{Z} is not reflexive ($1 \not\sim 1$ since $1^2 = 1 \neq 0$), is symmetric (since $ab = 0 \Rightarrow ba = 0$) and is not transitive (since $1 \sim 0$ and $0 \sim 1$ but $1 \not\sim 1$).
- (f) The relation $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1b_2 = a_2b_1$ on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ is reflexive, symmetric and transitive (since $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1/b_1 = a_2/b_2 \in \mathbb{Q}$) and so an equivalence relation.
- (g) Proposition 19.1.2 asserts that congruence modulo m is an equivalence relation on the set of integers.
- (h) More generally, Proposition 22.2.1 asserts that the relation \sim_Π arising from a partition Π of the set X is an equivalence relation. We will demonstrate in the next section that every equivalence relation arises from a partition.

Notice that these properties of a relation are universal statements and so to prove that one fails it is only necessary to give a single counter-example.

22.3 Equivalence relations and partitions

We saw in Chapter 21 that the partition of the set of integers into congruence classes modulo m arises from the relation of congruence modulo m (see Proposition 21.1.3). This is a quite general phenomenon. Any equivalence relation on a set X determines a partition of the set X to which it corresponds. The construction of the partition is an immediate generalization of Proposition 21.1.3.

Definition 22.3.1 Suppose that \sim is an equivalence relation on a non-empty set X . For each $a \in X$ we define the equivalence class of a to be the set of elements of X which are equivalent to a . We denote this

class by $\boxed{[a]}$. Thus

$$[a] = \{x \in X \mid x \sim a\}.$$

Observe that each equivalence class is a subset of X . We denote the set of all equivalence classes by X/\sim , i.e.

$$X/\sim = \{[a] \mid a \in X\} \subseteq \mathcal{P}(X).$$

This is a straightforward generalization of the idea of congruence class; when the equivalence relation is congruence modulo m on the set of integers then the equivalence classes are the congruence classes modulo m . We can now generalize Proposition 21.1.3 and its proof.

Theorem 22.3.2 Suppose that \sim is an equivalence relation on the set X . Then, for $a, b \in X$,

- (i) $a \sim b \Leftrightarrow [a] = [b]$,
- (ii) $a \not\sim b \Leftrightarrow [a] \cap [b] = \emptyset$.

Proof (i) ' \Rightarrow ': Suppose that $a \sim b$. Then $x \in [a] \Rightarrow x \sim a \Rightarrow x \sim b$ (by transitivity) $\Rightarrow x \in [b]$ so that $[a] \subseteq [b]$. Similarly, since $a \sim b \Rightarrow b \sim a$ (symmetry), $[b] \subseteq [a]$ and so $[a] = [b]$.

' \Leftarrow ': Suppose that $[a] = [b]$. Then, since $a \in [a]$ (by reflexivity), $a \in [b]$ so that $a \sim b$.

(ii) ' \Rightarrow ' Suppose that $a \not\sim b$. Suppose for contradiction that $[a] \cap [b] \neq \emptyset$. Then we can choose $x_0 \in [a] \cap [b]$. But then $x_0 \sim a$ and $x_0 \sim b \Rightarrow a \sim x_0$ and $x_0 \sim b$ (by symmetry) $\Rightarrow a \sim b$ (by transitivity) contradicting our hypothesis. Hence our assumption must be false and $[a] \cap [b] = \emptyset$.

' \Leftarrow ': Suppose that $[a] \cap [b] = \emptyset$ and, for contradiction, that $a \sim b$. Then $a \in [a]$ (by reflexivity) and $a \in [b]$ (by assumption) so that $a \in [a] \cap [b]$ and so $[a] \cap [b] \neq \emptyset$ giving the required contradiction. Hence $a \not\sim b$. \square

Corollary 22.3.3 Suppose that \sim is an equivalence relation on a non-empty set X . Then the set of equivalence classes $\Pi = X/\sim$ is a partition of X . The relation arising from this partition is \sim .

Proof The theorem shows that distinct equivalence classes are disjoint. They cover X because, for each $x \in X$, $x \in [x]$ (reflexivity). They are non-empty because by definition an equivalence class is $[a]$ for some $a \in X$ and again reflexivity ensures that $a \in [a]$.

Part (i) of the theorem is the statement that \sim is equal to \sim_{Π} the relation arising from the partition. \square

This is the converse to Proposition 22.2.1 and demonstrates that the notions of an equivalence relation on the set X and a partition of the set X correspond and are simply different ways of thinking about the same concept.

We saw earlier that a surjection with domain X gives rise to a partition of X . As a final result in this chapter we reformulate this in terms of equivalence relations.

Proposition 22.3.4 *Let $f: X \rightarrow Y$ be a surjection. Define an equivalence relation on X by $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$. Then the map f induces a bijection $X/\sim \rightarrow Y$ by $[x] \mapsto f(x)$.*

Proof Define $F: X/\sim \rightarrow Y$ by $F([x]) = f(x)$ for each $x \in X$. We must check that this function is well-defined. Suppose that $x_1, x_2 \in X$. Then

$$\begin{aligned} [x_1] = [x_2] &\Rightarrow x_1 \sim x_2 \\ &\Rightarrow f(x_1) = f(x_2) \quad \text{by definition of } \sim. \end{aligned}$$

The function F is a surjection since f is a surjection. The proof that it is injective is as follows. Suppose that $[x_1], [x_2] \in X/\sim$. Then

$$\begin{aligned} F([x_1]) = F([x_2]) &\Rightarrow f(x_1) = f(x_2) \quad \text{by definition of } F \\ &\Rightarrow x_1 \sim x_2 \quad \text{by definition of } \sim \\ &\Rightarrow [x_1] = [x_2]. \end{aligned}$$

Thus F is a bijection. \square

Example 22.3.5 Define a function $f: \mathbb{Z} \times (\mathbb{Z} - \{0\}) \rightarrow \mathbb{Q}$ by $f(a, b) = a/b$. Then $f(a_1, b_1) = f(a_2, b_2) \Leftrightarrow a_1/b_1 = a_2/b_2 \Leftrightarrow a_1b_2 = a_2b_1$ and so the equivalence relation \sim on $\mathbb{Z} \times \mathbb{Z} - \{0\}$ induced by the function f as in Theorem 22.3.4 is the equivalence relation of Example 22.2.2(f). It follows that there is a bijection $F: (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim \rightarrow \mathbb{Q}$.

This formalizes the relationship between fractions and rationals discussed in Chapter 13. There we observed that two fractions a_1/b_1 and a_2/b_2 represent the same rational number if and only if $a_1b_2 = a_2b_1$, i.e. $(a_1, b_1) \sim (a_2, b_2)$. We can think of the set of fractions as $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ with (a, b) written as a/b .

Now with hindsight we can see how to recast the material in Section 13.1 in the language of equivalence relations. We start with the

equivalence relation on the set $\mathbb{Z} \times (\mathbb{Z} - \{0\})$:

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1.$$

Then we *define* the set of rational numbers to be the set of equivalence classes of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ under this equivalence relation. Now it can be seen that the notation $q = \langle a/b \rangle$ indicating that the fraction a/b represents the rational q simply anticipated the notation $q = [(a, b)]$ indicating that the pair (a, b) represents the equivalence class q .

Addition and multiplication of rational numbers (that is equivalence classes) may now be defined by

$$\begin{aligned} [(a_1, b_1)] + [(a_2, b_2)] &= [(a_1 b_2 + a_2 b_1, b_1 b_2)], \\ [(a_1, b_1)] \times [(a_2, b_2)] &= [(a_1 a_2, b_1 b_2)], \end{aligned}$$

and as in Proposition 13.1.5 these operations are well-defined.

The set of integers may be embedded in the set of rationals by letting $a \in \mathbb{Z}$ correspond to $[(a, 1)]$. It is now possible to check that the above definitions of addition and multiplication of rationals extend the definitions for integers and satisfy all the basic algebraic properties of numbers discussed in Chapter 2. It follows that $[(a, b)]$ is the unique rational solution to the equation $bx = a$. The notion of inequality between integers can also be extended to the rationals (see Problems III, Question 21).

Having done this we can agree to use the fraction a/b to represent the equivalence class $[(a, b)]$ and so obtain the usual notation for the rational numbers.

Exercises

22.1 For each of the following relations on the set X determine whether it is reflexive, whether it is symmetric and whether it is transitive. For those which are equivalence relations, describe the equivalence classes.

- (i) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow a + b$ is even.
- (ii) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow a + b$ is odd.
- (iii) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow a + b$ is divisible by 3.
- (iv) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow a^2 = b^2$.
- (v) For $X = \{1, 2\}$, put $a \sim b \Leftrightarrow a = 1$ and $b = 1$.
- (vi) For $X = \{1, 2\}$, put $a \sim b \Leftrightarrow a = 1$ or $b = 1$.
- (vii) For $X = \mathbb{R} \times \mathbb{R}$, $(a_1, a_2) \sim (b_1, b_2) \Leftrightarrow a_1 = b_1$.
- (viii) For $X = \mathbb{R} \times \mathbb{R}$, $(a_1, a_2) = (b_1, b_2) \Leftrightarrow a_1^2 + a_2^2 = b_1^2 + b_2^2$.

22.2 Describe the equivalence relation on \mathbb{Z} determined by the partition $\Pi = \{A, B, C\}$ where $A = \mathbb{Z}^+$, $B = \mathbb{Z}^-$ and $C = \{0\}$.

22.3 Define a function $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}$ by $f(x_1, x_2) = x_1 - x_2$. Prove that this is a surjection. Identify the equivalence classes of the equivalence relation defined by $(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow f(x_1, x_2) = f(y_1, y_2)$.

Problems V: Modular arithmetic

1. Prove, for positive integers n , that 7 divides $6^n + 1$ if and only if n is odd.
2. Prove that, for all integers a and b , $a^2 + b^2 \equiv 0, 1, 2, 4$ or 5 modulo 8. Deduce that there do not exist integers a and b such that $a^2 + b^2 = 12345790$.
3. Suppose that a positive integer is written in decimal notation as $n = a_k a_{k-1} \dots a_2 a_1 a_0$ where $0 \leq a_i \leq 9$. Prove that n is divisible by 9 if and only if the sum of its digits $a_k + a_{k-1} + \dots + a_1 + a_0$ is divisible by 9.
4. Suppose that a positive integer is written in decimal notation as $n = a_k a_{k-1} \dots a_2 a_1 a_0$ where $0 \leq a_i \leq 9$. Prove that n is divisible by 11 if and only if the alternating sum of its digits $a_0 - a_1 + \dots + (-1)^k a_k$ is divisible by 11.
5. Find a test similar to those in the previous questions for divisibility by 99.
6. Prove that the diophantine equation $3x^2 + 4y^2 = 5z^2$ has no non-trivial (i.e. $(x, y, z) \neq (0, 0, 0)$) solutions.

[Give a proof by contradiction. Obtain a contradiction by proving that if there is a non-trivial solution then there is a solution (x_1, y_1, z_1) with $x_1 \not\equiv 0 \pmod{5}$ or $y_1 \not\equiv 0 \pmod{5}$.]

Deduce that the equation $3x^2 + 4y^2 = 5$ has no rational solutions.

- 7.** What is the last digit of 2^{1000} ?
- 8.** Prove that the Fibonacci number u_n (see Definition 5.4.2) is divisible by 3 if and only if n is divisible by 4.
- 9.** Solve the following linear congruences:
- (i) $3x \equiv 15 \pmod{18}$;
 - (ii) $3x \equiv 16 \pmod{18}$;
 - (iii) $4x \equiv 16 \pmod{18}$;
 - (iv) $4x \equiv 14 \pmod{18}$.
- 10.** Solve the following linear congruences:
- (i) $23x \equiv 16 \pmod{107}$;
 - (ii) $234x \equiv 20 \pmod{366}$;
 - (iii) $234x \equiv 6 \pmod{366}$;
 - (iv) $234x \equiv 36 \pmod{366}$.
- 11.** Using the result of Question 10(iv), solve the diophantine equation
- $$234x + 366y = 36.$$
- 12.** Write down the multiplication table for R_{15} . From the table identify the invertible elements modulo 15 and their inverses.
- 13.** Prove that each row in the multiplication table for R_m either includes the element 1 or includes the element 0 more than once (but not both).
- 14.** Using a counting argument, prove from the multiplication table for R_m that, for each integer a , there exists an integer b_1 such that $ax \equiv b_1 \pmod{m}$ has no solution if and only if there exists an integer b_2 such that $ax \equiv b_2 \pmod{m}$ has more than one solution modulo m .
- 15.** Prove that 245 is invertible modulo 666 and find its inverse. Hence solve the linear congruences:
- (i) $245x \equiv 3 \pmod{666}$;
 - (ii) $245x \equiv 656 \pmod{666}$.
- 16.** Identify the invertible elements of \mathbb{Z}_{18} and write down their inverses.

17. For each of the following relations on the set X determine whether it is reflexive, whether it is symmetric and whether it is transitive. For those which are equivalence relations, describe the equivalence classes.

- (i) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow ab \neq 0$.
- (ii) For $X = \mathbb{Z}$, put $a \sim b \Leftrightarrow ab \geq 0$.
- (iii) For $X = \mathbb{Z}^+$, put $a \sim b \Leftrightarrow ab > 0$.
- (iv) For $X = \mathbb{Z} - \{0\}$, put $a \sim b \Leftrightarrow ab > 0$.
- (v) For $X = \mathbb{Z}^+$, put $a \sim b \Leftrightarrow ab < 0$.
- (vi) For $X = \mathbb{Z} - \{0\}$, put $a \sim b \Leftrightarrow ab < 0$.

18. Which of the following formulae define a (well-defined) function $f: \mathbb{Q} \rightarrow \mathbb{Q}$?

- (i) $f(a/b) = a^2/b^2$.
- (ii) $f(a/b) = a^2/b^3$.
- (iii) $f(a/b) = b/a$.
- (iv) $f(a/b) = a + b$.
- (v) $f(a/b) = (a - b)/2b$.

19. Which of the following formulae define a (well-defined) function $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_4$?

- (i) $f([a]_6) = [a + 1]_4$.
- (ii) $f([a]_6) = [2a]_4$.
- (iii) $f([a]_6) = [a^2]_4$.

Part VI

Prime numbers

23

The sequence of prime numbers

To conclude this book we now spend some time exploring the theory of prime numbers, one of the most fascinating and oldest areas of number theory and one in which some apparently very simple questions still remain unanswered. It is a branch of mathematics which until recently seemed remote from any applications but this has now changed. In this chapter we consider the sequence of prime numbers and factorization into primes.

23.1 Definition and basic properties

Definition 23.1.1 A positive integer n is said to be **prime** when $n > 1$ and the only positive divisors of n are 1 and n . If an integer $n > 1$ is not prime then it is said to be **composite**.

Thus $n > 1$ is composite if and only if it can be written as a product $n = ab$ of integers a and b such that $1 < a < n$ and $1 < b < n$. If a prime number n is the product of two positive integers, $n = ab$, then either $a = 1$ and $b = n$ or $a = n$ and $b = 1$.

To some extent it is a matter of convention whether we call the number 1 prime but it is convenient to exclude it for reasons which will become clear in the next chapter. Thus the positive integers are partitioned into three subsets: the set of primes, the set of composites, and the set of units (which just consists of 1).

The first few prime numbers are as follows:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Proposition 23.1.2 *Every integer greater than 1 can be written as a product of prime numbers.*

Here we think of a prime number as a product of a single prime number, namely itself! We can extend this result to include 1 by adopting the convention that the product of no numbers at all is equal to 1 (remember that $x^0 = 1$).

The proof of Proposition 23.1.2 is *the* classic example of a proof by strong induction (see Section 5.4).

Proof The proof is by induction. We prove by strong induction on n the statement that, for $n \geq 2$, the number n may be written as a product of primes.

Base case: 2 is a prime number and so a product of a single prime.

Inductive step: Suppose now as inductive hypothesis that, for some $k \geq 2$, if $2 \leq n \leq k$ then n may be written as a product of primes. Then if the number $k + 1$ is prime it is a product of a (single) prime. If the number $k + 1$ is not prime then it is composite in which case we can write $k + 1 = ab$ where $2 \leq a, b \leq k$. But then by inductive hypothesis a and b may be written as products of primes so that by combining these products we write $k + 1$ as a product of primes. Hence in both cases $k + 1$ is a product of primes as required to prove the inductive step.

Conclusion: Hence, by induction, n is a product of primes for all $n \geq 2$.

□

The key property of prime numbers is the following result which appears in Book Seven of the *Elements* of Euclid.

Theorem 23.1.3 *Suppose that p is a prime number and p divides ab for positive integers a and b . Then p divides a or p divides b .*

Constructing a proof. This is an example of a result where the conclusion is an ‘or’ statement. What is required can be summarized as follows.

Given	Goal
p a prime number p divides ab	p divides a or p divides b

Recall from Section 4.4 that we prove an ‘or’ statement by proving that if the first statement is false then the second must be true. This gives

the following strategy.

Given	Goal
p a prime number	
p divides ab	
p does not divide a	p divides b

This is easy to achieve once we recognize that, when p is prime, its only divisors are ± 1 and $\pm p$ and so these are the only candidates for common divisors of p and another integer a . So if we are told that p (and so $-p$) does not divide a the only common divisors are ± 1 and so the numbers are coprime. Theorem 17.3.2 now gives the result.

Proof Suppose that p divides ab . Now if p does not divide a then, since p is a prime number, p and a are coprime. It follows from Theorem 17.3.2 that p divides b . Thus either p divides a or p divides b as required. \square

This property of prime numbers is usually taken as the definition of a prime number in more advanced work. Notice that if an integer n greater than 1 is not prime then it does not satisfy this property. For there are then integers a and b such that $1 < a, b < n$ and $n = ab$. But now n divides ab but n does not divide a and n does not divide b . This shows that the property of prime numbers described in Theorem 23.1.3 characterizes prime numbers amongst the integers greater than 1.

23.2 The sieve of Eratosthenes

The problem of determining whether or not a positive integer is prime and the factorization of composite numbers into primes has always intrigued mathematicians. Recently methods of public-key cryptography† have been discovered which make use of the product of two large primes. It is relatively easy to find large prime numbers but if then they are multiplied together recovering the prime factors (which as we will see in the next section are unique) is an enormously time consuming task even with the help of a computer and is impractical using known techniques if the prime numbers are large enough. The codes are public in the sense that the knowledge of how to encode a message is made public. The coding technique uses remainders modulo a product of two large primes. To

† Accessible accounts of some of the basic ideas may be found in D.M. Davis, *The nature and power of mathematics*, Princeton University Press, 1993, and J.F. Humphreys and M.Y. Prest, *Numbers, groups and codes*, Cambridge University Press, 1989.

decode a message it is necessary to make use of the prime factors which are not made public. So anyone can encode a message but only someone knowing the prime numbers can decode it.

In this book we restrict attention to a basic and ancient method for listing primes named after Eratosthenes of Cyrene (ca. 276-ca. 194 B.C.) who was director of the library in Alexandria.

The most obvious approach to deciding whether a positive integer n is prime is to try all smaller positive integers one by one. If none (except 1) divides n then it must be prime. As soon as one does divide n then we know that n must be composite. This task is shortened once we realize that we do not have to try every integer less than n .

Proposition 23.2.1 If $n \geq 2$ is a composite number, then it has a prime factor not exceeding \sqrt{n} .

Proof Since n is composite we can write $n = ab$ where a and b are integers such that $1 < a, b < n$. If $a \leq \sqrt{n}$, then we choose a prime factor of a to obtain a prime factor of n which is less than or equal to \sqrt{n} . On the other hand, if $a > \sqrt{n}$, then $b = n/a < \sqrt{n}$ and so we can take a prime factor of b . \square

So to decide whether n is prime or composite it is sufficient to try all prime numbers not exceeding \sqrt{n} . We can organize this into a systematic method for finding all the prime numbers not exceeding some given number, an algorithm called the ‘Sieve of Eratosthenes’. The simplest way to explain the algorithm is to give an example.

Example 23.2.2 To find all prime numbers not exceeding 100.

First of all write out the sequence of integers from 2 to 100 as follows.

The first number in the list, the number 2, is necessarily prime but all multiples of 2 are necessarily composite so we cross them out.

The next of the remaining numbers is 3, which must also be prime. Again, all multiples of 3 are necessarily composite and so we cross out those which remain.

At each stage the next remaining number is necessarily prime since all multiples of lower primes have been crossed out. We then cross out all multiples of this number. So here we proceed to 5 and then 7.

Now, since there are no more primes not greater than $\sqrt{100} = 10$, the positive integers which remain must all be prime by Proposition 23.2.1 and so we have found all the primes less than 100, namely those integers not crossed out below.

2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99
								100

Thus the primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 and 97 (25 in all).

23.3 The fundamental theorem of arithmetic

We have shown (Proposition 23.1.2) that every positive integer greater than 1 is prime or a product of primes. In this section it is demonstrated that this factorization is essentially unique, a result known as the fundamental theorem of arithmetic. It is a curiosity of history that, although all the results about prime numbers proved so far are very ancient, the fundamental theorem is a relatively modern theorem and its first clear statement and proof only appeared in the nineteenth century in Gauss's *Disquisitiones arithmeticae*.

Theorem 23.3.1 (Fundamental theorem of arithmetic) *Every positive integer greater than 1 can be written uniquely as a product of prime*

numbers with the prime factors in the product written in non-decreasing order.

The point of the final part about the order of the factors is simply that in general the expression as a product of primes is clearly not unique because we can reorder the factors. For example we have $12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = 3 \times 2 \times 2$ giving three ways of writing 12 as a product of primes. However, these expressions are obtained simply by reordering the factors and we can uniquely specify an order by requiring the factors to be in non-decreasing order, in this case giving the first expression.

