

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
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
Tenth printing 2007

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.

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
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	59
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	121
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	189
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

$$\pi > 3 \text{ and } \pi < 4$$

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

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

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

$$a < b \Leftrightarrow ac < bc \quad \text{if } c > 0,$$

$$a < b \Leftrightarrow ac > bc \quad \text{if } c < 0.$$

- (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 ‘ $(P \Rightarrow Q)$ 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 $a^2 - 3a + 2 = 0$. □

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

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. \square

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	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 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 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 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* ' $(\text{not } Q) \Rightarrow (\text{not } P)$ ' 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

$(\text{not } P)$ is the statement $ac > bc$,
 $(\text{not } Q)$ is the statement $c > 0$,

and so the statement $(\text{not } Q) \Rightarrow (\text{not } P)$ 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 ' $(\text{not } P) \Rightarrow Q$ ' (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 $a^2 \geq 7a$ then $a \leq 0$ or $a \geq 7$.

38 **Part I: Mathematical statements and proofs**

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, 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, ... 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.

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

Alternatively we can start on the other side as follows.

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

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 $1 \leq 2$, $n \leq 2^n$.

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

Conclusion: Hence, by induction, $n \leq 2^n$ 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 num-

bers $\boxed{\sum_{i=1}^n a(i)}$ 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 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 factorial n , written $n!$, 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 $P(1)$, $P(2)$, \dots , $P(k - 1)$. 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) $[P(n)$ 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 $[P(n)$ 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, $[P(n)$ 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, \dots , 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 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

$$\begin{aligned} \text{(i)} \quad & \prod_{i=1}^1 a(i) = a(1), \text{ and} \\ \text{(ii)} \quad & \prod_{i=1}^{k+1} a(i) = \left(\prod_{i=1}^k a(i) \right) a(k+1) \text{ for } k \geq 1. \end{aligned}$$

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

shape: .

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

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

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.]