We can write the theorem more symbolically by saying that each integer $n > 1$ can be written uniquely in the form

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

where $r \geq 1$, $k_i \in \mathbb{Z}^+$ and each p_i is a prime number with $p_1 < p_2 < \dots < p_r$. We call this the *standard prime factorization* of n . If we allow $r = 0$ we can include the number 1 in this by adopting the convention that it is the product of no prime numbers.

We have already proved the existence of the prime factorization (Proposition 23.1.2) and so our task now is to prove uniqueness. To do this we generalize Theorem 23.1.3.

Proposition 23.3.2 *Suppose that p is a prime number and p divides a product of positive integers $a_1 a_2 \dots a_m$. Then p divides a_i for some i such that $1 \leq i \leq m$.*

Proof The proof is by induction on m .

Base case: For $m = 1$ this result says p divides $a_1 \Rightarrow p$ divides a_1 which is certainly true.

Inductive step: Suppose that, for some $k \geq 1$, the result is true for $m = k$. Then we can deduce it for $m = k + 1$ as follows.

$$\begin{aligned} p \text{ divides } a_1 a_2 \dots a_k a_{k+1} \\ \Rightarrow p \text{ divides } (a_1 a_2 \dots a_k) a_{k+1} \\ \Rightarrow p \text{ divides } a_1 a_2 \dots a_k \text{ or } p \text{ divides } a_{k+1} \quad (\text{by Theorem 23.1.3}) \\ \Rightarrow p \text{ divides } a_i \text{ for some } i \text{ such that } 1 \leq i \leq k \\ \quad (\text{by inductive hypothesis}) \text{ or } p \text{ divides } a_{k+1} \\ \Rightarrow p \text{ divides } a_i \text{ for some } i \text{ such that } 1 \leq i \leq k + 1. \end{aligned}$$

This proves the inductive step.

Conclusion: Hence the result is true for all positive integers m . \square

Proof of Theorem 23.3.1 We have already proved that factorization into primes is possible (Proposition 23.1.2). We prove uniqueness by contradiction. So suppose, for contradiction, that there is some integer $n > 1$ which has two different factorizations into primes:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

where the p_i s and the q_j s are all primes and $p_1 \leq p_2 \leq \dots \leq p_r$, $q_1 \leq q_2 \leq \dots \leq q_s$. We can now cancel any common primes from the two factorizations so that we get an equality as above with $p_i \neq q_j$ for all i and j . [Notice that not all the primes will cancel since we were supposing that the factorizations were different.] However, this contradicts Proposition 23.3.2 since clearly p_1 divides $p_1 p_2 \dots p_r$ and so p_1 divides $q_1 q_2 \dots q_s$ whereas p_1 does not divide any q_j since q_j is prime and different from p_1 . This contradiction shows that our original hypothesis is false and so we have proved the theorem. \square

23.4 Applications of the fundamental theorem of arithmetic

A direct application of the fundamental theorem of arithmetic is to find all the divisors of a number.

Proposition 23.4.1 Suppose that $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the standard prime factorization of a positive integer a . Then b is a divisor of a if and only if it can be written in the form $b = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}$ where $0 \leq l_i \leq k_i$ for $1 \leq i \leq r$.

Example 23.4.2 The standard prime factorization of 72 is $72 = 2^3 \times 3^2$. Hence the divisors of 72 are $2^{l_1} \times 3^{l_2}$ where $0 \leq l_1 \leq 3$ and $0 \leq l_2 \leq 2$. This gives $2^0 \times 3^0 = 1$, $2^1 \times 3^0 = 2$, $2^2 \times 3^0 = 4$, $2^3 \times 3^0 = 8$, $2^0 \times 3^1 = 3$, $2^1 \times 3^1 = 6$, $2^2 \times 3^1 = 12$, $2^3 \times 3^1 = 24$, $2^0 \times 3^2 = 9$, $2^1 \times 3^2 = 18$, $2^2 \times 3^2 = 36$ and $2^3 \times 3^2 = 72$.

Proof of Proposition 23.4.1 Recall that b is a divisor of a if and only if there is an integer q such that $a = bq$. Now the standard prime factorizations of b and q must combine to give the standard prime factorization of a , by the uniqueness part of the fundamental theorem. It is clear then that if $a = bq$ the standard prime factorization of b must be obtained from

the standard prime factorization of a by simply omitting some factors. Thus b has the given form.

Conversely if b has the given form then b divides a since we can take $q = p_1^{k_1-l_1} p_2^{k_2-l_2} \dots p_r^{k_r-l_r}$. \square

Corollary 23.4.3 *Given positive integers a and b suppose that $p_1 < p_2 < \dots < p_r$ are the primes occurring in the prime factorization of a or in the prime factorization of b so that $a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ and $b = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}$ where k_i and l_i are non-negative integers. Then the greatest common divisor of a and b is given by $p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ where m_i is the minimum of the two numbers k_i and l_i .*

Proof This is immediate from the proposition. \square

Example 23.4.4 Consider the greatest common divisor $(72, 30)$ (Example 11.3.3). The standard prime factorizations are $72 = 2^3 \times 3^2 = 2^3 \times 3^2 \times 5^0$, $30 = 2 \times 3 \times 5 = 2^1 \times 3^1 \times 5^1$. Hence the greatest common divisor is $2^1 \times 3^1 \times 5^0 = 6$.

It is important to realize that this is not a practical way of finding the greatest common divisor of two numbers of substantial size since factorization into primes is in general very time-consuming.

We can also use the fundamental theorem to give an alternative proof of the irrationality of $\sqrt{2}$.

Theorem 13.2.1 *There does not exist a rational number whose square is 2.*

Proof This proof is also by contradiction. Suppose for contradiction that there is a rational number $q \in \mathbb{Q}$ such that $q^2 = 2$. Since $q^2 = (-q)^2$ we may suppose that q is positive. Write $q = a/b$ where $a, b \in \mathbb{Z}^+$. Then $a^2 = 2b^2$. Let $2 < p_2 < \dots < p_r$ be the primes occurring as factors of a or of b . Then $a = 2^{k_1} p_2^{k_2} \dots p_r^{k_r}$ and $b = 2^{l_1} p_2^{l_2} \dots p_r^{l_r}$ where k_i and l_i are non-negative integers. This means that $a^2 = 2^{2k_1} p_2^{2k_2} \dots p_r^{2k_r}$ and $2b^2 = 2^{2l_1+1} p_2^{2l_2} \dots p_r^{2l_r}$. But by the fundamental theorem these expressions must be the same and so in particular $2k_1 = 2l_1 + 1$ which is impossible for integers k_1 and l_1 . This provides the necessary contradiction demonstrating that our hypothesis that there exists a rational square root of 2 is false and so proving the theorem. \square

23.5 The distribution of prime numbers

The sequence of primes is very irregular and it is extremely difficult to see any pattern in it. We can, however, prove that there are infinitely many primes. The following result is also from the *Elements* of Euclid (Book Nine) and is one of the great classic proofs by contradiction.

Theorem 23.5.1 *There are infinitely many prime numbers.*

Proof The proof is by contradiction. Suppose for contradiction that the set P of primes is finite, say of cardinality n . Then we can list the elements of P :

$$P = \{ p_1, p_2, \dots, p_n \}.$$

Now consider the positive integer $m = p_1 p_2 \dots p_n + 1$. This number is not divisible by p_i for $1 \leq i \leq n$ since the remainder is 1. But, by Proposition 23.1.2, m may be written as a product of primes and so is divisible by some prime p which must then not be an element of P . However, P was the set of all primes and so this is a contradiction showing that our assumption that the set of primes is finite must be false. Hence the set of primes must be infinite. \square

If we carry on with the Sieve of Eratosthenes we find that the number of primes gradually thins out. It is natural to ask whether it is possible to give a formula for the n th prime number or less ambitiously for an estimate for the number of primes at each stage. Mathematicians carried out enormous calculations by hand in the investigation of the distribution of prime numbers. Attempts were made to find simple expressions which took prime values; for example Leonhard Euler proved that $n^2 - n + 41$ is prime for $1 \leq n \leq 40$. Gauss investigated the distribution of the primes up to 3000000 and found 216745 of them! There are in fact 216817 but a few slips were inevitable in such an enormous hand calculation.

Definition 23.5.2 For $n \in \mathbb{Z}^+$ we write $\boxed{\pi(n)}$ for the number of primes not exceeding n .

Thus $\pi(2) = 1$, $\pi(10) = 4$, $\pi(100) = 25$ and calculation shows that $\pi(1000) = 168$, $\pi(10^6) = 78498$. One of the most remarkable theorems of the nineteenth century gives an estimate for $\pi(n)$ for large values of n .

Theorem 23.5.3 (Prime number theorem) *The ratio of $\pi(n)$ and $n/\log_e n$ approaches 1 as n grows without bound.*

Here $\log_e n$ is the natural logarithm of n which is the area under the graph of the function $x \mapsto 1/x$ between $x = 1$ and $x = n$.

The theorem says that $\pi(n)$ and $n/\log_e n$ are *asymptotic*. The precise statement requires the idea of a null sequence introduced in Definition 8.3.2: it is the statement that the sequence $n \mapsto (\pi(n) \log_e n)/n - 1$ is null. This means that $n/\log_e n$ gives a good estimate for $\pi(n)$ if n is large enough. To get some idea of how good an estimate consider the following table.[†]

n	$\pi(n)$	$n/\log_e n$	ratio
10^3	168	144.8	1.160
10^6	78498	72382.4	1.085
10^9	50847534	48254942.4	1.054
10^{12}	37607912018	36191206825.3	1.039

The first person to suggest publicly that a result along these lines was true was the French mathematician Adrien-Marie Legendre who suggested in 1798 that $\pi(n)$ is approximately equal to $n/(\log_e n - 1.08366)$ on the basis of extensive calculations. Gauss had already in 1793 reached the conclusion that $\pi(n)$ is asymptotic to $n/\log_e n$ according to unpublished work found amongst his papers. However, he found an even better approximation. As a result of his calculations he estimated that the number of primes in the interval from a to b is approximately $\int_a^b \frac{dx}{\log_e x}$. The agreement is striking: for example between 2600000 and 2700000 Gauss found 6762 primes whereas $\int_{2600000}^{2700000} \frac{dx}{\log_e x} = 6761.332$. He discusses this estimate in a letter he wrote in 1849.[‡]

The prime number theorem was finally proved in 1896 independently by the French mathematician Jacques Hadamard and by the Belgian mathematician C.J. de la Vallée-Poussin making use of ideas from ad-

[†] Extracted from Kenneth Rosen, *Elementary number theory and its applications*, Addison-Wesley, 1988. The values of $\pi(n)$ for large n are not found by the methods described in this book which involve testing all the numbers up to n but by evaluating some approximate formula for $\pi(n)$ to an accuracy of a half – which determines $\pi(n)$ since it is obviously an integer.

[‡] An account of Gauss's work on the distribution of primes including a translation of this letter is to be found in an article by L.J. Goldstein, A history of the prime number theorem, *American Mathematical Monthly*, volume 80, Mathematical Association of America, 1973 (pages 599–615).

vanced calculus.†. De la Vallée-Poussin showed in addition that $\pi(n)$ is more accurately represented by the ‘logarithmic integral’ $\text{li}(n) = \int_0^n \frac{dx}{\log_e x}$ (which can be given a well-defined value in spite of the fact that $\log_e 1 = 0$) than by any expression of the form $n/(\log_e n - A)$ where A is a constant, confirming conjectures suggested by Gauss’s calculations.

Before leaving this topic it is worth remarking on a remarkable theorem proved the British mathematician J.E. Littlewood in 1914. He showed that, although for all values of n for which it has been calculated $\text{li}(n) - \pi(n)$ is positive, this difference takes positive and negative values infinitely often as n runs through the positive integers. This is an example of a ‘pure existence’ result and the proof gave no indication at all how to find a value of n for which the difference is negative. In 1933, Littlewood’s student S. Skewes proved that there was a value of n for which the difference is negative before you reach $\exp \exp \exp \exp 79$ (using the exponential function $\exp(x) = e^x$ inverse to the natural logarithm \log_e). This reduces the search for n for which the difference is negative to a finite search – but illustrates how knowing that a task is finite may be no help at all in carrying it out. The number arising here is normally considered to be larger than any number which had previously arisen in a pure mathematical argument. Subsequent work by Skewes in 1955 marginally reduced the bound – to a number with about $10^{10^{100}}$ decimal places!

Exercises

23.1 Use the Sieve of Eratosthenes to find all the prime numbers less than 200.

23.2 Write 4148 and 7684 as products of prime numbers. Hence find $\gcd(4148, 7684)$.

23.3 Prove that there exists an integer n such that $n^2 - n + 41$ (Euler’s formula) is not prime.

23.4 Prove that for each positive integer n there is a sequence of n consecutive integers all of which are composite.

[Hint: Consider $(n+1)! + i$.]

† A beautiful argument motivating the prime number theorem and using only the basic ideas of the calculus may be found in R. Courant and H. Robbins, *What is mathematics?* Oxford University Press, 1941 (pages 482–486).

23.5 Euler's totient function $\phi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ is defined by putting $\phi(n)$ equal to the number of positive integers not exceeding n which are coprime to n . Prove that if p is prime then $\phi(p^k) = p^k - p^{k-1}$.

23.6 Use the method of proof of this chapter to prove that there does not exist a rational number q such that $q^3 = 2$.

23.7 Consider the set of positive integers of the form $4q + 1$. Notice that this set of numbers is closed under multiplication. Call an element n of this set a pseudo-prime when $n > 1$ and the only divisors of n in this set are 1 and n .

Prove that every $n > 1$ in the set can be written as a product of pseudo-primes but that this factorization is not always unique. So the analogue of the fundamental theorem of arithmetic is false in this set of numbers.

24

Congruence modulo a prime

In this final chapter we consider a number of results concerning expressions which are automatically divisible by some given prime number. The results given here have their origins in the seventeenth century but it is convenient to formulate and prove them using the idea of congruence.

Although the results may appear only to be of theoretical interest these ideas do in fact provide an important ingredient in the techniques of public-key cryptography using prime numbers referred to in the previous chapter. Furthermore the ideas introduced in this chapter led to the development of group theory, the study of symmetry, which is now an enormously rich subject with many applications both within mathematics and in many branches of science.

24.1 Fermat's little theorem

We first consider a striking result known as Fermat's 'little' theorem to distinguish it from his 'great' or 'last' theorem which was discussed in Chapter 18. As so often with Fermat's results it is not known how he proved the result although he mentioned that he had found a proof in a letter dated 18 October 1640. Euler was the first to publish a proof, in 1736, and a variant of this proof appears as Problems VI, Question 17. Apparently this proof also appears in an unpublished manuscript by Gottfried Leibniz some time before 1683.

In Chapter 21 we introduced operations of addition, subtraction and multiplication on the set \mathbb{Z}_m of congruence classes of the integers modulo m and observed that an element $[a]_m \in \mathbb{Z}_m$ has a (unique) multiplicative inverse $[a']_m$ (i.e. $[a]_m \times [a']_m = [1]_m$ or equivalently $aa' \equiv 1 \pmod{m}$) if

and only if a is coprime to m . For example, when $m = 10$ we saw that $[1]_{10}$, $[3]_{10}$, $[7]_{10}$ and $[9]_{10}$ are invertible in \mathbb{Z}_{10} .

In the case when the modulus is a prime number, say p , then every non-zero class in \mathbb{Z}_p is invertible because all numbers a such that $0 < a < p$ are coprime to p . This makes arithmetic modulo p , or in \mathbb{Z}_p , particularly simple. This fact can be used to prove some striking results in number theory and Fermat's little theorem is an example.

Theorem 24.1.1 (Fermat's little theorem) *If p is a prime number and a is a positive number which is not a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.*

Equivalently we can assert that $a^{p-1} - 1$ is divisible by p . The proof which follows was first given by the Scottish mathematician James Ivory in 1806.[†]

Proof We make use of the function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ used in the proof of Theorem 21.4.1. Since a is not a multiple of p , a and p are coprime. We define $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ by $f([x]_p) = [a]_p \times [x]_p = [ax]_p$. As in the proof of Theorem 21.4.1, since $(a, p) = 1$, this function is an injection so that, by the pigeonhole principle, it is a bijection.

Now $f[0]_p = [0]_p$ and so the $(p - 1)$ classes $[a]_p, [2a]_p, \dots, [(p - 1)a]_p$ are simply the classes $[1]_p, [2]_p, \dots, [p - 1]_p$ in a different order. Hence

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

This means that

$$a \times 2a \times \cdots \times (p - 1)a \equiv 1 \times 2 \times \cdots \times (p - 1) \pmod{p}$$

or

$$a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}.$$

But now, since p is prime, $(p - 1)!$ and p are coprime and so, by Proposition 19.3.2, we can divide through by $(p - 1)!$ to obtain $a^{p-1} \equiv 1 \pmod{p}$ as required. \square

Corollary 24.1.2 *If p is prime then, for all integers a , $a^p \equiv a \pmod{p}$.*

Proof There are two cases. If a is a multiple of p then so is a^p and so

[†] According to H. Davenport, *The higher arithmetic, an introduction to the theory of numbers*, Cambridge University Press, Sixth edition 1992.

$a^p \equiv 0 \equiv a \pmod{p}$. If a is not a multiple of p then it is immediate from the theorem that $a^p \equiv a \pmod{p}$. \square

This theorem can be used to determine the congruence class of a high power modulo a prime.

Example 24.1.3 To determine the congruence class of $3^{203} \pmod{11}$.

Solution By Fermat's little theorem $3^{10} \equiv 1 \pmod{11}$. Hence $3^{203} = (3^{10})^{20} \times 3^3 \equiv 1 \times 27 \equiv 5 \pmod{11}$. \square

It should be observed that Fermat's little theorem does not necessarily give the minimal positive power of a which is congruent to 1 modulo p and this may be less than $p - 1$. This is clear when $a = 1$. For a more interesting example consider $p = 7$. Here $2^3 \equiv 1 \pmod{7}$.

The smallest positive integer n such that $a^n \equiv 1 \pmod{p}$ is called the *order* of a modulo p . It is not difficult to deduce from Fermat's theorem that the order of any element divides $p - 1$ (see Problems VI, Question 14).

It is also true, but harder to prove, that for each prime p there is some number a with order $p - 1$ modulo p . Such a number is called a *primitive root* modulo p . The proof is another counting argument.[†]

24.2 Wilson's theorem

Another attractive result concerning divisibility by a prime p is the following.

Theorem 24.2.1 (Wilson's theorem) *If p is prime, then $(p - 1)! \equiv -1 \pmod{p}$.*

Equivalently, $(p - 1)! + 1$ is divisible by p . The theorem is named after the English mathematician John Wilson who conjectured it on the basis of numerical calculations. He was a student of Edward Waring who included it in his book *Meditationes algebraicae* in 1770 suggesting that it would be very hard to prove. The following year the French mathematician Joseph Lagrange published a proof.

Example 24.2.2 Consider the case of $p = 11$. Then $10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2$. We could determine the remainder after dividing

[†] See for example D.M. Burton, *Elementary number theory*, Allyn and Bacon, 1976.

by 11 by a direct calculation. However, notice the following congruences modulo 11:

$$10 \equiv -1;$$

$$9 \times 5 = 45 \equiv 1;$$

$$8 \times 7 = 56 \equiv 1;$$

$$6 \times 2 = 12 \equiv 1;$$

$$4 \times 3 = 12 \equiv 1.$$

Using these we see that $10! = 10 \times (9 \times 5) \times (8 \times 7) \times (6 \times 2) \times (4 \times 3) \equiv (-1) \times 1 \times 1 \times 1 \times 1 = -1$ as claimed.

In this calculation we paired off each number between 2 and 9 with its inverse modulo 11. This method works for any prime modulus and provides a general proof.

Proof of Theorem 24.2.1 For $p = 2$, $(p - 1)! = 1! = 1 \equiv -1 \pmod{2}$ and so the result is true.

Suppose now that p is prime and $p \geq 3$. Then each integer a such that $1 \leq a \leq p - 1$ is coprime to p (since p is prime) and so by Theorem 20.1.5 there is a unique integer $a' \in R_p$ such that $aa' \equiv 1 \pmod{p}$. Using the language of Definition 21.4.3, a' is an inverse of a modulo p .

If $a = 1$ or $a = p - 1$ then $a' = a$. For other values of a , $a' \neq a$. To see this observe that

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\Leftrightarrow x^2 - 1 \equiv 0 \pmod{p} \\ &\Leftrightarrow (x - 1)(x + 1) \equiv 0 \pmod{p} \\ &\Leftrightarrow p \text{ divides } (x - 1)(x + 1) \\ &\Leftrightarrow p \text{ divides } x - 1 \text{ or } p \text{ divides } x + 1 \\ &\quad \text{since } p \text{ is prime (using Theorem 23.1.3)} \\ &\Leftrightarrow x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p}. \end{aligned}$$

Thus the $p - 3$ integers $2, 3, \dots, p - 2$ may be divided into pairs a and a' such that $aa' \equiv 1 \pmod{p}$. This means that their product $2 \times 3 \times \dots \times (p - 2) \equiv 1 \pmod{p}$ and so $(p - 1)! \equiv p - 1 \equiv -1 \pmod{p}$ as required. \square

In fact Wilson's theorem provides a criterion for a number to be prime: an integer $n > 1$ is prime if and only if $(n - 1)! \equiv -1 \pmod{n}$ (see Exercise 24.4) but this is not a useful criterion since the calculation of $(n - 1)!$ is very time-consuming if n is large.

24.3 Looking for primes

Fermat's little theorem gives some indication of how it might be possible to prove that a number is prime without trying all possible factors or that it is composite without actually factorizing it. Notice that the theorem can be restated in the following way.

Corollary 24.3.1 *Given a positive integer n , if $a^n \not\equiv a \pmod{n}$ for some integer a , then n is not prime.*

Proof This is simply the contrapositive of Corollary 24.1.2. □

Example 24.3.2 For example, taking $n = 63$, $2^{63} = 2^{60} \times 2^3 = (2^6)^{10} \times 2^3 = (64)^{10} \times 8 \equiv 1^{10} \times 8 = 8 \pmod{63}$ and so $2^{63} \not\equiv 2 \pmod{63}$. Hence 63 is not prime.

It is of course easier to prove that 63 is composite by observing that $63 = 7 \times 9$ and this particular result is not an efficient way of proving that a number is composite. It does, however, point the way to seeking more efficient tests which show that numbers are composite.

It is natural to ask whether we can do something similar to prove that a number is prime. Is there some sort of converse to Corollary 24.3.1?

Apparently, at one time the Chinese believed that, if $2^n \equiv 2 \pmod{n}$, then n is prime, but in fact this is false as can be seen by the following.

Example 24.3.3 $2^{341} \equiv 2 \pmod{341}$ but $341 = 11 \times 31$ is not prime.

To see this observe that, by Fermat's theorem, $2^{10} \equiv 1 \pmod{11}$. Also $2^5 = 32 \equiv 1 \pmod{31}$ so that $2^{10} \equiv 1 \pmod{31}$. This means that $2^{10} - 1$ is divisible by 11 and by 31 and so these primes are amongst its prime factorization. Thus $2^{10} - 1$ is a multiple of $11 \times 31 = 341$, i.e. $2^{10} \equiv 1 \pmod{341}$. It follows that $2^{340} \equiv 1 \pmod{341}$ so that $2^{341} \equiv 2 \pmod{341}$.

This conjecture was perhaps a bit optimistic. More realistic might be to hope that, if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ which are coprime to n , then n is prime. In fact this fails too.

Example 24.3.4 We have $a^{560} \equiv 1 \pmod{561}$ for all integers a coprime to 561 but $561 = 3 \times 11 \times 17$ is not prime.

First of all notice that if a is coprime to 561, then $(a, 3) = 1$, $(a, 11) = 1$ and $(a, 17) = 1$. Then, by Fermat's theorem we have $a^2 \equiv 1 \pmod{3}$ so that $a^{560} \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ so that $a^{560} \equiv 1 \pmod{11}$ and

$a^{16} \equiv 1 \pmod{17}$ so that $a^{560} \equiv 1 \pmod{17}$. This means that $a^{560} - 1$ is divisible by 3, by 11 and by 17 and so, as in Example 24.3.3, it is divisible by $561 = 3 \times 11 \times 17$, i.e. $a^{560} \equiv 1 \pmod{561}$.

Nevertheless, these ideas can be developed to give tests for primality and this is an important area of active mathematical research.[†]

Exercises

- 24.1** Find the remainder after $2^{1000000}$ is divided by 17.
- 24.2** Suppose that p is an odd prime. Prove that $a^{2p-1} \equiv a \pmod{2p}$.
- 24.3** Use Fermat's theorem to find the inverse of 7 modulo 17 in R_{17} , the set of remainders modulo 17.
- 24.4** Prove that, for an integer $n > 2$, if $(n-1)! \equiv -1 \pmod{n}$ then n is prime.
- 24.5** Prove that, if p and q are distinct prime numbers, then

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

[†] See K.H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Second edition 1988.

Problems VI: Prime numbers

1. Find the prime factorizations of 3480 and 4284 and hence find their greatest common divisor. Compare the amount of work with the solution of Problems IV, Question 6(ii).
2. Prove that there are infinitely many prime numbers which are congruent to 3 modulo 4.
3. Let $E \subseteq \mathbb{Z}$ be the set of even integers. Call an even integer *E-prime* if it is not the product of two other even integers. Prove that 60 can be written as the product of *E-primes* in two quite distinct ways.
4. Re-prove Corollary 17.2.1 using the fundamental theorem of arithmetic.
5. Re-prove the result of Problems IV, Question 13 that $(a, b)[a, b] = ab$ for positive integers a and b using the fundamental theorem of arithmetic.
6. Find the number of positive divisors of the number $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ (where p_1, p_2, \dots, p_r are distinct primes).
7. Prove that if a and b are coprime, and a and c are coprime, then a and bc are coprime.
8. Prove that, if a and b are coprime, then ab is a perfect square if and only if a and b are both perfect squares.

9. Prove that, if m_1 and m_2 are coprime positive integers, then

$$a \equiv b \pmod{m_1 m_2} \Leftrightarrow a \equiv b \pmod{m_1} \text{ and } a \equiv b \pmod{m_2}.$$

10. Use the inclusion-exclusion principle (Problems III, Question 4) to deduce from Exercise 23.5 that if n has the standard prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

where ϕ is Euler's totient function.

11. Use the inclusion-exclusion principle to find the number of positive integers no greater than 100 which are perfect powers ($n = m^r$ for positive integers m and r with $r \geq 2$). Check the result of your calculation by listing these numbers. Do the same calculation for positive integers no greater than 1000.

12. Prove that if the polynomial equation $a_n x^n + \dots + a_1 x + a_0 = 0$ (with integer coefficients) has a rational solution $x = r/s$ (in its lowest terms) then r divides a_0 and s divides a_n .

Deduce that every rational solution of $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ is an integer.

Hence show that the equation $x^3 - 8x + a = 0$ has no rational solutions if $a \equiv \pm 1 \pmod{5}$.

13. Recall that, given a prime p , the order modulo p of an integer $a \not\equiv 0 \pmod{p}$ is the least positive integer n such that $a^n \equiv 1 \pmod{p}$. Find the orders modulo p of all the non-zero elements of R_p for $p = 5$ and $p = 11$.

14. Use Fermat's little theorem to prove, by contradiction, that for a prime p the order modulo p of each integer $a \not\equiv 0 \pmod{p}$ divides $p - 1$.

[Try a proof by contradiction using the division theorem.]

15. Suppose that p is prime and does not divide the integer a . Prove that in the infinite decimal representation of the rational number a/p the number of recurring digits is given by the order of 10 modulo p (and so by the previous question divides $p - 1$).

16. Find the remainders when

- (i) $29!$ is divided by 31 ,
- (ii) $18!$ is divided by 23 ,
- (iii) $18!$ is divided by 437 .

17. [Euler's proof of Fermat's little theorem.] Suppose that p is a prime number. Prove that, for $0 < i < p$, the binomial coefficient $\binom{p}{i}$ is a multiple of p .

[By Theorem 12.2.10 $p! = i!(p-i)!\binom{p}{i}$. Now use the fundamental theorem of arithmetic.]

Deduce that $(a+b)^p \equiv a^p + b^p \pmod{p}$. Hence prove, by induction on a , that $a^p \equiv a$ for all $a \in \mathbb{Z}$. Deduce Fermat's little theorem.

18. [Gauss's proof of Fermat's little theorem.] Let p be a prime and a a non-zero element of R_p .

(i) Prove that there exists a positive integer m such that $a^m \equiv 1 \pmod{p}$ (and so there is a least such, the order of a modulo p).

[Notice that the set $\{[a^k]_p \mid k \in \mathbb{Z}^+\}$ is a subset of \mathbb{Z}_p and so finite.]

(ii) Prove that an equivalence relation may be defined on $R_p - \{0\}$ by $x_1 \sim x_2 \Leftrightarrow x_1 \equiv x_2 a^k$ for some $k \in \mathbb{Z}^+$.

(iii) Prove that the number of elements in each equivalence class is n , the order of a .

(iv) Prove that n divides $p-1$ (proving the result of Question 14 without using Fermat's theorem).

(v) Deduce Fermat's theorem.

Solutions to exercises

The reader should not imagine that the solutions which follow are the only possible correct solutions of the exercises. Of course for some, such as completing the truth tables in Exercises 1, there is a unique ‘right answer’ and anything else is wrong. But most exercises ask for a proof and for these there may be more than one possible proof and in any case the same proof may be set out in a variety of ways. If the reader’s solution is different from the author’s then the reader should pause and check whether both solutions are correct.

Exercises 1 (page 8)

1.1	P	Q	P and Q
	T	T	T
	T	F	F
	F	T	F
	F	F	F

1.2 (i)	P	Q	P and Q	not (P and Q)
	T	T	T	F
	T	F	F	T
	F	T	F	T
	F	F	F	T

(ii)	P	Q	not P	not Q	(not P) or (not Q)
	T	T	F	F	F
	T	F	F	T	T
	F	T	T	F	T
	F	F	T	T	T

(iii) and (iv)		P	Q	not P	not Q	P and (not Q)	(not P) or Q
T	T	F	F			F	T
T	F	F	T			T	F
F	T	T	F			F	T
F	F	T	T			F	T

Notice that the final columns of the first two tables are the same. This tells us that the statements ‘not (P and Q)’ and ‘(not P) or (not Q)’ are logically equivalent, or have the same meaning.

1.3	a	b	$a < b$	$a = b$	$a \leq b$
	1	1	F	T	T
	2	1	F	F	F
	1	2	T	F	T
	-2	1	T	F	T

1.4 The easiest way of thinking about this question is to imagine filling in a table as follows.

good	1	2
neither	3	4
bad	5	6
	boys	girls

The idea is that each child will be placed in this table according to sex and mathematical ability (we assume that the assessment of ability does not present any problems). Thus in region 1 is the list of boys who are good at mathematics, in region 2 is the list of girls who are good at mathematics, region 2 together with region 4 provides the list of girls who are not bad at mathematics, and so on. We can now interpret each of the given statements as statements about this table.

- (i) Regions 4 and 6 are empty.
- (ii) Regions 2 and 4 are empty.
- (iii) Region 2 is empty.
- (iv) Region 6 is not empty.
- (v) Regions 4 and 6 are not both empty.
- (vi) Region 1 is empty.
- (vii) Regions 4 and 6 are empty.

From this we see that statement (v) is the negation of statement (i) whereas statement (vii) is logically equivalent to statement (i).

1.5 Recall that $|a|$ is defined by $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a \leq 0$. So we consider these two cases separately.

If $a \geq 0$, then $|a|^2 = a^2$ by definition.

If $a \leq 0$, then $|a|^2 = (-a)^2 = a^2$.

Since for every real number a , $a \geq 0$ or $a \leq 0$ we have proved that $|a|^2 = a^2$.

Notice that if $a = 0$ then $a \geq 0$ and $a \leq 0$. This is not a problem since in this case both definitions (a and $-a$) give 0. We say that the modulus of a real number is *well-defined* (see Example 8.1.8).

Exercises 2 (page 19)

2.1 (i) True. (ii) False. (iii) True. (iv) False. (v) False. (vi) True. (vii) True. (viii) True. (ix) False. (x) True. (xi) True.

Notice that statement (viii) is true because the statement ' $n = 2$ and $n = -1$ ' is false for all integers n .

[In fact there is a certain ambiguity about the last three parts of this question. Consider statement (ix). As explained in the text, the statement $n^2 - n - 2 = 0 \Rightarrow n = 2$ is strictly speaking a predicate giving a different proposition for each value of n . It is usual to interpret such a predicate as a universal statement meaning that the implication is true whatever value is assigned to the free variable n . This particular universal implication is false since, when $n = -1$, $n^2 - n - 2 = 0$ but $n \neq 2$. In the same way the universal implication $n^2 - n - 2 = 0 \Rightarrow n = -1$ is false. This leads to the conclusion that statement (ix) is false and this would be the normal interpretation.]

However the reader should be aware that statement (ix) can be viewed differently. The whole statement can be viewed as a predicate with free variable n and we can consider whether this predicate is true whatever integer value is assigned to n . This is indeed the case for, although the first implication is false when $n = -1$ and the second one is false when $n = 2$, one or other of them is true whatever value is assigned to n .

The precise meaning of more complicated universal statements such as this may be made clear by using the quantifier ' \forall ' to be discussed in Chapter 7: the symbols ' $\forall n$ ' are read 'for all n '. Statement (ix) is false if it is interpreted as

$$(\forall n, n^2 - n - 2 = 0 \Rightarrow n = 2) \text{ or } (\forall n, n^2 - n - 2 = 0 \Rightarrow n = -1).$$

It is true if it is interpreted as

$$\forall n, (n^2 - n - 2 = 0 \Rightarrow n = 2) \text{ or } (n^2 - n - 2 = 0 \Rightarrow n = -1).$$

Statements (x) and (xi) are true whichever way they are interpreted.]

2.2 Notice that if n is an integer then either $n \leq 0$ or $n \geq 1$.

	$n > 0$	$n \geq 1$	$n > 0 \Rightarrow n \geq 1$
$n \leq 0$	F	F	T
$n \geq 1$	T	T	T

Here the last column follows from the previous two using the truth table for ‘implies’. Since both entries in the last column are ‘T’ we have proved the universal implication $n > 0 \Rightarrow n \geq 1$ for integers n .

From the discussion in the chapter, the corresponding universal implication for a real number is false (see Table 2.1.2). This illustrates the importance of being clear about the range of values of the variables in a predicate.

2.3	P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
	T	T	T	T	T
	T	F	F	T	F
	F	T	T	F	F
	F	F	T	T	T

2.4	P	Q	$P \text{ or } Q$	$P \text{ and } Q$	$P \Rightarrow (P \text{ or } Q)$	$(P \text{ and } Q) \Rightarrow P$
	T	T	T	T	T	T
	T	F	T	F	T	T
	F	T	T	F	T	T
	F	F	F	F	T	T

Since all entries in the final two columns are ‘T’ these statements are true regardless of the truth values of the statements P and Q .

2.5 (i)	P	Q	$P \Rightarrow Q$	$\text{not } Q$	$\text{not } P$	$(\text{not } Q) \Rightarrow (\text{not } P)$
	T	T	T	F	F	T
	T	F	F	T	F	F
	F	T	T	F	T	T
	F	F	T	T	T	T

Since the entries in the third and sixth columns are identical the corresponding statements are logically equivalent: an implication is equivalent to its contrapositive.

(ii)	P	Q	$P \text{ or } Q$	$\text{not } P$	$(\text{not } P) \Rightarrow Q$
	T	T	T	F	T
	T	F	T	F	T
	F	T	T	T	T
	F	F	F	T	F

Since the entries in the third and-fifth columns are identical the corresponding statements are logically equivalent.

2.6 We must prove that there is no integer k such that $7k = 100$. For any integer k , $k \leq 14$ or $k \geq 15$. Hence $7k \leq 98$ or $7k \geq 105$ so that $7k \neq 100$.

Exercises 3 (page 29)

3.1 (i) We simplify each side by multiplying out.

$$\begin{aligned} (a+b-c)^2 &= a^2 + b^2 + c^2 + 2ab - 2ac - 2bc, \\ (a+b)^2 + (a-c)^2 + (b-c)^2 - a^2 - b^2 - c^2 &= a^2 + b^2 + c^2 + 2ab - 2ac - 2bc. \end{aligned}$$

Therefore $(a+b-c)^2 = (a+b)^2 + (a-c)^2 + (b-c)^2 - a^2 - b^2 - c^2$.

(ii) As with Proposition 3.2.1 we start with the goal and work backwards taking care to get the implications in the right direction.

$$\begin{aligned} bc + ac + ab \leq a^2 + b^2 + c^2 &\Leftarrow 0 \leq a^2 + b^2 + c^2 - bc - ac - ab \\ &\Leftarrow 0 \leq 2a^2 + 2b^2 + 2c^2 - 2bc - 2ac - 2ab \\ &\Leftarrow 0 \leq (b-c)^2 + (a-c)^2 + (a-b)^2 \\ &\Leftarrow 0 \leq (b-c)^2 \text{ and } 0 \leq (a-c)^2 \\ &\quad \text{and } 0 \leq (a-b)^2 \end{aligned}$$

and this final statement is certainly true for all real numbers a , b and c . Hence $bc + ac + ab \leq a^2 + b^2 + c^2$.

3.2 This is a case of spelling out the definitions. Suppose that a divides b and b divides c . Then $b = aq$ for some integer q and $c = bp$ for some integer p . [Notice that we cannot use the same letter q in both cases since there is no reason to expect that these two numbers will be equal.] Hence $c = bp = (aq)p = a(qp)$ so that a divides c since qp , the product of two integers, is an integer. Thus, if a divides b and b divides c then a divides c .

3.3 This can be proved directly from the definitions as follows.

Suppose that n is an even integer. Then $n = 2q$ for some integer q . Therefore $n^2 = (2q)^2 = 4q^2 = 2(2q^2)$ and so, since $2q^2$ is an integer, n^2 is even. Hence, if n is even then n^2 is even.†

Alternatively, this may be deduced from the previous result since, for any even integer a , 2 divides a and a divides a^2 .

3.4 Again from the definitions, if 0 divides a , then there is an integer q such that $a = 0 \times q$. Since $0 \times q = 0$ this means that $a = 0$.

Conversely, $0 = 0 \times 0$ and so 0 divides 0.

3.5 Remember that $b \geq c$ is shorthand for $b > c$ or $b = c$ so we must prove that $b > c \Rightarrow ab \geq ac$ and $b = c \Rightarrow ab \geq ac$. The first follows from the inequality axioms: $b > c \Rightarrow ab > ac$ (since $a > 0$) $\Rightarrow ab \geq ac$. The second is even easier: $b = c \Rightarrow ab = ac \Rightarrow ab \geq ac$.

[Notice here the methods for using and proving ‘or’ statements. To use an ‘or’ statement it is necessary to show that each component statement separately leads to the desired conclusion. To prove an ‘or’ statement it is sufficient to prove one of the component statements. Proofs of ‘or’ statements are considered further in the next chapter.]

3.6 Given negative real numbers a and b suppose that $a < b$. Then $a^2 > ab$ (multiplying through by $a < 0$) and $ab > b^2$ (multiplying through by $b < 0$). Hence $a^2 > b^2$. It follows that $a < b \Rightarrow a^2 > b^2$.

[This proof mimics the proof of Proposition 3.1.1. We could have deduced the result from Proposition 3.1.1 by observing that if a and b are negative then $-a$ and $-b$ are positive and that $a < b \Rightarrow -b < -a$. The reader should write out the details of this proof.]

3.7 The condition is not necessary. To prove that $4ab < (a+b)^2 \nRightarrow a < b$ it is sufficient to give a single example of numbers a and b for which the implication fails, say $a = 2$, $b = 1$ for which $4ab = 8 < (a+b)^2 = 9$ but $a \not< b$. On examining the proof of Proposition 3.2.1 we find that each implication is reversible apart from the last step. This means that $4ab < (a+b)^2 \Leftrightarrow a \neq b$ and so a necessary and sufficient condition is $a \neq b$.

† This proof is discussed in more detail in Chapter 7 (Proposition 7.3.2).

3.8 (i) Suppose that a and b are real numbers such that $0 \leq a < b$; then either $a = 0$ or $a > 0$. If $a > 0$ then we have already proved (Proposition 3.1.1) that $a^2 < b^2$. If $a = 0$ then $a^2 = 0$ and since $b > 0$ implies that $b^2 > 0$ we again have $a^2 < b^2$. So in either case $a^2 < b^2$. Hence $0 \leq a < b \Rightarrow a^2 < b^2$.

(ii) By definition the modulus of any real number is non-negative. Hence, if $|a| < |b|$ then $0 \leq |a| < |b|$ and so by the first part $|a|^2 < |b|^2$. But (by Exercise 1.5) $|a|^2 = a^2$ and $|b|^2 = b^2$ so that $a^2 < b^2$ as required.

(iii) $|a| = |b| \Rightarrow a^2 = |a|^2 = |b|^2 = b^2$ (using Exercise 1.5 again).

(iv) If $|a| \leq |b|$ then $|a| < |b|$ or $|a| = |b|$. In the first case $a^2 < b^2$ by (ii) and in the second case $a^2 = b^2$ by (iii) and so in either case $a^2 \leq b^2$. Thus $|a| \leq |b| \Rightarrow a^2 \leq b^2$ as required.

Exercises 4 (page 37)

4.1 Suppose for contradiction that m and n are integers such that $14m + 21n = 100$. Then 7 divides 14 and 7 divides 21 so that, since $100 = 7(2m + 3n)$, 7 divides 100. But 7 does not divide 100 [by Exercise 2.6 if a proof is insisted upon] and so we have a contradiction. Hence such integers m and n do not exist.

4.2 Given that n is an integer such that n^2 is odd, suppose for contradiction that n is even. Then, by Exercise 3.3, n^2 is even, contradicting the statement that n^2 is odd. Hence our assumption that n is even must be false, i.e. n is odd. Thus n^2 is odd $\Rightarrow n$ is odd, as required.

4.3 The contrapositive of the required result reads

$$n \text{ is even} \Rightarrow n^2 \text{ is even.}$$

This is true by Exercise 3.3 and so the required result is true.

4.4 Suppose that a is an integer such that $a^2 \geq 7a$. To see that it follows that $a \leq 0$ or $a \geq 7$ suppose that $a \not\leq 0$. Then $a > 0$ so that $a^2 \geq 7a \Rightarrow a \geq 7$ by dividing through by the positive number a . Hence $a^2 \geq 7a \Rightarrow a \leq 0$ or $a \geq 7$.

4.5 Suppose that a and b are real numbers such that $a \leq b$ and $b \leq a$. Suppose in addition, for contradiction, that $a \neq b$. Then, by the trichotomy law (Axioms 3.1.2(i)) $a < b$ or $a > b$. But $a < b$ contradicts

our hypothesis that $b \leq a$ and $a > b$ contradicts our hypothesis that $a \leq b$ and so in either case we have a contradiction as required. Thus our assumption that $a \neq b$ must be false and so $a = b$ as required.

4.6 The contrapositive of Exercise 3.8(iv) reads

$$a^2 > b^2 \Rightarrow |a| > |b|.$$

(i) Interchanging a and b this gives $a^2 < b^2 \Rightarrow |a| < |b|$ and so combining this with Exercise 3.8(ii) we have proved $|a| < |b| \Leftrightarrow a^2 < b^2$ as required.

(ii) We have already proved (Exercise 3.8(iii)) that $|a| = |b| \Rightarrow a^2 = b^2$. For the converse, suppose that $a^2 = b^2$ and, for contradiction, that $|a| \neq |b|$. Then, by trichotomy, either $|a| < |b|$ in which case $a^2 < b^2$ giving a contradiction, or $|a| > |b|$ in which case $a^2 > b^2$ giving a contradiction. Since we necessarily obtain a contradiction our assumption that $|a| \neq |b|$ must be false and so $|a| = |b|$ as required to prove that $a^2 = b^2 \Rightarrow |a| = |b|$.

4.7 Using the previous question, $|a + b| \leq |a| + |b| \Leftrightarrow (a + b)^2 \leq (|a| + |b|)^2 \Leftrightarrow a^2 + 2ab + b^2 \leq a^2 + 2|ab| + b^2 \Leftrightarrow ab \leq |ab|$ which is always true. From a similar argument with ' \leq ' replaced by '=' throughout, we see that equality holds if and only if $ab = |ab|$ and so if and only if $ab \geq 0$.

[This result is known as the ‘triangle inequality’ because when generalized to complex numbers it corresponds to the geometric fact that the sum of the lengths of any two sides of a triangle is not less than the length of the third side.]

Exercises 5 (page 51)

5.1 In this case $P(n)$ is the statement ‘3 divides $(n^3 - n)$ ’ or ‘ $n^3 - n = 3q$ for some integer q ’.

For the base case, the statement $P(1)$ simply says that 3 divides 0 which is certainly true since $0 = 3 \times 0$.

We can sum up what is needed for the inductive step as follows.

Given	Goal
k a positive integer 3 divides $k^3 - k$	3 divides $(k + 1)^3 - (k + 1)$

If we spell out what divisibility means this becomes the following.

Given	Goal
k a positive integer $k^3 - k = 3q$ for some integer q	$(k+1)^3 - (k+1) = 3p$ for some integer p

[Notice here that we should not use the letter q in both the given and the goal statements about divisibility by 3, since there is no reason to expect that they will be the same integer (in fact they can't be). So the letter p is used in the goal statement.]

This suggests that we let q be an integer such that $k^3 - k = 3q$ and try to find the p we want in terms of it. So we manipulate $(k+1)^3 - (k+1)$ in the hope that we can relate it to $k^3 - k$.

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

This shows that the number we require is given by $p = q + k^2 + k$.

We now write this out formally using the template of section 3.1.

Proof We use induction on n .

Base case: For $n = 1$, $n^3 - n = 1 - 1 = 0 = 3 \times 0$ and so 3 divides $n^3 - n$.

Inductive step: Suppose now as inductive hypothesis that 3 divides $k^3 - k$ for some positive integer k . Then $k^3 - k = 3q$ for some integer q . Hence $(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = (k^3 - k) + 3(k^2 + k) = 3(q + k^2 + k)$ and so 3 divides $(k+1)^3 - (k+1)$, as required.

Conclusion: Hence, by induction, n divides $n^3 - n$ for all positive integers n . \square

5.2 So far statements proved by induction have used the symbol ' n ' for the free variable in the predicate. This is the most common symbol for an integer free variable but other symbols can be used – this question uses the symbol ' m '.

The inductive step requires us to prove that, for $k \geq 10$,

$$k^3 \leq 2^k \Rightarrow (k+1)^3 \leq 2^{k+1}.$$

To prove this notice first of all that $k^3 \leq 2^k \Rightarrow 2k^3 \leq 2^{k+1}$ giving us one side of the desired inequality. The desired conclusion will follow if we can prove that $(k+1)^3 \leq 2k^3$.

Now starting from the other side we can expand: $(k+1)^3 = k^3 + 3k^2 + 3k + 1$. Hence

$$\begin{aligned}(k+1)^3 \leq 2^{k+1} &\Leftarrow k^3 + 3k^2 + 3k + 1 \leq 2k^3 \\ &\Leftrightarrow 3k^2 + 3k + 1 \leq k^3.\end{aligned}$$

But if $k \geq 10$, $3k^2 + 3k + 1 \leq 3k^2 + 3k^2 + k^2 = 7k^2 \leq k^3$.

Proof We use induction on m .

Base case: For $m = 10$, $m^3 = 1000$ and $2^m = 1024$ and so $m^3 \leq 2^m$.

Inductive step: Suppose as inductive hypothesis that $k^3 \leq 2^k$ for some $k \geq 10$. Then $(k+1)^3 = k^3 + 3k^2 + 3k + 1 \leq k^3 + 3k^2 + 3k^2 + k^2$ (since $k \geq 1$) = $k^3 + 7k^2 \leq k^3 + k^3$ (since $k \geq 7$) = $2k^3 \leq 2 \times 2^k$ (by inductive hypothesis) = 2^{k+1} and so the result holds for $m = k+1$ as required.

Hence, by induction, $m^3 \leq 2^m$ for all $m \geq 10$. \square

[We only needed $k \geq 7$ in proving the inductive step. Does this mean that the result holds for all $m \geq 7$? Why not?]

5.3 We use induction on n .

Base case: For $n = 1$, $n \geq 1$.

Inductive step: Suppose as inductive hypothesis that $k \geq 1$ for some positive integer k . Then since $k+1 \geq k$ it follows that $k+1 \geq 1$ proving the inductive step.

Hence by induction on n , $n \geq 1$ for all positive integers n .

[The reader may find this a curious exercise. However, although we have made use of this result in examples several times as if it were a 'self-evident truth' it was not included in the basic properties given earlier. It can be deduced from these basic properties, and this is how to do it.]

5.4 In this case the statement $P(n)$ to be proved for all integers $n \geq 0$ is $\sum_{i=0}^n x^i = (1 - x^{n+1})/(1 - x)$.

Thus $P(k)$ reads $\sum_{i=0}^k x^i = (1 - x^{k+1})/(1 - x)$, and $P(k+1)$ reads $\sum_{i=0}^{k+1} x^i = (1 - x^{(k+1)+1})/(1 - x)$ or, simplifying, $\sum_{i=0}^{k+1} x^i = (1 - x^{k+2})/(1 - x)$.

Proof We use induction on n .

Base case: For $n = 0$, $\sum_{i=0}^n x^i = x^0 = 1$ and $(1 - x^{n+1})/(1 - x) = (1 - x)/(1 - x) = 1$ and so the result holds.

Inductive step: Suppose now as inductive hypothesis that $\sum_{i=0}^k x^i = (1 - x^{k+1})/(1 - x)$ for some $k \geq 0$. Then $\sum_{i=0}^{k+1} x^i = \sum_{i=0}^k x^i + x^{k+1} =$

$(1-x^{k+1})/(1-x) + x^{k+1}$ (by inductive hypothesis) $= (1-x^{k+1}+x^{k+1}-x^{k+2})/(1-x) = (1-x^{k+2})/(1-x)$ as required.

Conclusion: Hence $\sum_{i=0}^n x^i = (1-x^{n+1})/(1-x)$ for all $n \geq 0$. \square

[This sum is known as a *geometric progression* with ratio x .]

5.5 We prove this result by induction on n .

Base case: For $n = 0$, $\sum_{i=0}^n (a+ib) = a$ and $\frac{1}{2}(n+1)(2a+nb) = \frac{1}{2} \times 2a = a$ and so the result holds.

Inductive step: Suppose as inductive hypothesis that $\sum_{i=0}^k (a+ib) = \frac{1}{2}(k+1)(2a+kb)$ for some $k \geq 0$. Then $\sum_{i=0}^{k+1} (a+ib) = \sum_{i=0}^k (a+ib) + (a+(k+1)b) = \frac{1}{2}(k+1)(2a+kb) + (a+kb+b) = \frac{1}{2}(2ka+k^2b+2a+kb+2a+2kb+2b) = \frac{1}{2}(2ka+k^2b+4a+3kb+2b) = \frac{1}{2}(k+2)(2a+kb+b) = \frac{1}{2}(k+2)(2a+(k+1)b)$ as required to prove the result for $n = k + 1$.

Conclusion: Hence the result holds for all $n \geq 0$.

Alternatively, this result can be deduced from Proposition 5.3.1 as follows.

$$\begin{aligned}\sum_{i=0}^n (a+ib) &= \sum_{i=1}^n a + b \sum_{i=1}^n i \\ &= (n+1)a + \frac{1}{2}n(n+1)b \\ &= \frac{1}{2}(n+1)(2a+bn).\end{aligned}$$

[This sum is known as an *arithmetic progression* with difference b .]

5.6 We can prove this by induction on n starting at $n = 0$. In this case $P(n)$ is simply the statement ' $u_n = n3^{n-1}$ '.

Base case: For $n = 0$ the formula gives $0 \times 3^{-1} = 0$ agreeing with the definition of u_0 .

Inductive step: Now suppose that $u_k = k3^{k-1}$ for some non-negative integer k . Then $u_{k+1} = 3u_k + 3^k$ (by definition of the sequence) $= 3k3^{k-1} + 3^k$ (by inductive hypothesis) $= k3^k + 3^k = (k+1)3^k$ as required to prove the formula for $n = k + 1$.

Conclusion: Hence, by induction, $u_n = n3^{n-1}$ for all non-negative integers n .

5.7 (i) The proof is by induction on n using the inductive definition of x^n in Definition 5.3.3.

Base case: For $n = 0$, $x^n y^n = 1 = (xy)^n$ as required.

Inductive step: Suppose as inductive hypothesis that $x^k y^k = (xy)^k$ for some non-negative integer k . Then, by the inductive steps in the definitions of x^n , y^n and $(xy)^n$, $x^{k+1} y^{k+1} = (x \cdot x^k)(y \cdot y^k) = (xy)(xy)^k = (xy)^{k+1}$ as required to prove the result for $n = k + 1$.

Conclusion: Hence, by induction, $x^n y^n = (xy)^n$ for any real numbers x and y and non-negative integers n .

(ii) Base case: For $n = 0$, $x^{m+n} = x^m = x^m x^0 = x^m x^n$ as required.

Inductive step: Suppose as inductive hypothesis that $x^{m+k} = x^m x^k$ for some non-negative integer k . Then $x^{m+k+1} = x x^{m+k}$ (by the inductive step in the definition) = $x x^m x^k$ (by inductive hypothesis) = $x^m x x^k = x^m x^{k+1}$ (by the inductive step in the definition) as required to prove the result for $n = k + 1$.

Conclusion: Hence, by induction on n , $x^{m+n} = x^m x^n$ for any real number x and non-negative integers m and n .

[Notice that in order for this identity to hold for $m = 1$ and $n = 0$ it is necessary to define $x^0 = 1$ for $x \neq 0$. The identity does not require any particular value for x^0 when $x = 0$.]

(iii) Base case: For $n = 0$, $(x^m)^n = 1 = x^0 = x^{mn}$ as required.

Inductive step: Suppose as inductive hypothesis that $(x^m)^k = x^{mk}$ for some non-negative integer k . Then $(x^m)^{k+1} = x^m (x^m)^k$ (by the inductive step in the definition of $(x^m)^n$) = $x^m x^{mk}$ (by inductive hypothesis) = x^{m+mk} (by part (ii) of the question) = $x^{m(k+1)}$ as required to prove the result for $n = k + 1$.

Conclusion: Hence, by induction on n , $(x^m)^n = x^{mn}$ for any real number x and non-negative integers m and n .

Exercises 6 (page 72)

6.1 (i) $0 \not< 0$ and so $0 \notin (0, 1)$.

$0 \leq 0 \leq 1$ and so $0 \in [0, 1]$.

$0 \leq 0 < 1$ and so $0 \in [0, 1)$.

$0 \not< 0$ and so $0 \notin (0, 1]$.

(ii) $[a, b] - (a, b) = \{a, b\}$.

(iii) Since $(a, b) = \emptyset$ is a non-existence statement it is hard to work with directly. So we prove this result by proving the equivalent contrapositive statement:

$$(a, b) \neq \emptyset \Leftrightarrow a < b.$$

\Rightarrow : Suppose that $(a, b) \neq \emptyset$. Then we may choose an element $x \in (a, b)$. This means that $a < x$ and $x < b$ which implies that $a < b$.

\Leftarrow : Suppose that $a < b$. Then $2a < a+b < 2b$ so that $a < (a+b)/2 < b$ which means that $(a+b)/2 \in (a, b)$ so that $(a, b) \neq \emptyset$.

The equivalent statements for the other intervals are:

$$[a, b] = \emptyset \Leftrightarrow a > b;$$

$$[a, b) = \emptyset \Leftrightarrow a \geq b;$$

$$(a, b] = \emptyset \Leftrightarrow a \geq b.$$

(iv) Suppose that $[a, b] \subseteq (c, d)$. Then since $a \in [a, b]$ we must have $a \in (c, d)$ and so in particular $c < a$. Similarly $b \in [a, b] \Rightarrow b \in (c, d) \Rightarrow b < d$.

Conversely, if $c < a$ and $b < d$ then $x \in [a, b] \Rightarrow a \leq x \leq b \Rightarrow c < x < d \Rightarrow x \in (c, d)$ and so $[a, b] \subseteq (c, d)$.

6.2 (i) For a real number a , $a \in \{x \in \mathbb{R} \mid x^2 + x - 2 = 0\} \Leftrightarrow a^2 + a - 2 = 0 \Leftrightarrow (a-1)(a+2) = 0 \Leftrightarrow a-1 = 0$ or $a+2 = 0 \Leftrightarrow a = 1$ or $a = -2 \Leftrightarrow a \in \{1, -2\}$.

Hence $\{x \in \mathbb{R} \mid x^2 + x - 2 = 0\} = \{1, -2\}$.

(ii) For $a \in \mathbb{R}$, $a \in \{x \in \mathbb{R} \mid x^2 + x - 2 < 0\} \Leftrightarrow a^2 + a - 2 < 0 \Leftrightarrow (a-1)(a+2) < 0 \Leftrightarrow (a-1 > 0 \text{ and } a+2 < 0) \text{ or } (a-1 < 0 \text{ and } a+2 > 0) \Leftrightarrow (a > 1 \text{ and } a < -2) \text{ or } (a < 1 \text{ and } a > -2) \Leftrightarrow a < 1 \text{ and } a > -2$ [Notice that there are no real numbers which are both less than -2 and greater than 1] $\Leftrightarrow a \in (-2, 1)$.

Hence $\{x \in \mathbb{R} \mid x^2 + x - 2 < 0\} = (-2, 1)$.

An alternative proof would be to construct a table as follows –

	$x - 1$	$x + 2$	$x^2 + x - 2 = (x-1)(x+2)$
$x < -2$	–	–	+
$x = -2$	–	0	0
$-2 < x < 1$	–	+	–
$x = 1$	0	+	0
$x > 1$	+	+	+

– from which it is immediate that $x^2 + x - 2 < 0 \Leftrightarrow -2 < x < 1$.

(iii) This is immediate from the above table or by trichotomy from parts (i) and (ii). Alternatively, a proof may be constructed by writing down a chain of equivalences as in parts (i) and (ii).

- 6.3** (i) $\{3\} = \{x \in \mathbb{Z} \mid x = 3\}$.
(ii) $\{1, 2, 3\} = \{x \in \mathbb{Z} \mid 0 < x < 4\}$.
(iii) $\{1, 3\} = \{x \in \mathbb{Z} \mid 0 < x < 4 \text{ and } x \text{ is odd}\}$.

6.4	$x \in A$	$x \in B$	$x \in C$	$x \in B \cup C$	$x \in A \cap (B \cup C)$
	T	T	T	T	T
	T	T	F	T	T
	T	F	T	T	T
	T	F	F	F	F
	F	T	T	T	F
	F	T	F	T	F
	F	F	T	T	F
	F	F	F	F	F

	$x \in A$	$x \in B$	$x \in C$	$x \in A \cap B$	$x \in A \cap C$	$x \in (A \cap B) \cup (A \cap C)$
	T	T	T	T	T	T
	T	T	F	T	F	T
	T	F	T	F	T	T
	T	F	F	F	F	F
	F	T	T	F	F	F
	F	T	F	F	F	F
	F	F	T	F	F	F
	F	F	F	F	F	F

Now since the final columns are the same we see that the two sets contain the same elements, i.e. are equal.

The Venn diagram for this result is shown on the next page; region i corresponds to line i in the above tables. We easily see that both sets correspond to regions 1, 2 and 3.

6.5 It is best to prove the implications ' \Rightarrow ' and ' \Leftarrow ' separately in each case.

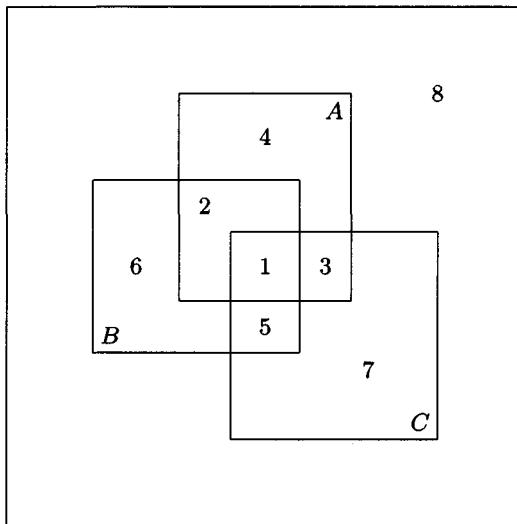
(i) ' $\RightarrowB \subseteq A \cup B$ since $x \in B \Rightarrow x \in A$ or $x \in B$. Conversely, given that $A \subseteq B$, $x \in A \Rightarrow x \in B$ so that $x \in A$ or $x \in B \Rightarrow x \in B$, i.e. $A \cup B \subseteq B$.

' \Leftarrow ' This follows immediately from $A \subseteq A \cup B$.

(ii) ' $\RightarrowA \cap B \subseteq A$ since $x \in A$ and $x \in B \Rightarrow x \in A$. Conversely, given that $A \subseteq B$, $x \in A \Rightarrow x \in B$ so that $x \in A \Rightarrow x \in A$ and $x \in B$, i.e. $A \subseteq A \cap B$.

' \Leftarrow ' This follows immediately from $A \cap B \subseteq B$.

Alternatively, this result follows from Problems I, Question 2.



6.6 Let us start by summarizing what is needed.

Given	Goal
$A \cap B \subseteq C$ $x \in B$	$x \notin A - C$

Since the goal is a negative statement this suggests a proof by contradiction as follows.

Given	Goal
$A \cap B \subseteq C$ $x \in B$ $x \in A - C$	contradiction

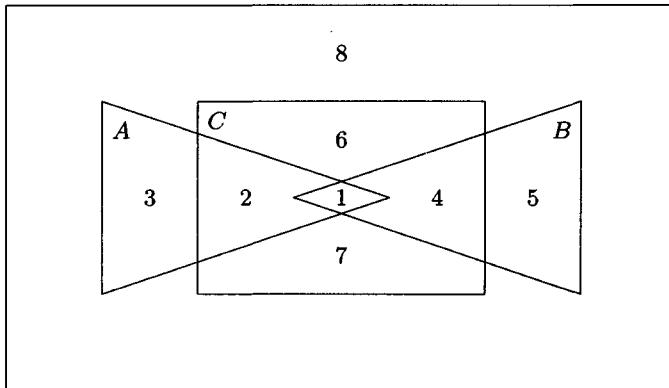
Now if we remember the definition of the difference of two sets this becomes the following.

Given	Goal
$A \cap B \subseteq C$ $x \in B$ $x \in A$ $x \notin C$	contradiction

Now the proof is apparent for $x \in B$ and $x \in A \Rightarrow x \in A \cap B \Rightarrow x \in C$ (using $A \cap B \subseteq C$) which contradicts $x \notin C$. This can be written out formally as follows.

Proof Suppose that $A \cap B \subseteq C$ and $x \in B$. Suppose for contradiction that $x \in A - C$. Then $x \in A$ and so, since also $x \in B$, we have $x \in A \cap B$ which implies that $x \in C$. But $x \in A - C$ implies that $x \notin C$ and so we have a contradiction. Hence our assumption must be false and $x \notin A - C$ as required. \square

A Venn diagram illustrating this result is given below.



In the diagram the set $A - C$ is given by region 3 which clearly contains no points of B (regions 1, 4 and 5).

Notice that although this seems the natural way of drawing this diagram two regions 6 and 7 together make up $C - (A \cup B)$ and there is no logical distinction between them. This is a case where the geometry of the diagram does not correspond to anything in the set theory. It indicates why proofs using Venn diagrams are not really entirely satisfactory and the best proof of this result is that given above.

6.7 Recall that $A \subseteq B$ is defined to mean

$$x \in A \Rightarrow x \in B. \quad (1)$$

Hence $B^c \subseteq A^c$ means

$$x \in B^c \Rightarrow x \in A^c$$

or equivalently

$$x \notin B \Rightarrow x \notin A. \quad (2)$$

The two statements (1) and (2) are contrapositives of each other and so equivalent. Hence $A \subseteq B \Leftrightarrow B^c \subseteq A^c$.

Exercises 7 (page 86)

7.1 (i) $\{m \in \mathbb{Z}^+ \mid \exists n \in \mathbb{Z}^+, m \leq n\} = \mathbb{Z}^+$: given $m \in \mathbb{Z}^+$ take $n = m$ to prove that $\exists n \in \mathbb{Z}^+, m \leq n$.

(ii) $\{m \in \mathbb{Z}^+ \mid \forall n \in \mathbb{Z}^+, m \leq n\} = \{1\}$: it is true that $\forall n \in \mathbb{Z}^+, 1 \leq n$ but for $m \neq 1$ a counterexample to $\forall n \in \mathbb{Z}^+, m \leq n$ is provided by $n = 1$ since $m \not\leq 1$;

(iii) $\{n \in \mathbb{Z}^+ \mid \exists m \in \mathbb{Z}^+, m \leq n\} = \mathbb{Z}^+$: given $n \in \mathbb{Z}^+$ take $m = n$ to prove that $\exists m \in \mathbb{Z}^+, m \leq n$.

(iv) $\{n \in \mathbb{Z}^+ \mid \forall m \in \mathbb{Z}^+, m \leq n\} = \emptyset$: given $n \in \mathbb{Z}^+$ a counterexample to $\forall m \in \mathbb{Z}^+, m \leq n$ is provided by $m = n + 1$ since $n + 1 \not\leq n$.

7.2 (i) False: a counterexample is $m = 2, n = 1$.

(ii) True: an example is $m = n = 1$.

(iii) True: see 7.1(i).

(iv) True: see 7.1(ii).

(v) True: see 7.1(iii).

(vi) False: see 7.1(iv).

7.3 (i) False: a counterexample is $m = 2, n = 1$.

(ii) True: an example is $m = n = 1$.

(iii) True: given $m \in \mathbb{Z}$ put $n = m$.

(iv) False: for each $m \in \mathbb{Z}$ a counterexample is given by $n = m - 1$.

(v) True: given $n \in \mathbb{Z}$ put $m = n$.

(vi) False: for each $n \in \mathbb{Z}$ a counterexample is given by $m = n + 1$.

7.4 (i) True: for each $x \in \mathbb{R}$, take $y = -x$.

(ii) False: for each $y \in \mathbb{R}$, the predicate is false for $x = 1 - y$.

(iii) True: take $y = 0$.

(iv) True: take $y = 0$.

(v) False: take $x = 0$.

(vi) False: take $x = 0$.

(vii) True: since ‘odd’ means ‘not even’.

(viii) False: ' $\forall n, n$ is even' is false, e.g. $n = 1$, and ' $\forall n, n$ is odd' is false, e.g. $n = 0$.

7.5 Suppose that $n \in \mathbb{Z}^+$ is such that $\exists q \in \mathbb{Z}^+, n = 2q + 1$. Then we can take $q \in \mathbb{Z}^+$ such that $n = 2q + 1$. This means that $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1$ and so $n^2 = 2p + 1$ where $p = 2q^2 + 2q$ so that $\exists p \in \mathbb{Z}^+, n^2 = 2p + 1$ as required.

[This proof illustrates how we *use* a statement involving \exists simply by using an element with the stated property and that we *prove* a statement involving \exists by constructing an element with the stated property.]

7.6 We can write the statement as follows.

$$\begin{aligned} \forall a, b \in \mathbb{Z}, [(\exists q_1 \in \mathbb{Z}, a = 2q_1) \text{ and } (\exists q_2 \in \mathbb{Z}, b = 2q_2)] \\ \Rightarrow \exists p \in \mathbb{Z}, a + b = 2p. \end{aligned}$$

Suppose that a and b are even. Then, by definition, $a = 2q_1$ and $b = 2q_2$ for integers q_1 and q_2 . Therefore $a + b = 2q_1 + 2q_2 = 2(q_1 + q_2)$ and so $a + b$ is even since $q_1 + q_2$ is an integer. Hence, if a and b are even then $a + b$ is even.

7.7 Suppose that $(x, y) \in (A \times B) \cup (C \times D)$. Then $(x, y) \in A \times B$ or $(x, y) \in C \times D$. We now examine these two cases in turn.

If $(x, y) \in A \times B$, then $x \in A$ and $y \in B$. Thus $x \in A \cup C$ and $y \in B \cup D$. Hence $(x, y) \in (A \cup C) \times (B \cup D)$ as required. On the other hand, if $(x, y) \in C \times D$ an almost identical argument demonstrates that $(x, y) \in (A \cup C) \times (B \cup D)$.

Thus $(x, y) \in (A \times B) \cup (C \times D) \Rightarrow (x, y) \in (A \cup C) \times (B \cup D)$ as required.

To give a counterexample to the equality of these sets we try a case of small sets just to see what happens – and it works.

Suppose that all four sets consist of just a single element: $A = \{a\}$, $B = \{b\}$, $C = \{c\}$ and $D = \{d\}$. Then $A \times B = \{(a, b)\}$ and $C \times D = \{(c, d)\}$ so that the left-hand side $(A \times B) \cup (C \times D) = \{(a, b), (c, d)\}$. However, $A \cup C = \{a, c\}$ and $B \cup D = \{b, d\}$ so that $(A \cup C) \times (B \cup D) = \{(a, b), (a, d), (c, b), (c, d)\}$. Thus $(A \cup C) \times (B \cup D)$ is not a subset of $(A \times B) \cup (C \times D)$ since it contains the element (a, d) .

7.8 (i) False. (ii) False. (iii) True. (iv) False.

7.9 Suppose that A is a subset of \mathbb{Z}^+ , the set of positive integers. Then $A = \mathbb{Z}^+$ if

- (i) $1 \in A$, and
- (ii) $\forall k \in \mathbb{Z}^+ ((1 \leq n \leq k \Rightarrow n \in A) \Rightarrow k + 1 \in A)$.

Exercises 8 (page 99)

8.1 Given $(x, y) \in \mathbb{R}^2$, by the trichotomy law precisely one of $x < y$, $x = y$ and $x > y$ is true. There is no ambiguity in the definition of $g(x, y)$ in the first and the last cases. If $x = y$ then $x \leq y$ and $x \geq y$ and so two definitions are given, y in the first case and x in the second; these values are the same since we are considering the case $x = y$. Hence g is well-defined.

If $x \geq y$, then $x - y \geq 0$ so that $|x - y| = x - y$. Thus, in this case, $f(x, y) = (x + y)/2 + (x - y)/2 = x = g(x, y)$. On the other hand, if $x \leq y$, then $x - y \leq 0$ so that $|x - y| = -(x - y) = y - x$. This implies that, in this case, $f(x, y) = (x + y)/2 + (y - x)/2 = y = g(x, y)$. Since, for each $(x, y) \in \mathbb{R}^2$, $x \geq y$ or $x \leq y$ this proves that $f = g$.

[Strictly speaking the values of the function f should be written $f((x, y))$ (and similarly for g) since the function is evaluated at the point $(x, y) \in \mathbb{R}^2$. It is usual to write the values simply as $f(x, y)$ and it is common to describe f as a function of two variables x and y .]

8.2 The four composite functions are given by

- (i) $f \circ f(x) = (x^3)^3 = x^9$,
- (ii) $f \circ g(x) = (1 - x)^3$,
- (iii) $g \circ f(x) = 1 - x^3$,
- (iv) $g \circ g(x) = 1 - (1 - x) = x$ so that $g \circ g = I_{\mathbb{R}}$, the identity function.

For the set, $fg(x) = gf(x) \Leftrightarrow (1 - x)^3 = 1 - x^3 \Leftrightarrow 1 - 3x + 3x^2 - x^3 = 1 - x^3 \Leftrightarrow x(x - 1) = 0 \Leftrightarrow x = 0$ or $x = 1$. Hence $\{x \in \mathbb{R} \mid fg(x) = gf(x)\} = \{0, 1\}$.

8.3 There are lots of possibilities here. The following functions are as required:

- (i) $f_1 = I_{\mathbb{R}}$, the identity function;

$$(ii) f_2(x) = \begin{cases} x^2 & \text{if } x \neq 0, \\ 1 & \text{if } x = 0; \end{cases}$$

another example is given by $f_2(x) = e^x$ (the exponential function);

$$(iii) f_3(x) = \begin{cases} x & \text{if } x \notin \mathbb{Z}, \\ x + 1/2 & \text{if } x \in \mathbb{Z}; \end{cases}$$

$$(iv) f_4(x) = n \in \mathbb{Z} \text{ if } n \leq x < n + 1.$$

8.4 Suppose that we are given $\varepsilon \in \mathbb{R}^+$. Then

$$1/n < \varepsilon \Leftrightarrow n > 1/\varepsilon$$

and so if we choose an integer $N > 1/\varepsilon$ we have $n \geq N \Rightarrow n > 1/\varepsilon \Rightarrow |1/n| = 1/n < \varepsilon$ as required to show that $1/n$ is null.

8.5 (i) This is the graph of the function whose values are given by the following table.

x	$f(x)$
a	z
b	y
c	z
d	x

(ii) This is not the graph of a function since no element is specified for the value at c .

(iii) This is not the graph of a function since two elements are specified for the value at b .

(iv) This is the graph of the function whose values are given by the following table.

x	$f(x)$
a	y
b	z
c	w
d	x

Exercises 9 (page 113)

9.1 (i) $y = f_1(x) \Leftrightarrow y = 2x + 5 \Leftrightarrow x = (y - 5)/2$. So f_1 is a bijection and the inverse is given by $f_1^{-1}(x) = (x - 5)/2$.

(ii) $y = f_2(x) \Leftrightarrow y = x^2 + 2x + 1 = (x + 1)^2$. So the function is not

injective (for example $f_2(-2) = f_2(0) = 1$) and it is not surjective (since $(x+1)^2 \geq 0$ for all real x).

(iii) $y = f_3(x) \Leftrightarrow y = x^2 - 2x = (x-1)^2 - 1$. So again this is not injective (for example $f_3(0) = f_3(2) = 0$) and is not surjective (since $(x-1)^2 - 1 \geq -1$ for all real x).

(iv) $y = 1/x \Leftrightarrow x = 1/y$ and $y = 0 \Leftrightarrow x = 0$ and so f_4 is a bijection which is its own inverse.

Sketching the graphs is quite a help in doing these questions.

9.2 (i) Notice that the inverse function is not defined for $x \leq 5$ since then $(x-5)/2 \notin \mathbb{R}^+$. So $f_1: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is an injection but not a surjection since, for example, 5 is not a value.

(ii) $y = f_2(x) = (x+1)^2 \Leftrightarrow x = -1 \pm \sqrt{y}$. Here $x \in \mathbb{R}^+ \Leftrightarrow 1 < \pm\sqrt{y}$ so we need $y > 1$ and must take the positive square root. Thus the function $\mathbb{R}^+ \rightarrow \mathbb{R}^+$ is not a surjection (for example 1 is not a value) but is an injection.

(iii) This example does not restrict to a function $\mathbb{R}^+ \rightarrow \mathbb{R}^+$ since, for example, $f_3(1) = -1$.

(iv) This is still a bijection which is its own inverse since $1/x > 0 \Leftrightarrow x > 0$.

9.3 (i) Suppose that $x, y \in \mathbb{R}$. Then

$$y = 3x + 2 \Leftrightarrow 3x = y - 2 \Leftrightarrow x = (y - 2)/3.$$

Hence $f_1^{-1}(x) = (x - 2)/3$.

(ii) Suppose that $x, y \in \mathbb{R}$. Then

$$y = x^3 + 1 \Leftrightarrow x^3 = y - 1 \Leftrightarrow x = \sqrt[3]{y - 1}.$$

Hence $f_2^{-1}(x) = \sqrt[3]{x - 1}$.

9.4 Suppose that $gf(x_1) = gf(x_2)$ for elements $x_1, x_2 \in X$. Since g is an injection, $f(x_1) = f(x_2)$. Since f is an injection $x_1 = x_2$ as required to prove that $g \circ f$ is an injection.

9.5 We can verify the conditions of Proposition 9.2.5 to prove that $g \circ f$ and $f^{-1} \circ g^{-1}$ are inverses of each other as follows.

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ f^{-1} \circ g^{-1} = g \circ I_Y \circ g^{-1} = g \circ g^{-1} = I_Z$$

and similarly $(f^{-1} \circ g^{-1}) \circ (g \circ f) = I_X$.

Thus $g \circ f$ is invertible (or equivalently a bijection) with inverse $f^{-1} \circ g^{-1}$.

[This result shows that composites of bijections are very easy to deal with. Notice the reversal of order when writing down the inverse.]

9.6 Suppose that f is a surjection. Then, given $y_0 \in Y$ there exists $x_0 \in X$ such that $f(x_0) = y_0$. But then $(x_0, y_0) \in X \times \{y_0\} \cap G_f$ and so $X \times \{y_0\} \cap G_f \neq \emptyset$.

Conversely, suppose that $\forall y \in Y, (X \times \{y\}) \cap G_f \neq \emptyset$. Then to show that f is a surjection we must show that, given $y_0 \in Y$, there exists an element $x_0 \in X$ such that $f(x_0) = y_0$. $(X \times \{y_0\}) \cap G_f \neq \emptyset$ so we can choose $(x_1, y_1) \in X \times \{y_0\} \cap G_f$. But then $(x_1, y_1) \in X \times \{y_0\}$ so that $x_1 \in X$ and $y_1 = y_0$. Also $(x_1, y_1) \in G_f$ and so $y_1 = f(x_1)$. It follows that $y_0 = f(x_1)$ and so we can take $x_0 = x_1$. Hence f is a surjection.

9.7 (i) Suppose that $B_1 \subseteq B_2$. Then $x \in \overleftarrow{f}(B_1) \Rightarrow f(x) \in B_1 \Rightarrow f(x) \in B_2 \Rightarrow x \in \overleftarrow{f}(B_2)$. Hence $\overleftarrow{f}(B_1) \subseteq \overleftarrow{f}(B_2)$.

(ii) The result follows from $x \in \overleftarrow{f}(B_1 \cap B_2) \Leftrightarrow f(x) \in B_1 \cap B_2 \Leftrightarrow f(x) \in B_1$ and $f(x) \in B_2 \Leftrightarrow x \in \overleftarrow{f}(B_1)$ and $x \in \overleftarrow{f}(B_2) \Leftrightarrow x \in \overleftarrow{f}(B_1) \cap \overleftarrow{f}(B_2)$.

(iii) The result follows from $x \in \overleftarrow{f}(B_1 \cup B_2) \Leftrightarrow f(x) \in B_1 \cup B_2 \Leftrightarrow f(x) \in B_1$ or $f(x) \in B_2 \Leftrightarrow x \in \overleftarrow{f}(B_1)$ or $x \in \overleftarrow{f}(B_2) \Leftrightarrow x \in \overleftarrow{f}(B_1) \cup \overleftarrow{f}(B_2)$.

When we consider the converse of (i) we realize that we have no control over elements of B_1 which are not values of the function. To give a very simple example consider the function $f: \{a\} \rightarrow \{a, b\}$ defined by $f(a) = a$. Take $B_1 = \{b\}$ and $B_2 = \{a\}$. Then $\overleftarrow{f}(B_1) = \emptyset \subseteq \overleftarrow{f}(B_2) = \{a\}$ whereas clearly $B_1 \not\subseteq B_2$. Thus $\overleftarrow{f}(B_1) \subseteq \overleftarrow{f}(B_2) \not\Rightarrow B_1 \subseteq B_2$.

[The implication does hold if f is a surjection and the reader should consider how to write out the proof of this.]

Exercises 10 (page 132)

10.1 Since X is finite of cardinality n there exists a bijection $f: \mathbb{N}_n \rightarrow X$.

Suppose that Y is also finite of cardinality n . Then there is a bijection

$g: \mathbb{N}_n \rightarrow Y$. Since a bijection is invertible we can now write down a bijection as required, $g \circ f^{-1}: X \rightarrow \mathbb{N}_n \rightarrow Y$.

Conversely, given a bijection $h: X \rightarrow Y$ we can deduce that $|Y|$ is finite of cardinality n by writing down the bijection $h \circ f: \mathbb{N}_n \rightarrow X \rightarrow Y$.

10.2 The statement $P(n)$ to be proved by induction is: ‘Given any collection X_1, X_2, \dots, X_n of pairwise disjoint finite sets, their union is finite and $|X_1 \cup X_2 \cup \dots \cup X_n| = |X_1| + |X_2| + \dots + |X_n|$.’

Base case: For $n = 1$ this just says $|X_1| = |X_1|$ which is clearly true.

Inductive step: Suppose that the result holds when n is some positive integer k . To deduce that the result holds for $n = k+1$, suppose that X_1, X_2, \dots, X_{k+1} is some collection of $k+1$ finite sets. Then, by inductive hypothesis the union of the first k of these sets is finite and

$$|X_1 \cup X_2 \cup \dots \cup X_k| = |X_1| + |X_2| + \dots + |X_k|.$$

Hence, by the addition theorem, $(X_1 \cup \dots \cup X_k) \cup X_{k+1}$ is a finite set and

$$\begin{aligned} |X_1 \cup X_2 \cup \dots \cup X_k \cup X_{k+1}| &= |X_1 \cup X_2 \cup \dots \cup X_k| + |X_{k+1}| \\ &= |X_1| + |X_2| + \dots + |X_k| + |X_{k+1}| \end{aligned}$$

so that the result holds for $n = k + 1$.

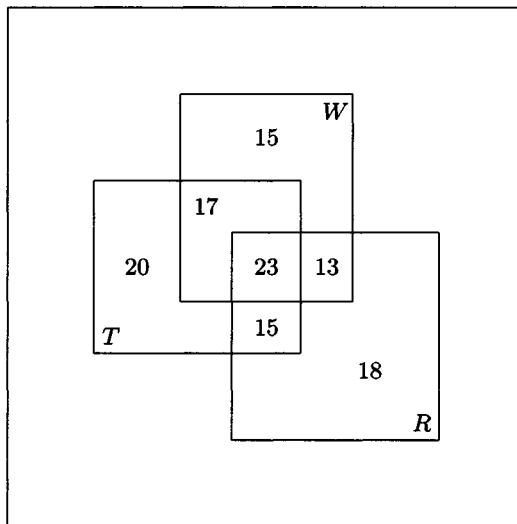
Hence by induction the result holds for all positive integers n .

10.3 The cardinality of $X \times Y$ is $3 \times 2 = 6$. An explicit bijection $f: \mathbb{N}_6 \rightarrow X \times Y$ is given by the following table.

i	1	2	3	4	5	6
$f(i)$	(a, d)	(a, e)	(b, d)	(b, e)	(c, d)	(c, e)

10.4 This sort of question is probably best answered using a Venn diagram. Let T denote the set of triangular tiles, R denote the set of red tiles and W denote the set of wooden tiles. Then we have the Venn diagram on the next page.

The total number in the whole square is 144 and we wish to know the number in the outer region representing $(W \cup R \cup T)^c$. There are eight disjoint regions and we can calculate the numbers in the other seven regions from the given data as follows. We are given that $|W \cap R \cap T| = 23$. Since we are given that $|W \cap R| = 36$ we see, from the addition theorem, that $|(W \cap R) - (W \cap R \cap T)| = 13$. Continuing in this way we can fill in the numbers as shown. Now we can calculate $|W \cup R \cup T| = 121$. So



again using the addition theorem we get $|W \cup R \cup T|^c = 144 - 121 = 23$. Hence there are 23 blue plastic square tiles.

Alternatively we can use the inclusion-exclusion principle (Proposition 10.3.2) without drawing a diagram. This gives

$$\begin{aligned}
 & |W \cup R \cup T| \\
 &= |W| + |R| + |T| - |W \cap R| - |W \cap T| - |R \cap T| + |W \cap R \cap T| \\
 &= 68 + 69 + 75 - 36 - 40 - 38 + 23 \\
 &= 121
 \end{aligned}$$

which gives the same result as before.

Exercises 11 (page 143)

11.1 The proof is by induction on n .

Base case: For $n = 1$, if $f: \mathbb{N}_1 \rightarrow X$ is a surjection then we must have $X = \{f(1)\}$ and so $|X| = 1$.

Inductive step: Suppose that for some $k \geq 1$ the result holds for $n = k$. To deduce the result for $n = k + 1$, suppose that $f: \mathbb{N}_{k+1} \rightarrow X$ is a surjection. There are two cases.

- (i) Suppose that $f|_{\mathbb{N}_k}: \mathbb{N}_k \rightarrow X$ is a surjection. Then, by inductive hypothesis, X is finite and $|X| \leq k$ so that certainly $|X| \leq k + 1$, as required for the inductive step.

(ii) Otherwise $f(k+1) \notin \vec{f}(\mathbb{N}_k)$ and so we may define a function $f_1: \mathbb{N}_k \rightarrow X - \{f(k+1)\}$ by $f_1(i) = f(i)$. This too is a surjection and so, by inductive hypothesis, $|X - \{f(k+1)\}| \leq k$. Hence, by the addition theorem, $|X| \leq k+1$, as required for the inductive step.

This completes the proof of the inductive step.

Hence, by induction, the result is true for all positive integers n .

11.2 Suppose that c_1 and c_2 are maximum elements of A , a set of real numbers. Then, since c_1 is a maximum and $c_2 \in A$, $c_1 \geq c_2$, and since c_2 is a maximum and $c_1 \in A$, $c_2 \geq c_1$. Hence $c_1 \leq c_2$ and $c_1 \geq c_1$ so that $c_1 = c_2$ as required.

11.3 Checking the possibilities gives:

$$\begin{aligned} D(88) &= \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 11, \pm 22, \pm 44, \pm 88\}; \\ D(136) &= \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 17, \pm 34, \pm 68, \pm 136\}. \end{aligned}$$

Hence $D(88) \cap D(136) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$ so that the greatest common divisor $(88, 136) = 8$.

11.4 Suppose that c is a common divisor of a/d and b/d . Then, since c divides a/d , $a/d = cq$ for some $q \in \mathbb{Z}$ so that $a = cdq$ and thus cd divides a . Similarly, since c divides b/d then cd divides b [fill in the details]. Hence cd is a common divisor of a and b and so $cd \leq d$ by the definition of d . But if $cd \leq d$ then $c \leq 1$ (since d is positive). Thus every common factor of a/d and b/d is less than or equal to 1 and so $(a/d, b/d) = 1$ as required.

11.5 By Corollary 11.1.5, $|X| \leq |Y|$. Thus the statements we are asked to prove are contrapositives. We prove the statements \Rightarrow and the implications in the other directions follow since they are the contrapositives.

(i) Clearly, if $X = Y$ then $|X| = |Y|$.

(ii) Suppose now that $X \subset Y$ (in other words X is a *proper* subset not containing every element of Y). Let $y_0 \in Y$ be an element such that $y_0 \notin X$. Then $X - \{y_0\}$ is a finite set (Corollary 11.1.5 again) and by the addition theorem $|X - \{y_0\}| = |X| - 1$. Hence by Corollary 11.1.5 $|Y| \leq |X| - 1$ and so $|Y| < |X|$.

11.6 Let A be a set of positive integers without a least element. We prove that $\mathbb{N}_n \subseteq \mathbb{Z}^+ - A$ for all n by induction.

Base case: If $1 \in A$ it would be the least element, which is impossible. Hence $1 \in \mathbb{Z}^+ - A$.

Inductive step: Suppose as inductive hypothesis that $\mathbb{N}_k \subseteq \mathbb{Z}^+ - A$ for some positive integer k . Then if $k + 1 \in A$ it would be the least element by inductive hypothesis, which is impossible. Hence $k + 1 \in \mathbb{Z}^+ - A$ and so, using the inductive hypothesis again, $\mathbb{N}_{k+1} \subseteq \mathbb{Z}^+ - A$, completing the inductive step.

Hence $\mathbb{N}_n \subseteq \mathbb{Z}^+ - A$ for all n so that in particular $n \notin A$ for all n , which means that A is the empty set.

This proves that if a set of positive integers does not have a least element then it is empty. The contrapositive of this statement is the well-ordering principle, which is therefore also proved.

Exercises 12 (page 155)

12.1 Continuing Pascal's triangle from the last line on page 151 we obtain the following.

	1	7	21	35	35	21	7	1
1	8	28	56	70	56	28	8	1
1	9	36	84	126	126	84	36	9
1	10	45	120	210	252	210	120	45

From this we can read off that $\binom{10}{3} = 120$ and by the binomial theorem this is the required coefficient.

12.2 By the binomial theorem the required coefficient is $\binom{100}{2}$ and the formula evaluates this as $100!/2!98! = (100 \times 99)/(2 \times 1) = 4950$.

12.3 (i) Let X be the set of three people and Y the pack of 52 cards. Then each group selection corresponds to an injection $X \rightarrow Y$. By Proposition 12.1.4 the number of possibilities is $(52)_3 = 52 \times 51 \times 50 = 132600$.

(ii) Each set of three cards is an element of $\mathcal{P}_3(Y)$. By Definition 12.2.4 the number of possibilities is $\binom{52}{3} = 52 \times 51 \times 50/3! = 22100$.

12.4 (i) Let X be the set of three people and Y the set of five dishes. Then each group selection corresponds to a function $X \rightarrow Y$ (since two or more may select the same dish). By Proposition 12.1.2 the number of possibilities is $5^3 = 125$.

(ii) Calculating the number of possible orders for the chef is complicated by the fact that two or more people may select the same dish so that we are not simply counting subsets of Y . The possibilities are as follows. If the three dishes are distinct then the possibilities are the elements of $\mathcal{P}_3(Y)$ and so the number is $\binom{5}{3} = 5!/3!2! = 10$. If only two distinct dishes are selected then one must be selected once and the other twice so that the possibilities correspond to injections $\mathbb{N}_2 \rightarrow Y$ and the number is $(5)_2 = 5 \times 4 = 20$. If all three people select the same dish then the number of possibilities is 5. So the total number of possibilities is $10 + 20 + 5 = 35$.

[This approach to the problem is rather cumbersome and would be difficult to apply if the numbers were a little larger – think about applying it to find the number of possible orders by five people selecting from a menu of eight items. A less direct approach gives a simpler calculation. Let $Y = \{y_1, y_2, y_3, y_4, y_5\}$. Then each order corresponds to a triple $(y_{i_1}, y_{i_2}, y_{i_3})$ where $i_1 \leq i_2 \leq i_3$. A bijection from this set of triples to $\mathcal{P}_3(\mathbb{N}_7)$ is given by $(y_{i_1}, y_{i_2}, y_{i_3}) \mapsto \{i_1, i_2 + 1, i_3 + 2\}$. Hence the number of orders is $\binom{7}{3} = 7!/3!4! = 35$. This argument can be used to show that the number of possible selections of k objects (repetitions permitted) from n objects is given by $\binom{n+k-1}{k}$. So, for example, if five people select from a menu of eight items the number is $\binom{12}{5} = 12!/5!7! = 792$.]

12.5 The coefficient of x^n in $(1+x)^{2n}$ is $\binom{2n}{n}$.

In the product $(1+x)^n(1+x)^n$ the terms contributing to x^{2n} have the form $\binom{n}{i}x^i \times \binom{n}{n-i}x^{n-i}$. Hence

$$\binom{2n}{n} = \sum_{i=0}^n \binom{n}{i} \binom{n}{n-i} = \sum_{i=1}^n \binom{n}{i}^2$$

as required.

12.6 Suppose that the n consecutive integers are $k+1, k+2, \dots, k+n$. The binomial coefficient $\binom{k+n}{n}$ is given by $(k+n)_n/n!$. Since this is an integer by definition, it follows that $n!$ divides

$$(k+n)_n = (k+n)(k+n-1)\dots(k+1),$$

the product of the given set of integers.

12.7 By the binomial theorem,

$$\begin{aligned}(1+i)^n &= \sum_{j=0}^n \binom{n}{j} i^j \\ &= \sum_{0 \leq 2r \leq n} \binom{n}{2r} (-1)^r + \sum_{0 \leq 2r+1 \leq n} \binom{n}{2r+1} (-1)^r i,\end{aligned}$$

separating out the real and imaginary parts and using $i^2 = -1$.

However, $1+i = \sqrt{2}e^{i\pi/4}$ and so $(1+i)^n = 2^{n/2} \exp(in\pi/4)$. The given result follows on equating the real parts of these two expressions for $(1+i)^n$ using the fact that

$$2^{n/2} \exp(in\pi/4) = \begin{cases} 2^{2k} \exp(ik\pi), & \text{if } n = 4k, \\ & = 4^k (-1)^k = (-4)^k, \\ 2^{(4k+1)/2} \exp(i(4k+1)\pi/4), & \text{if } n = 4k+1, \\ & = 2^{(4k+1)/2} (-1)^k 2^{-1/2} (1+i) \\ & = (-4)^k (1+i), \\ 2^{2k+1} \exp(i(2k+1)\pi/2), & \text{if } n = 4k+2, \\ & = 2^{2k+1} (-1)^k i, \\ 2^{(4k+3)/2} \exp(i(4k+3)\pi/4), & \text{if } n = 4k+3, \\ & = 2^{(4k+3)/2} (-1)^k 2^{-1/2} (-1+i) \\ & = 2^{-1} (-4)^{k+1} (1-i). \end{cases}$$

Similarly, by equating the imaginary parts we obtain

$$\sum_{0 \leq 2r+1 \leq n} (-1)^r \binom{n}{2r+1} = \begin{cases} 0 & \text{if } n = 4k, \\ (-4)^k & \text{if } n = 4k+1, \\ 2(-4)^k & \text{if } n = 4k+2, \\ 2(-4)^k & \text{if } n = 4k+3. \end{cases}$$

Exercises 13 (page 169)

13.1 Suppose for contradiction that there is rational number q such that $q^2 = 3$. Write q as a fraction in lowest terms: $q = a/b$ so that a and b are integers such that $(a, b) = 1$. Now $q^2 = 3 \Rightarrow a^2/b^2 = 3 \Rightarrow a^2 = 3b^2 \Rightarrow a^2$ is divisible by 3. It follows that a must be divisible by 3.

Thus we can write $a = 3a_1$ for some $a_1 \in \mathbb{Z}$. But then $a^2 = 3b^2 \Rightarrow 9a_1^2 = 3b^2 \Rightarrow 3a_1^2 = b^2 \Rightarrow b^2$ is divisible by 3 $\Rightarrow b$ is divisible by 3, as above. Hence 3 is a common factor of a and b so that $(a, b) \neq 1$, contradicting the choice of a and b and giving the required contradiction.

Hence there does not exist a rational number whose square is 3.

13.2 Calculation gives

$$\begin{aligned} 1^2 = 1 &\leqslant 3 \leqslant 2^2 = 4, \\ (1.7)^2 = 2.89 &\leqslant 3 \leqslant (1.8)^2 = 3.24, \\ (1.73)^2 = 2.9929 &\leqslant 3 \leqslant (1.74)^2 = 3.0276. \end{aligned}$$

Hence $\sqrt{3} = 1.73\dots$

13.3 The same argument for $\sqrt{4}$ leads to $q^2 = 4 \Rightarrow a^2/b^2 = 4 \Rightarrow a^2 = 4b^2 \Rightarrow a^2$ is divisible by 4. However, it does not now follow that a is divisible by 4, e.g. we can have $a = 2$. All we can prove is that 4 divides $a^2 \Rightarrow 2$ divides a but this does not lead to a contradiction since $a = 2a_1 \Rightarrow 4a_1^2 = 4b^2 \Rightarrow a_1^2 = b^2$.

Of course there *does* exist a rational number whose square is 4, namely $2=2/1$.

13.4 From the definition, $1/3 = 0.\overline{3}$

$$\begin{aligned} &\Leftrightarrow \underbrace{0.33\dots33}_n \leqslant 1/3 \leqslant \underbrace{0.33\dots34}_n \text{ for each } n \in \mathbb{Z}^+ \\ &\Leftrightarrow \underbrace{33\dots33}_n \leqslant (10)^n/3 \leqslant \underbrace{33\dots34}_n \text{ for each } n \in \mathbb{Z}^+ \\ &\Leftrightarrow \underbrace{99\dots99}_n \leqslant (10)^n \leqslant \underbrace{100\dots02}_n \\ &\Leftrightarrow (10)^n - 1 \leqslant (10)^n \leqslant (10)^n + 2 \end{aligned}$$

which is certainly true.

13.5 Let $x = 1.778\dot{2}34\dot{5}$. Then $10000x = 17782.345\dot{2}34\dot{5}$ from which it follows that $9999x = 17782.345 - 1.778 = 17780.567 = 17780567/1000$. It follows that $x = 17780567/9999000$.

Exercises 14 (page 181)

14.1 The result is trivial if A is empty since then $A \cup B = B$.

Suppose otherwise that $|X| = n \in \mathbb{Z}^+$. Then there is a bijection $f: \mathbb{N}_n \rightarrow A$. Since B is denumerable there is a bijection $g: \mathbb{Z}^+ \rightarrow B$. We can now count $A \cup B$ by first counting the finite set A and then counting B (we cannot do it the other way round or we would never get to A). This gives a function $h: \mathbb{Z}^+ \rightarrow A \cup B$ defined by

$$h(i) = \begin{cases} f(i) & \text{if } 1 \leqslant i \leqslant n, \\ g(i-n) & \text{if } i \geqslant n+1. \end{cases}$$

This function is a surjection since f and g are surjections. For it to be an injection we need $A \cap B = \emptyset$ for otherwise any common elements will be counted twice. But so long as $A \cap B = \emptyset$ then it is an injection since f and g are. Thus h is a bijection as required to prove $A \cup B$ denumerable.

If A and B are not disjoint, replace A in the above argument by the finite set $A - B$.

[This argument should be compared with Theorem 10.2.1 and Proposition 10.3.1.]

14.2 In the same way as in the previous result we may assume that A and B are disjoint by replacing A by $A - B$. By Proposition 14.2.5, $A - B$ is either finite (in which case we can quote the previous result) or denumerable.

To count two disjoint denumerable sets we cannot count one and then the other since we will never get to the elements in the second. We overcome this by alternating between the sets as we count. Let $f: \mathbb{Z}^+ \rightarrow X$ and $g: \mathbb{Z}^+ \rightarrow Y$ be bijections. Then we can define a bijection $h: \mathbb{Z}^+ \rightarrow X \cup Y$ by

$$h(i) = \begin{cases} f(k) & \text{if } i = 2k - 1, \\ g(k) & \text{if } i = 2k. \end{cases}$$

Suppose that X is uncountable and $A \subseteq X$ is denumerable. Suppose for contradiction that $X - A$ is countable, i.e. finite or denumerable. Then, by what has just been proved, $X = A \cup (X - A)$ is denumerable, contradicting the uncountability of X . Hence $X - A$ is uncountable as required.

14.3 Using induction we can deduce from the previous result that any finite union of denumerable sets is denumerable. However, this method will not deal with a denumerable set of sets. To see how to do this, use the fact that A_n is denumerable to list the elements:

$$A_n = \{a_{1n}, a_{2n}, \dots, a_{mn}, \dots\}.$$

We can now display all the elements in the union of the sets in a double array as shown at the top of the next page. This looks very similar to the array in the proof of Proposition 14.2.3 and so we can use the same

diagonal method of counting as indicated.

\vdots	\vdots				
a_{14}	\vdots				
a_{13}	a_{23}	\dots			
a_{12}	a_{22}	a_{32}	\dots		
a_{11}	a_{21}	a_{31}	a_{41}	\dots	
\vdots	\vdots				
10	\vdots				
6	9	\dots			
3	5	8	\dots		
1	2	4	7	\dots	

This gives the bijection $\bigcup A_n \rightarrow \mathbb{Z}^+$:

$$a_{mn} \mapsto \frac{1}{2}(m+n-2)(m+n-1) + n.$$

[The condition that the sets are disjoint is not necessary for this result. The reader might like to consider how to deduce the general case from the special case of disjoint sets.]

14.4 Suppose that X and Y are two sets such that $|X| \leq |Y|$ and $|Y| \leq |X|$. We prove that $|X| = |Y|$ by contraction. Suppose, for contradiction, that $|X| \neq |Y|$. Then, since $|X| \leq |Y|$, we have $|X| < |Y|$ and, since $|Y| \leq |X|$, we have $|Y| < |X|$. But, by definition, if $|X| < |Y|$ there exists an injection $X \rightarrow Y$ and, by the Cantor–Schröder–Bernstein theorem, if $|Y| < |X|$, there does not exist an injection $X \rightarrow Y$. Thus we have obtained a contradiction so that our assumption that $|X| \neq |Y|$ is false. Hence $|X| = |Y|$ as required.

[The statement proved in this exercise is the more usual statement of the Cantor–Schröder–Bernstein theorem.]

Exercises 15 (page 197)

- 15.1** (i) $100 = 3 \times 33 + 1 \Rightarrow q = 33, r = 1$.
- (ii) $3 = 100 \times 0 + 3$.
- (iii) $100 = 7 \times 14 + 2$.

- (iv) $-100 = 7 \times (-15) + 5.$
- (v) $-105 = 7 \times (-15) + 0.$
- (vi) $-3 = 105 \times (-1) + 102.$
- (vii) $7684 = 4148 \times 1 + 3536.$
- (viii) $-7684 = 4148 \times (-2) + 612.$
- (ix) $1234567 = 1357 \times 909 + 1054.$
- (x) $0 = 17 \times 0 + 0.$

15.2 First of all notice that, if a is divisible by 5, then $a = 5q$ and so $a^2 = 25q^2 = 5(5q^2)$ is divisible by 5.

For the converse suppose that a^2 is divisible by 5 and, for contradiction, that a is not divisible by 5. Then, by the division theorem, $a = 5q + 1$, $a = 5q + 2$, $a = 5q + 3$ or $a = 5q + 4$. However,

$$\begin{aligned} a = 5q + 1 &\Rightarrow a^2 = (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1, \\ a = 5q + 2 &\Rightarrow a^2 = 5(5q^2 + 4q) + 4, \\ a = 5q + 3 &\Rightarrow a^2 = 5(5q + 6q + 1) + 4, \\ a = 5q + 4 &\Rightarrow a^2 = 5(5q + 8q + 3) = 1. \end{aligned}$$

Hence in each case the remainder is non-zero and so, by the division theorem, a^2 is not divisible by 5, giving the required contradiction. Hence, if a^2 is divisible by 5 then so is a as required.

15.3 First of all notice that if a^2 is divisible by 9 then it is certainly divisible by 3. For the converse, if a^2 is divisible by 3 then, by Proposition 15.2.1, a is divisible by 3, i.e. $a = 3q$ and so $a^2 = 9q^2$ is divisible by 9.

15.4 $98765432 = 3 \times 32921810 + 2$ has remainder 2 after division by 3 and so by Proposition 15.2.3 it is not a perfect square.

15.5 Suppose that n is a perfect square, say $n = a^2$ for some integer a . Then a is either even or odd, i.e. $a = 2q_0$ or $a = 2q_0 + 1$ for some integer q . Hence $a^2 = 4q_0^2$ or $a^2 = 4q_0^2 + 4q_0 + 1 = 4(q_0^2 + q_0) + 1$ so that $n = 4q$ (where $q = q_0^2$) or $n = 4q + 1$ (where $q = q_0^2 + q_0$) as required.

However, $1234567 = 4 \times 308641 + 3$ has remainder 3 after division by 4 and so is not a perfect square.

15.6 To find the first decimal place a_1 observe that $50 = 7 \times 7 + 1$ so that $7/10 < 5/7 < 8/10$ and $a_1 = 7$. Continuing in this way we obtain the following.

$$\begin{aligned} 50 &= 7 \times 7 + 1 \Rightarrow a_1 = 7 \\ 10 &= 7 \times 1 + 3 \Rightarrow a_2 = 1 \\ 30 &= 7 \times 4 + 2 \Rightarrow a_3 = 4 \\ 20 &= 7 \times 2 + 6 \Rightarrow a_4 = 2 \\ 60 &= 7 \times 8 + 4 \Rightarrow a_5 = 8 \\ 40 &= 7 \times 5 + 5 \Rightarrow a_6 = 5 \\ 50 &= 7 \times 7 + 1 \end{aligned}$$

At this point the calculation goes back to the beginning and so the decimal places begin to recur giving $5/7 = 0.\dot{7}1428\dot{5}$.

Exercises 16 (page 206)

16.1 Applying the Euclidean algorithm gives the following sequence of remainders.

$$\begin{array}{rcl} 7684 & & \\ 4148 & (-1) & \\ 3536 & (-1) & \\ 612 & (-5) & \\ 476 & (-1) & \\ 136 & (-3) & \\ 68 & (-2) & \\ 0 & & \end{array}$$

Thus $(7684, 4148) = 68$.

16.2 Applying the Euclidean algorithm gives the following sequence of remainders.

$$\begin{array}{rcl} 11033442 & & \\ 1102246 & (-10) & \\ 10982 & (-100) & \\ 4046 & (-2) & \\ 2890 & (-1) & \\ 1156 & (-2) & \\ 578 & (-2) & \\ 0 & & \end{array}$$

Thus $(11033442, 1102246) = 578$.

16.3 In the examples we have done we have always put $a > b$, writing down the larger number first. If we change the order of the numbers so that $a_0 = b < a_1 = a$ then the first step of the Euclidean algorithm will read

$$a_0 = a_1 \times 0 + a_0$$

and so (using the notation of Theorem 16.2.1) $a_2 = r_1 = a_0$. Since we now have $a_1 = a$, $a_2 = b$, the remaining steps of the algorithm are identical to the steps which arise from writing down the larger number first.

So the order of the numbers does not really matter. If the smaller number is written down first then the first step simply switches the order so that there is this one extra step.

16.4 Suppose that $c \in D(b, r)$. Then, since c divides b , $b = cq_1$ for some integer q_1 , and, since c divides r , $r = cq_2$. It follows that $a = bq + r = c(q_1q + q_2)$ so that c divides a and $c \in D(a, b)$. Thus $D(b, r) \subseteq D(a, b)$.

Exercises 17 (see page 215)

17.1 Extending the table of Solution 16.1 to keep track of the linear combinations we obtain the following.

$$\begin{array}{rcl} 7684 & = & 7684 \times 1 \quad + 4148 \times 0 \\ 4148 & = & 7684 \times 0 \quad + 4148 \times 1 \quad (-1) \\ 3536 & = & 7684 \times 1 \quad + 4148 \times (-1) \quad (-1) \\ 612 & = & 7684 \times (-1) + 4148 \times 2 \quad (-5) \\ 476 & = & 7684 \times 6 \quad + 4148 \times (-11) \quad (-1) \\ 136 & = & 7684 \times (-7) + 4148 \times 13 \quad (-3) \\ 68 & = & 7684 \times 27 \quad + 4148 \times (-50) \quad (-2) \\ 0 & & \end{array}$$

From this we see that $68 = 7684 \times 27 + 4148 \times (-50)$ and checking this does give $207468 - 207400 = 68$.

Hence one possible solution is $m = 27$, $n = -50$.

17.2 From the previous solution one possible solution is $m = 27$, $n = 50$.

17.3 Extending the table of Solution 16.2 we obtain the following.

$$\begin{array}{rcl}
 11033442 & = & 11033442 \times 1 & + 1102246 \times 0 \\
 1102246 & = & 11033442 \times 0 & + 1102246 \times 1 & (-10) \\
 10982 & = & 11033442 \times 1 & + 1102246 \times (-10) & (-100) \\
 4046 & = & 11033442 \times (-100) & + 1102246 \times 1001 & (-2) \\
 2890 & = & 11033442 \times 201 & + 1102246 \times (-2012) & (-1) \\
 1156 & = & 11033442 \times (-301) & + 1102246 \times 3013 & (-2) \\
 578 & = & 11033442 \times 803 & + 1102246 \times (-8038) & (-2) \\
 0 & & & &
 \end{array}$$

Hence $11033442 \times 803 + 1102246 \times (-8038) = 578$ and so one possible solution is $m = 803$, $n = -8038$.

[It is not so easy to check this solution on a calculator since rather large numbers arise!]

17.4 As in the proof of Lemma 16.1.2 we prove this result by proving that the set of common divisors of a , b and c is equal to the set of common divisors of $\gcd(a, b)$ and c . We can prove this as follows:

$$\begin{aligned}
 d &\text{ is a common divisor of } a, b \text{ and } c \\
 \Leftrightarrow d &\text{ divides } a, b \text{ and } c \\
 \Leftrightarrow d &\text{ divides } \gcd(a, b) \text{ and } c \text{ (using Corollary 17.2.1).}
 \end{aligned}$$

Now, since the two sets of common divisors are equal they must have the same greatest element as required.

From this and Exercise 16.2 we obtain $\gcd(11033442, 1102246, 6035) = \gcd(578, 6035)$. The Euclidean algorithm applied to these two integers gives the following sequence of remainders.

$$\begin{array}{rcl}
 6035 & & \\
 578 & (-10) & \\
 255 & (-2) & \\
 68 & (-3) & \\
 51 & (-1) & \\
 17 & (-3) & \\
 0 & &
 \end{array}$$

Hence $\gcd(11033442, 1102246, 6035) = \gcd(578, 6035) = 17$.

17.5 Extending the table in the previous solution to keep track of the linear combinations we obtain the following.

$$\begin{array}{rcl}
 6035 & = & 578 \times 0 + 6035 \times 1 \\
 578 & = & 578 \times 1 + 6035 \times 0 & (-10) \\
 255 & = & 578 \times (-10) + 6035 \times 1 & (-2) \\
 68 & = & 578 \times 21 + 6035 \times (-2) & (-3) \\
 51 & = & 578 \times (-73) + 6035 \times 7 & (-1) \\
 17 & = & 578 \times 94 + 6035 \times (-9) & (-3) \\
 0 & &
 \end{array}$$

Hence

$$\begin{aligned}
 17 &= 578 \times 94 + 6035 \times (-9) \\
 &= (11033442 \times 803 + 1102246 \times (-8038)) \times 94 + 6035 \times (-9) \\
 &\quad (\text{using the result of Exercise 17.3}) \\
 &= 11033442 \times 75482 + 1102246 \times (-755572) + 6035 \times (-9).
 \end{aligned}$$

Hence one solution is $m = 75482$, $n = -755572$, $p = -9$.

17.6 If $a_1 b_2 = a_2 b_1$ then a_2 divides $a_1 b_2$. But then, if a_2 and b_2 are coprime, a_2 divides a_1 and so in particular $a_2 \leq a_1$. But by symmetry the same argument can be used to prove that $a_1 \leq a_2$ so that $a_1 = a_2$. It follows from $a_1 b_2 = a_2 b_1$ that $b_1 = b_2$.

Notice that this result proves that the fraction in lowest terms representing a rational number (see Definition 13.1.3) is unique since $a_1 b_2 = a_2 b_1 \Leftrightarrow a_1/b_1 = a_2/b_2$.

Exercises 18 (page 224)

18.1 From Exercise 16.1, $(7684, 4148) = 68$. Now since $272 = 68 \times 4$ we see that 68 divides 272 so that the diophantine equations does have solutions.

From Exercise 17.1, $7684 \times 27 + 4148 \times (-50) = 68$. Multiplying through by 4 we see that one solution to the equation is given by $m = 27 \times 4 = 108$, $n = (-50) \times 4 = -200$.

Thus, for $m, n \in \mathbb{Z}$,

$$\begin{aligned}
 7684m + 4148n &= 272 \\
 \Leftrightarrow 7684m + 4148n &= 7684 \times 108 + 4148 \times (-200) \\
 \Leftrightarrow 7684(m - 108) + 4148(n + 200) &= 0
 \end{aligned}$$

$$\begin{aligned}
 &\Leftrightarrow 113(m - 108) + 61(n + 200) = 0 \\
 &\quad \text{dividing through by } \gcd(7684, 4148) = 68 \\
 &\Leftrightarrow (m - 108, n + 200) = (61q, -113q) \text{ for some } q \in \mathbb{Z} \\
 &\quad \text{since 61 and 113 are coprime} \\
 &\Leftrightarrow (m, n) = (108 + 61q, -200 - 113q) \text{ for some } q \in \mathbb{Z}.
 \end{aligned}$$

Thus the solutions to the diophantine equation are given by

$$(m, n) = (108 + 61q, -200 - 113q) \text{ for } q \in \mathbb{Z}.$$

18.2 Notice that $7684m - 4148n = 272 \Leftrightarrow 7684m + 4148(-n) = 272$. So the solutions are given by

$$(m, n) = (108 + 61q, 200 + 113q) \text{ for } q \in \mathbb{Z}.$$

18.3 Applying the Euclidean algorithm to the integers 516 and 564 gives the following sequence of remainders expressed as integer linear combinations of 516 and 564.

$$\begin{array}{rcl}
 564 & = & 516 \times 0 + 564 \times 1 \\
 516 & = & 516 \times 1 + 564 \times 0 & (-1) \\
 48 & = & 516 \times (-1) + 564 \times 1 & (-10) \\
 36 & = & 516 \times 11 + 564 \times (-10) & (-1) \\
 12 & = & 516 \times (-12) + 564 \times 11 & (-3) \\
 0 & &
 \end{array}$$

Since 12 divides 6432 there are solutions. Since $6432/12 = 536$ a solution is given by $m = -12 \times 536 = -6432$ and $n = 11 \times 536 = 5896$. Thus, to find the general solution,

$$\begin{aligned}
 &516m + 564n = 6432 \\
 &\Leftrightarrow 516m + 564n = 516 \times (-6432) + 564 \times 5896 \\
 &\Leftrightarrow 516(m + 6432) + 564(n - 5896) = 0 \\
 &\Leftrightarrow 43(m + 6432) + 47(n - 5896) = 0 \\
 &\quad \text{dividing through by } \gcd(516, 564) = 12 \\
 &\Leftrightarrow (m + 6432, n - 5896) = (47q, -43q) \text{ for some } q \in \mathbb{Z} \\
 &\quad \text{since 43 and 47 are coprime} \\
 &\Leftrightarrow (m, n) = (-6432 + 47q, 5896 - 43q) \text{ for some } q \in \mathbb{Z}.
 \end{aligned}$$

To find positive solutions notice that $m > 0 \Leftrightarrow -6432 + 47q > 0 \Leftrightarrow 47q > 6432 \Leftrightarrow q > 6432/47 = 136 + 40/47 \Leftrightarrow q \geq 137$. Similarly,

$n > 0 \Leftrightarrow 5896 - 43q > 0 \Leftrightarrow 43q < 5896 \Leftrightarrow q < 5896/43 = 137 + 5/43 \Leftrightarrow q \leq 137$. Thus the only solution with m and n both positive arises from $q = 137$. This gives the unique positive solution $(m, n) = (7, 5)$.

[If we are only seeking positive solutions to this particular problem then it is quicker to try the possibilities since necessarily $n < 6432/564$, i.e. $n \leq 11$. We simply try each positive integer less than 12 in turn to see whether $6432 - 564n$ is divisible by 516.]

Exercises 19 (page 239)

19.1 From 1998 to 2045 there are 12 leap years. Hence the day number of 6 September 2045 is $366 \times 12 + 365 \times 35 + 31 \times 5 + 30 \times 2 + 28 \times 1 + 6$. Working modulo 7 in order to obtain the remainder modulo 7 gives $2 \times 5 + 1 \times 0 + 3 \times 5 + 2 \times 2 + 0 \times 1 + 6 = 10 + 15 + 4 + 6 \equiv 3 + 1 + 4 + 6 = 14 \equiv 0$. Hence the day of the week is the same as 7 January 1998, namely Wednesday.

[In the Gregorian calendar which is at present the internationally accepted calendar, year n is a leap year when n is divisible by 4 but not by 100, or n is divisible by 400. Thus 2000 will be a leap year but 1900 was not.]

19.2 $a_1 \equiv a_2$ and $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 - a_2 = mq_1$ and $b_1 - b_2 = mq_2$ (for some integers q_1 and q_2) $\Rightarrow (a_1 - b_1) - (a_2 - b_2) = (a_1 - a_2) - (b_1 - b_2) = mq_1 - mq_2 = m(q_1 - q_2) \Rightarrow a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$.

19.3 If $n = a_k a_{k-1} \dots a_2 a_1 a_0$ in decimal notation, then

$$\begin{aligned} n &= a_k \times 10^k + a_{k-1} \times 10^{k-1} + \dots + a_2 \times 10^2 + a_1 \times 10 + a_0 \\ &\equiv a_k + a_{k-1} + \dots + a_2 + a_1 + a_0 \pmod{3} \end{aligned}$$

since $10 \equiv 1 \pmod{3}$ so that $10^i \equiv 1$ for positive integers i . Since an integer m is divisible by 3 if and only if $m \equiv 0 \pmod{3}$ we see that n is divisible by 3 if and only if $a_k + a_{k-1} + \dots + a_2 + a_1 + a_0$ is divisible by 3.

† For a discussion of different calendars and a formula for the day of the week of any date see K.H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Second edition 1988.

19.4 (i) $6x \equiv 24 \pmod{45} \Leftrightarrow 2x \equiv 8 \pmod{15} \Leftrightarrow x \equiv 4 \pmod{15}$ since $(2, 15) = 1$.

Hence $6x \equiv 24 \pmod{45} \Leftrightarrow x \equiv 4 \pmod{15}$, i.e. $6x \equiv 24 \pmod{45} \Leftrightarrow x \equiv 4, 19$ or $34 \pmod{45}$.

We can describe the solution set as $\{4 + 15q \mid q \in \mathbb{Z}\}$.

(ii) $10x \equiv 15 \pmod{45} \Leftrightarrow 2x \equiv 3 \pmod{9} \Leftrightarrow 2x \equiv 12 \pmod{9} \Leftrightarrow x \equiv 6 \pmod{9}$ since $(2, 9) = 1$.

Hence $10x \equiv 15 \pmod{45} \Leftrightarrow x \equiv 6 \pmod{9}$, i.e. $10x \equiv 15 \pmod{45} \Leftrightarrow x \equiv 6, 15, 24, 33$ or $42 \pmod{45}$.

We can describe the solution set as $\{6 + 9q \mid q \in \mathbb{Z}\}$.

19.5 $ab_1 \equiv ab_2 \pmod{m} \Leftrightarrow \frac{a}{(a, m)}b_1 \equiv \frac{a}{(a, m)}b_2 \pmod{\frac{m}{(a, m)}}$ by Proposition 19.3.1 $\Leftrightarrow b_1 \equiv b_2 \pmod{\frac{m}{(a, m)}}$ by Proposition 19.3.2, since $a/(a, m)$ and $m/(a, m)$ are coprime (by Exercise 11.4).

Exercises 20 (page 249)

20.1 (i) Since $(3, 11) = 1$ there is a unique solution modulo 11. Either try the integers 0 to 10 in turn or say $3x \equiv 5 \equiv -6 \pmod{11} \Leftrightarrow x \equiv -2 \equiv 9 \pmod{11}$ to see that the solutions are given by $x \equiv 9 \pmod{11}$.

(ii) Since $(10, 35) = 5$ which does not divide 16 there are no solutions.

(iii) Since $(10, 35) = 5$ divides 5 there are solutions. To find them: $10x \equiv 5 \pmod{35} \Leftrightarrow 2x \equiv 1 \equiv 8 \pmod{7} \Leftrightarrow x \equiv 4 \pmod{7}$.

(iv) Since $(10, 21) = 1$ there is a unique solution modulo 21. Trying the integers from 0 to 20 in turn we find that the solution is $x \equiv 16 \pmod{21}$.

Alternatively, we can say something like $10x \equiv 13 \pmod{21} \Leftrightarrow 10x \equiv 13 + 147 = 160 \pmod{21} \Leftrightarrow x \equiv 16 \pmod{21}$.

20.2 (i) Applying the Euclidean algorithm to 341 and 912 and writing each remainder as a multiple of 341 modulo 912 gives the equations at the top of the next page.

Thus 341 and 912 are coprime so that the congruence has a unique solution modulo 912. Since $341 \times (-115) \equiv 1 \pmod{912}$, the unique solution is given by $x \equiv -115 \times 15 = -1725 \equiv 99 \pmod{912}$.

Hence $341x \equiv 15 \pmod{912} \Leftrightarrow x \equiv 99 \pmod{912}$.

$$\begin{array}{rcl}
 912 & \equiv & 341 \times 0 \\
 341 & \equiv & 341 \times 1 & (-2) \\
 230 & \equiv & 341 \times (-2) & (-1) \\
 111 & \equiv & 341 \times 3 & (-2) \\
 8 & \equiv & 341 \times (-8) & (-13) \\
 7 & \equiv & 341 \times 107 & (-1) \\
 1 & \equiv & 341 \times (-115) & (-7) \\
 0
 \end{array}$$

(ii) Applying the Euclidean algorithm to 341 and 913 gives the following sequence of remainders.

$$\begin{array}{rcl}
 913 \\
 341 & & (-2) \\
 231 & & (-1) \\
 110 & & (-2) \\
 11 & & (-10) \\
 0
 \end{array}$$

Hence $\gcd(341, 913) = 11$ and so the congruence $341x \equiv 15 \pmod{913}$ has no solutions since 15 is not divisible by 11.

(iii) Applying the Euclidean algorithm to 345 and 912 and writing each remainder as a multiple of 345 modulo 912 gives the following.

$$\begin{array}{rcl}
 912 & \equiv & 345 \times 0 \\
 345 & \equiv & 345 \times 1 & (-2) \\
 222 & \equiv & 345 \times (-2) & (-1) \\
 123 & \equiv & 345 \times 3 & (-1) \\
 99 & \equiv & 345 \times (-5) & (-1) \\
 24 & \equiv & 345 \times 8 & (-4) \\
 3 & \equiv & 345 \times (-37) & (-8) \\
 0
 \end{array}$$

Hence $\gcd(345, 912) = 3$ which divides 15 so that solutions to the linear congruence exist. Since $15/3 = 5$ one solution is given by $x \equiv -37 \times 5 = -185 \pmod{912}$.

To find all the solutions observe that

$$\begin{aligned}
 345x \equiv 15 \pmod{912} &\Leftrightarrow 345x \equiv 345 \times (-185) \pmod{912} \\
 &\Leftrightarrow 115x \equiv 115 \times (-185) \pmod{304} \\
 &\Leftrightarrow x \equiv -185 \equiv 119 \pmod{304},
 \end{aligned}$$

since 115 and 304 are coprime (because we have divided through by the greatest common divisor).

Thus $345x \equiv 15 \pmod{912} \Leftrightarrow x \equiv 119 \pmod{304}$ or, if it is desired to write the solution modulo 912, $345x \equiv 15 \pmod{912} \Leftrightarrow x \equiv 119, 423$ or $727 \pmod{912}$.

20.3 When $a \equiv 0 \pmod{m}$ the linear congruence becomes simply $0 \equiv b \pmod{m}$ and so has nothing to do with x . It will be satisfied (for all values of x) when b is a multiple of m and will not be satisfied (for any value of x) when b is not a multiple of m .

This is precisely what Theorem 20.1.7 reduces to in this case. For if $a = 0$ then $\gcd(a, m) = m$ so that there is a solution if and only if m divides b . In this case there are m different solutions modulo m which means that everything is a solution.

[At first glance Theorem 20.1.7 makes no sense at all when $a = 0$ but after careful consideration we see that it does make sense but tells us something rather obvious. This phenomenon is quite common. If we have obtained some general result then it can be worth while thinking what it means in particularly simple cases. If it doesn't work in such cases then this can indicate that something has been missed in the general situation.]

Exercises 21 (page 261)

21.1 Suppose that $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$. Then $a_1 \equiv a_2$ and $b_1 \equiv b_2 \pmod{m}$ so that $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ and $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$ (by Proposition 19.1.3). Hence $[a_1 + b_1]_m = [a_2 + b_2]_m$ and $[a_1 - b_1]_m = [a_2 - b_2]_m$ so that addition and subtraction in \mathbb{Z}_m are well-defined.

21.2 These results are immediate since by definition (Definition 19.2.3) $r_m(c) \equiv c \pmod{m}$ for all integers c and so in particular for $a + b$, $a - b$ and ab .

21.3 The multiplication table for R_{12} is given below.

From this, looking which rows contain 1, we see that 1, 5, 7 and 11 are the invertible elements and that each is its own inverse.

[Notice that these are precisely the positive integers less than 12 which are coprime to 12 illustrating the result of the next exercise.]

\times	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

21.4 The integer a is invertible modulo m precisely when the linear congruence $ax \equiv 1 \pmod{m}$ has a solution. By Theorem 20.1.7, this congruence has a solution if and only if a and m are coprime and so this is a criterion for a to be invertible modulo m .

21.5 From Example 20.2.2 we see that 290 and 357 are coprime and that $290 \times (-16) \equiv 1 \pmod{357}$. Hence $([290]_{357})^{-1} = [-16]_{357} = [341]_{357}$.

- (i) $290x \equiv 2 \pmod{357} \Leftrightarrow x \equiv -16 \times 2 = -32 \equiv 325 \pmod{357} \Leftrightarrow x \equiv 325 \pmod{357}$.
- (ii) $290x \equiv 5 \pmod{357} \Leftrightarrow x \equiv -16 \times 5 = -80 \equiv 277 \pmod{357} \Leftrightarrow x \equiv 277 \pmod{357}$.
- (iii) $290x \equiv 355 \pmod{357} \Leftrightarrow x \equiv -16 \times 355 \equiv -16 \times (-2) = 32 \pmod{357} \Leftrightarrow x \equiv 32 \pmod{357}$.

21.6 To prove that the function g is well-defined suppose that $[a_1]_m = [a_2]_m$. Then $a_1 \equiv a_2 \pmod{m}$ so that $r_m(a_1) = r_m(a_2) \pmod{m}$ (by Proposition 19.2.4). It follows that $r_m(a_1) + 1 = r_m(a_2) + 1$ as required.

To see that g is the inverse of f observe that, for $i \in \mathbb{N}_m$, $[a]_m = f(i) \Leftrightarrow [a]_m = [i-1]_m \Leftrightarrow a \equiv i-1 \pmod{m} \Leftrightarrow r_m(a) = i-1$ (since $i-1 \in R_m$) $\Leftrightarrow r_m(a) + 1 = i \Leftrightarrow g([a]_m) = i$.

Exercises 22 (page 269)

- 22.1** (i) This is the same as congruence modulo 2 and so is an equivalence relation. There are two equivalence classes: the odd integers and the even integers.
- (ii) This is not reflexive ($0 \not\sim 0$), is symmetric (since $a + b = b + a$) and not transitive (since $0 \sim 1$ and $1 \sim 0$ but $0 \not\sim 0$).
- (iii) This is not reflexive ($1 \not\sim 1$), is symmetric (since $a + b = b + a$) and not transitive (since $1 \sim 2$ and $2 \sim 1$ but $1 \not\sim 1$).
- (iv) This is an equivalence relation. The equivalence classes are $\{0\}$, $\{1, -1\}$, $\{2, -2\}$, $\{3, -3\}$,
- (v) This is not reflexive ($2 \not\sim 2$), is symmetric $a \sim b \Leftrightarrow a = 1$ and $b = 1 \Leftrightarrow b \sim a$ and is transitive ($a \sim b$ and $b \sim c \Rightarrow a = b = c = 1 \Rightarrow a \sim c$).
- (vi) This is not reflexive ($2 \not\sim 2$), is symmetric and is not transitive ($2 \sim 1$ and $1 \sim 2$ but $2 \not\sim 2$).
- (vii) This is an equivalence relation. The equivalence classes are lines parallel to the y -axis.
- (viii) This is an equivalence relation. The equivalence classes are circles with centre the origin.

22.2 The equivalence relation may be described by $a \sim b \Leftrightarrow ab > 0$ or $a = b = 0$.

22.3 To see that f is a surjection suppose that $a \in \mathbb{Z}$. If $a > 0$ then $f(a, 0) = a$; if $a = 0$ then $f(1, 1) = 0$; and if $a < 0$ then $f(0, -a) = a$. Thus f is a surjection. The equivalence relation is given by $(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow x_1 - x_2 = y_1 - y_2$. The equivalence classes have the form $\{(x_1, x_2) \mid x_1 - x_2 = k\}$ for some $k \in \mathbb{Z}$.

[This example gives one method of defining the set of integers \mathbb{Z} starting from the set of positive integers \mathbb{Z}^+ : we may define \mathbb{Z} to be the set of equivalence classes of the above equivalence relation on \mathbb{Z}^+ .]

Exercises 23 (page 287)

23.1 Applying the sieve of Erastosthenes gives the array on the next page.

Thus the primes less than 200 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109,

113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199 (46 in all).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

23.2 $4148 = 2^2 \times 17 \times 61$.

$$7684 = 2^2 \times 17 \times 113.$$

$$\text{Hence } \gcd(4148, 7684) = 2^2 \times 17 = 68.$$

[This is the same result as obtained in Exercise 16.1 by the Euclidean algorithm. Even with numbers of this size the method used in Chapter 16 is more efficient.]

23.3 For $n = 41$, $n^2 - n + 41 = 41^2 - 41 + 41 = 41^2$.

23.4 For $2 \leq i \leq n+1$ the integer $(n+1)! + i$ is divisible by i and so is composite. This provides a sequence of n consecutive composite numbers.

23.5 By the fundamental theorem of arithmetic an integer is not coprime to p^k if and only if it is a multiple of p . But now $1 \leq pq \leq p^k$ if and only if $1 \leq q \leq p^{k-1}$ and so there are p^{k-1} positive integers not

exceeding p^k which are not coprime to p^k . Hence the number which are coprime to p^k is $p^k - p^{k-1}$.

23.6 Suppose for contradiction that there is a rational number $q \in \mathbb{Q}$ such that $q^3 = 2$. Write $q = a/b$ where $a, b \in \mathbb{Z}^+$. Then $a^3 = 2b^3$. Let $2 < p_2 < \dots < p_r$ be the primes occurring as factors of a or of b . Then $a = 2^{k_1}p_2^{k_2}\dots p_r^{k_r}$ and $b = 2^{l_1}p_2^{l_2}\dots p_r^{l_r}$ where k_i and l_i are non-negative integers. This means that $a^3 = 2^{3k_1}p_2^{3k_2}\dots p_r^{3k_r}$ and $2b^3 = 2^{3l_1+1}p_2^{3l_2}\dots p_r^{3l_r}$. But by the fundamental theorem these expressions must be the same and so in particular $3k_1 = 3l_1 + 1$ which is impossible for integers k_1 and l_1 . This provides the necessary contradiction demonstrating that our hypothesis that there exists a rational cube root of 2 is false and so proving that no such rational number exists.

23.7 The proof that every integer $4q + 1$ for $q \in \mathbb{Z}^+$ is a product of pseudo-primes is by strong induction on q .

Base case: 5 ($q = 1$) is a prime and so a pseudo-prime.

Inductive step: Suppose as inductive hypothesis that each number $4q + 1$ is a product of pseudo-primes for $1 \leq q \leq k$. If $4(k + 1) + 1$ is a pseudo-prime then it is a product of a (single) pseudo-prime. Otherwise we can write $4(k + 1) + 1 = ab$ where $a > 1$ and $b > 1$ and $a \equiv b \equiv 1 \pmod{4}$. But then, by inductive hypothesis a and b may be written as products of pseudo-primes so that, by combining these products, we write $4(k + 1) + 1$ as a product of pseudo-primes. Hence in both cases $4(k + 1) + 1$ is a product of pseudo-primes, proving the inductive step.

Hence by induction, $4q + 1$ is a product of pseudo-primes for all $q \geq 1$.

Notice that a product of two primes congruent to 3 modulo 4 is necessarily a pseudo-prime. So for example $3 \times 3 = 9$, $3 \times 7 = 21$ and $7 \times 7 = 49$ are pseudo-primes. Thus $9 \times 49 = 21 \times 21 = 441$ has two distinct expressions as a product of pseudo-primes (and this is the smallest such number).

Exercises 24 (page 294)

24.1 By Fermat's theorem $2^{16} \equiv 1 \pmod{17}$. Hence $2^{1000000} \equiv 1 \pmod{17}$ since 16 divides 1000000 and so the remainder after $2^{1000000}$ is divided by 17 is 1.

24.2 By Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$ and $a^p \equiv a \pmod{p}$ so that $a^{2p-1} \equiv a \pmod{p}$. This means that p is a prime factor of $a^{2p-1} - a$.

However, $a^2 \equiv a \pmod{2}$ and so, by induction on n , $a^n \equiv a \pmod{2}$ for all positive integers n . In particular 2 is a prime factor of $a^{2p-1} - a$. Since p is odd, it follows that $2p$ is a divisor of $a^{2p-1} - a$, i.e. $a^{2p-1} \equiv a \pmod{2p}$.

24.3 By Fermat's theorem, $7^{16} \equiv 1 \pmod{17}$ and so an inverse of 7 modulo 17 is given by 7^{15} . Now $7^2 = 49 \equiv -2$, so $7^4 \equiv 4$, $7^8 \equiv 16 \equiv -1$ so that $7^{15} \equiv -1 \times 4 \times (-2) \times 7 = 56 \equiv 5$. Hence 5 is the inverse of 7 modulo 17.

24.4 The proof is by contradiction. Suppose that $n > 2$, $(n-1)! \equiv -1 \pmod{n}$ but that, for contradiction, n is not prime. Then there is an integer a such that $1 < a < n$ which divides n .

- (i) Since $1 < a < n$, it follows that $1 < a \leq n-1$ and so $(n-1)! \equiv 0 \pmod{a}$.
- (ii) Since a divides n and $(n-1)! \equiv -1 \pmod{n}$ it follows that $(n-1)! \equiv -1 \pmod{a}$ and so, since $a > 1$, $(n-1)! \not\equiv 0 \pmod{a}$.

This gives the necessary contradiction.

Hence our assumption that n is not prime must be false and so n is prime as required.

24.5 First of all notice that $p^{q-1} + q^{p-1} \equiv q^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem since p and q are coprime being distinct primes. Similarly $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$. Thus p and q are amongst the primes in the prime factorization of $p^{q-1} + q^{p-1} - 1$ which must therefore be divisible by pq . Hence $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Bibliography: suggestions for further reading

- G. Birkhoff and S. Mac Lane, *A survey of modern algebra*, Macmillan, Fourth edition 1977.
- Carl B. Boyer and Uta C. Merzbach, *A history of mathematics*, Wiley, Second edition 1989.
- Victor Bryant, *Yet another introduction to analysis*, Cambridge University Press, 1990.
- David M. Burton, *Elementary number theory*, Allyn and Bacon, 1976.
- Harold Davenport, *The higher arithmetic, an introduction to the theory of numbers*, Cambridge University Press, Sixth edition 1992.
- Donald M. Davis, *The nature and power of mathematics*, Princeton University Press, 1993.
- Keith Devlin, *Sets, functions and logic, an introduction to advanced mathematics*, Chapman and Hall, Second edition 1992.
- A. Gardiner, *Infinite processes, background to analysis*, Springer-Verlag, 1982.
- Carl Friedrich Gauss, *Disquisitiones arithmeticae* (translated by Arthur A. Clarke), Springer-Verlag, 1986.
- Rod Haggerty, *Fundamentals of mathematical analysis*, Addison-Wesley, Second edition 1993.
- J.F. Humphreys and M.Y. Prest, *Numbers, groups and codes*, Cambridge University Press, 1989.
- Kenneth H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, Second edition 1988.
- Alan Tucker, *Applied combinatorics*, Wiley, 1995.
- Daniel J. Velleman, *How to prove it, a structured approach*, Cambridge University Press, 1994.

List of symbols

$P(n)$, $P(m, n)$ predicates 4	∞ infinity 116
π pi 5	χ_A characteristic function 117
$a \leq b$, $a = \pm b$ 6	$\mathbb{N}_n = \{1, 2, \dots, n\}$ 124
$ a $ modulus of a 7, 93	$ X $ cardinality of X 124, 178
\Rightarrow implies 10	$D(a)$ divisors 140
$\not\Rightarrow$ does not imply 12	(a, b) , $\gcd(a, b)$ 141
\square end of proof 17	$\text{Fun}(X, Y)$ functions 145
$\sum a(i)$ sum 46	$(n)_m$ falling factorial 146
x^n power 48, 56, 109, 186	$\text{Inj}(X, Y)$ injections 146
$n!$ factorial 48	χ_A characteristic function 148
$\prod a(i)$ product 55	$\mathcal{P}_r(X)$ r -subset 149
$\mathbb{Z}, \mathbb{Z}^+, \mathbb{Z}^{\geq}$ integers 62	$\binom{n}{r}$ binomial coefficient 149
\mathbb{Q} rationals 62, 162	\aleph_0 aleph null 171
$\mathbb{R}, \mathbb{R}^+, \mathbb{R}^{\geq}$ reals 62	e base of natural logarithms 180
\mathbb{C} complex numbers 62	$[a, b]$, $\text{lcm}[a, b]$ 227
\in, \notin set elements 62	$a \equiv b \pmod{m}$ congruence 232
\emptyset empty set 65	R_m remainders 234
\subseteq, \subset subset 66	$r_m: \mathbb{Z} \rightarrow R_m$ remainder function 235
$A \cap B$ intersection 67	$[a]_m$ congruence class 251
$A \cup B$ union 67	\mathbb{Z}_m congruence classes 253
$A - B$ difference 67	$a \sim b$, $a \not\sim b$ relation 264
$\mathcal{P}(X)$ power set 70	$a \sim_{\Pi} b$ partition relation 264
A^c complement 70	$[a]$ equivalence class 267
$(a, b), [a, b], [a, b), (a, b]$ real intervals 72	X/\sim set of equivalence classes 267
\forall for all 75	$\pi(n)$ primes 285
\exists for some 76	\log_e natural logarithm 286
$(x, y) \in X \times Y$ Cartesian product 83	$\text{li}(n)$ logarithmic integral 287
c_y constant function 91	$\phi(n)$ Euler's totient function 288
I_X identity function 91	
$f A$ restriction of f 94	
$g \circ f$ composite 94	
$\lim f$ limit of sequence 96	
$\text{Im } f$ image of f 98, 103	
\sqrt{y} square root 105	
f^{-1} inverse function 106, 111	
$x^{1/n}$, $\sqrt[n]{x}$ n th root 109	
$\overleftarrow{f}, \overleftarrow{f}$ 111	
$A \Delta B$ symmetric difference 116	
$[a, \infty), (a, \infty)$ real intervals 116	

Index

- absolute value 7
- absorption laws 115
- abstraction 61, 144, 250
- addition 18, 113, 161, 255, 256
 - addition law for inequalities 24
 - addition principle 128
- aleph null 171
- algebra 203
- algebraic number 180, 187
- algebraic number properties 18, 159, 256
 - algebraic structure 18
- algorithm 203, 280
- al-Khowarizmi, Mohammed ibn-Musa 203
- all 75
- ambiguity 22, 141
- analysis 97
- and 7, 25
- antecedent 11
- any 75, 76
- Archimedes 5
 - Archimedean axiom 166
- arithmetic 15, 191
 - arithmetic modulo a prime 290
 - arithmetic of congruence classes 254
 - arithmetic of remainders 256
- arithmetic progression 309
- arrow picture of a function 90
- associativity 19, 71, 96, 119
- asymptotic 286
- axiom 17
 - axiomatic method 18
- Babylonians 157
- base 48
- base case 40, 44
- BASIC 203
- Bernoulli's inequality 55
- bijection 102, 107, 147
- bijective 108
- Binet, J.P.M. 80
- Binet formula 50
- binomial coefficients 57, 149
 - binomial theorem 153
- Bolzano, Bernhard 172
- bound variable 75
- box picture of a function 90
- calendar 231, 336
- Cantor, Georg 177
 - Cantor–Schröder–Bernstein theorem 180, 329
 - Cantor's diagonal process 177
- cardinality 123, 178
- Cartesian product 83, 98, 245
- cause 12
- characteristic function 117, 148
- closed interval 72
- codes 279
- codomain 89
- Cohen, Paul 178
- commensurable 158
- common divisor 140
- commutativity 18, 71, 95, 119
- complement of a set 70
- completeness axiom 166
- complex number 62, 156, 159, 306
- composite number 277
- composition of functions 94
- conclusion 11
- conditional statement 12
 - conditional definition of set 63
- congruence 231, 232
 - congruence class 231, 250, 251, 262
- conjunction 7
- consequent 11
- constant function 91
- constructive definition of set 64
- continuity axiom 166
- continuum hypothesis 178
- contradiction 30
- contrapositive 34

convergence 96
 converse 14
 coordinate 83
 coprime integers 141, 212, 242
 cosine function 5, 109
 countable set 171
 counterexample 79
 counting 123, 144, 157, 170, 325
 counting argument 133, 170, 250
 cryptography 279
 cypherization 157
 days of the week 231
 decimal 164
 decimal arithmetic 168
 de la Vallée-Poussin, C.J. 286
 De Morgan, Augustus 71
 De Morgan laws 71
 Dedekind, Richard 39, 112, 158, 173,
 251
 definition 15
 inductive 45
 recursive 45
 Deligne, Pierre 152
 denominator 159
 denumerable set 171, 174
 derangement 185
 diagonal set 130
 difference of sets 67
 Diophantus 216
 diophantine equation 216, 245
 Dirichlet, Lejeune 136, 218
 disjoint sets 67
 disjunction 6
 disproof by counterexample 79
 disproof of statements involving
 quantifiers 79
 distributivity 19, 71
 divides 16
 3 divisibility by 239
 9 divisibility by 271
 11 divisibility by 271
 division 19, 159, 162, 237
 division theorem 141, 191, 226
 divisor 140, 283
 domain 89
 dummy variable 64, 75
 e 180
 each 75
 element 62
 empty set 65
 enumerable set 171
 equal functions 93
 equal sets 65
 equipotent sets 171
 equivalence class 266
 equivalence relation 265
 equivalent 15, 300
 Erastosthenes of Cyrene 280
 sieve of Erastosthenes 280
 Euclid 17, 50, 158, 200, 217, 278, 285
 Euclidean algorithm 200, 202, 225,
 245
 Euclidean plane 84
 Eudoxus 158
 Euler, Leonhard 4, 218, 285, 289, 297
 Euler's totient function 288, 296
 even integer 16, 142, 231, 235, 250, 251,
 254
 every 75
 exhaustive cases 26
 existence 13, 192, 287
 existential quantifier 76
 existential statement 75
 exponent 48, 56, 109, 186
 laws of exponents 52, 56, 186
 exponential function 287
 factor 140
 factorial 48
 falling factorial 146
 false 6
 Fermat, Pierre de 217, 289
 Fermat's last theorem 217
 Fermat's little theorem 290, 297
 Fibonacci 49
 Fibonacci number 49, 57, 225, 272
 Fibonacci's rabbit problem 57
 field 18
 finite decimal 165, 186
 finite set 128, 133, 136
 formula 91
 fraction 159, 268
 free variable 4, 74
 function 89, 99, 144
 of two variables 317
 fundamental theorem of arithmetic 282
 Galileo Galilei 172
 Gauss, Carl Friedrich 232, 281, 285, 297
 geometric progression 309
 geometry 17
 given-goal diagram 23
 Goldbach, Christian 4
 Goldbach conjecture 4
 golden ratio 50
 graph 98
 greatest common divisor (gcd) 140, 199,
 207, 211, 225, 227, 295
 group theory 289
 Hadamard, Jacques 286
 half-infinite interval 116
 half-open interval 72
 Hermite, Charles 180
 highest common factor 140
 Hindu–Arabic numerals 157
 homogeneous equation 221

Humpty Dumpty's principle 15
 hypothesis 11
 identity function 91
 if 14, 106
 if and only if 15
 iff 15
 image of an element 89
 image of a function 97, 103, 111
 implication 10
 implies 14
 inclusion function 95
 inclusion-exclusion principle 131, 182,
 296
 incommensurable 158
 index 48, 56, 109, 186
 laws of indices 52, 56, 186
 induction principle 39, 139, 184
 strong induction 48, 88
 inductive definition 45
 inductive hypothesis 40
 inductive step 40
 inequality axioms 23
 infinity 116
 infinite decimal 164, 166, 186, 198,
 225, 296
 infinite set 128, 170
 infinite sequence 97
 inhomogeneous equation 221
 injection 101, 146
 integer 15, 62
 integral domain 18
 intersection of sets 66
 interval of real numbers 72, 116
 closed 72
 half-infinite 116
 half-open 72
 open 72
 inverse function 106, 320
 right inverse 118
 inverse modulo m 260
 invertible function 106
 invertible modulo m 260
 irrational number 164
 isomorphism 257
 Ivory, James 290
 Lagrange, Joseph 291
 Lamé, Gabriel 203
 Lamé's theorem 226
 least common multiple (lcm) 226, 295
 Legendre, Adrien-Marie 218, 286
 Leibniz, Gottfried 289
 Leibniz's rule 185
 lemma 127
 Leonardo of Pisa 49
 limit 96
 Lindemann, Ferdinand 180
 linear combination 207
 linear congruence 238, 240
 linear diophantine equation 216, 258
 Liouville, Joseph 180
 listing elements 63, 89
 Littlewood, J.E. 287
 logarithm 286
 logarithmic integral 287
 logical connectives 5
 lowest terms 160
 magnitude 158
 map 89
 mathematical invention 27
 mathematical statement 3
 mathematical truth 17
 maximum 138
 measurement 157
 minimum 138
 modular arithmetic 233
 modulus 231
 modulus function 7, 93
 multiple 140, 116
 multiplication 18, 113, 161, 255, 256
 multiplication law for inequalities 24
 multiplication principle 130
 natural logarithm 286
 natural number 62, 123
 necessary 14
 necessary and sufficient 15
 negation 7
 negative integer 157
 Newton, Isaac 153
 non-constructive proof 259
 non-existence result 30
 not 7
 null sequence 96
 number 123, 157
 number theory 15
 numerator 159
 odd integer 16, 32, 142, 231, 250, 251,
 254
 one-to-one function 101
 only if 14
 onto function 102
 open interval 72
 or 5, 25, 27, 35, 304
 order axioms 23
 order modulo a prime 291, 296
 ordered pair 83
 paradox 172
 partition 252, 262, 266
 Pascal, Blaise 151
 Pascal's triangle 151
 Peano, Giuseppe 18, 62, 112
 Peano's axioms 112
 Pearce, Benjamin 71
 perfect square 197, 198
 permutation 147

pi 5
 pigeonhole principle 133, 136, 146, 180,
 250, 259
 place value system 157
 positive integers 62, 112
 power set 70, 148, 178, 262
 powers 48, 56, 109, 186
 powers modulo a prime 291
 predicate 4, 74, 81
 pre-image 102, 111
 prime number 4, 277
 primality test 293
 prime factor 280
 prime factorization 282
 prime number theorem 286
 primitive root 291
 principal value of inverse circular
 functions 109
 product 55, 113
 proof 10, 21, 77
 backwards 27
 by cases 25
 by contradiction 30, 163, 285
 by contrapositive 34
 by counterexample 79
 by enumeration 26
 by example 77
 by induction 39, 80
 construction 22
 direct 21
 non-constructive 259
 of statements involving quantifiers 77
 template 32, 42, 44, 49
 proper subset 66
 proposition 3, 16, 74
 public-key cryptography 279, 289
 Pythagoras 158
 Pythagoras's theorem 158, 161
 Pythagorean triples 217
 Pythagoreans 158
 quantifiers 74
 quotient 191
 rational number 62, 159, 176, 268
 real number 62, 164, 166
 recurring decimal 166, 225, 296
 reflexivity 233, 264
 relation 264
 relatively prime 141
 remainder 191, 231, 234
 remainder map 235
 residue 234
 restriction 94
 right inverse 118
 root 109
 sequence 96
 set 61
 sexagesimal fraction 157
 sine function 108
 singleton set 70
 Skewes, S. 287
 solution set 65, 245
 some 76
 square root 105
 square root of 2 irrational 162, 165,
 284
 squaring the circle 180
 statement 3
 strong induction 48, 88, 278
 subset 66, 148
 subtraction 19, 162, 255, 256
 successor 39, 112
 successor function 112
 sufficient 14
 sum 46, 113
 sum of squares 225, 236
 surjection 102, 184
 syllogism 25
 symbols 24
 symmetric difference 116
 symmetry 233, 264
 tangent function 109
 then 14
 transcendental number 180
 transitivity 24, 233, 264
 triangle inequality 306
 trichotomy law 24
 true 6
 truth table 6, 67
 truth value 6
 uncountable set 171, 176
 union of sets 67
 uniqueness 192, 235, 243
 unit 277
 unity 19
 universal quantifier 75
 universal set 70
 universal statement 13, 74, 301
 universal implication 13
 value 4, 89
 Venn diagram 68
 Waring, Edward 291
 well-defined 93, 125, 161, 186, 235, 255,
 268, 273, 301
 well-ordering principle 139, 143, 184
 Wiles, Andrew 218
 Wilson, John 291
 writing mathematics 22
 zero 19, 157

CORRECTIONS TO
An Introduction to Mathematical Reasoning

BY PETER J. ECCLES
NOVEMBER 16, 2009

Thanks to Jerry Folland and John Palmieri for pointing out these corrections.

- p. 56, problem 21: $x + 1/x$ is to be interpreted as $x + (1/x)$, not $(x + 1)/x$. Same goes for $x^n + 1/x^n$.
- p. 78, line 6 from bottom: $a \rightarrow n$.
- p. 97, last line of proof of Example 8.3.3: $\text{is} \rightarrow \text{as}$.
- p. 125, 5th line of text: $n - i$ should be $n + 1 - i$.
- p. 184, problem 14: N should be \mathbb{N} .
- p. 185, problem 18, line 4: the summation should be from 0 to k , not 0 to n .
- p. 185, problem 20, second line: change “disjoint” to “distinct.”
- p. 267, second displayed equation: \mathbb{Z} should be X .
- p. 269, last line: $(a_1, a_2) = (b_1, b_2)$ should be $(a_1, a_2) \sim (b_1, b_2)$.
- p. 270, problem 22.2: Z^+ should be \mathbb{Z}^+ .
- p. 323, last 3 lines: In the last two sentences X and Y need to be switched.
- p. 327, solution to problem 14.1, line 2: $|X|$ should be $|A|$.
- p. 341, solution to problem 22.3: Change $f(a, 0)$ to $f(a + 1, 1)$, and $f(0, -a)$ to $f(1, 1 - a)$.

MORE CORRECTIONS TO
An Introduction to Mathematical Reasoning
BY PETER J. ECCLES
APRIL 19, 2013

- p. 57, problem 25: the right side of the formula is actually not defined if $m = 1$, because u_{m-1} appears. So either prove this for all positive integers n and all integers $m \geq 2$, or define u_0 to be zero.
- p. 95, Proposition 8.2.3(i): the codomain of the composition should be W , not Z .
- p. 117, problem 14: the set in the last line of the problem should be $\{x \in \mathbb{R} \mid f \circ g(x) = g \circ f(x)\}$.
- p. 225, problem 7: it should say “takes precisely $n - 1$ steps” (instead of n steps), and it should be for $n \geq 2$.