MA103
Introduction to Abstract Mathematics
Lecture Notes, First Half

Martin Anthony

Preface by Martin Anthony

The text of these notes is mainly an edited version of the first half of a subject guide I wrote for the University of London International Programmes.

I thank Michele Harvey for her help with the material on complex numbers. I am grateful to Keith Martin, Jan van den Heuvel and Amol Sasane for carefully reading a draft of the subject guide and for suggesting ways in which to improve it.

These notes also incorporate materials written in previous years by Jan van den Heuvel and Graham Brightwell and I am grateful to them for allowing me to use these.

Thanks also to Mark Baltovic for help with typesetting.

These lecture notes were edited by Peter Allen. I am very grateful to Martin Anthony for writing all the good content; the mistakes are my fault.

Contents

Chapter 1
Introduction

In this very brief introduction, I aim to give you an idea of the nature of this subject and to advise on how best to approach it. I also give general information about these notes and recommended reading.

1.1 What is this course about?

There are two main concepts in this course, and they are the two main concepts you will learn, use, and re-use throughout your degree. After you have finished your degree, you might never again use some of the mathematics you learn: but the ways of thinking which you will be shown, will practice, and will steadily improve through your time here will stay with you. These ways of thinking which you spend three years training are what in the end prepare you for your future career. These concepts are *abstraction* and *proof*.

You probably saw before at least some idea of what a mathematical proof is (but it is fine if you did not—we will cover it!), and you probably do not know what 'abstraction' should be (which is also fine). So I will begin by giving an example of abstraction which you met long ago. Choose a number, multiply it by itself, then add your chosen number four times, and finally add four. For example:

$$\begin{aligned} &1\times 1+1+1+1+1+4=9 \;\; &&=3\times 3=(1+2)\times(1+2)\\ &2\times 2+2+2+2+2+4=16 &&=4\times 4=(2+2)\times(2+2)\\ &3\times 3+3+3+3+3+4=25 &&=5\times 5=(3+2)\times(3+2) \quad \text{and so on}\ldots \end{aligned}$$

These are *concrete examples*. You probably see that there is a pattern to the answers we get. We can write it more generally:

$$x\times x+4\times x+4=(x+2)\times(x+2)\,.$$

This is a *mathematical statement*. It's something which is either true or false (depending on what x is). It means the same as the following English:

> Choose a number, multiply it by itself, then add your chosen number four times, and finally add four. You will get the same answer as if you add two to your chosen number to get a new number, then multiply the new number by itself.

Writing x in an equation, rather than 'your chosen number' in an English phrase, is an example of a (simple) abstraction. Here the purpose is to simplify the presentation. There is no *need* to write equations with xs in them; you could do it all in words—and

indeed long ago that is what people did. Of course, it's hard to get anything done like that. If you show the equation to a small child, it won't mean anything to them, while they can read and understand the sentence. But once you understand what the symbols in the equation mean, then it's much quicker and easier to read or write.

Now we come to proof. Is the statement above (however it's written) *true* for some other values of x than the three we checked by calculation? And if so, why? The purpose of a proof is *not* just to be certain that a statement is true. It also explains *why* a statement is true. As you probably know, the statement we wrote is true for all integers. Here is a proof.

Proof.

$$\begin{aligned}
&(x+2)\times(x+2)\\
=&(x+2)\times x+(x+2)\times 2 && \text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+(x+2)\times 2 && \text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+x\times 2+2\times 2 && \text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+x\times 2+4 && (2\times 2=4)\\
=&x\times x+2\times x+2\times x+4 && \text{(multiplication is commutative)}\\
=&x\times x+(2+2)\times x+4 && \text{(multiplication distributes over addition)}\\
=&x\times x+4\times x+4 && (2+2=4)
\end{aligned}$$

We can see that each line is equal to the previous one, for any integer x, because of the reason given on the right. Most of the reasons are *axioms*—statements which we are assuming to be true—and a couple are little calculations which you should check. So in particular the first and last lines are equal for any integer x, in other words the statement

$$(x+2)\times(x+2)=x\times x+4\times x+4$$

is true for any integer x. That's what we wanted to prove. □

Of course, you will never want to write down a proof in this kind of detail. You would much rather write at most a couple of lines of algebra expanding out the brackets, just as you would have done in school, or simply write 'it is obvious that $(x+2)\times(x+2)=x\times x+4\times x+4$'. This is fine. You just need to be aware that when you write 'it is obvious...' that you are promising that if someone really wants to see the details, you would be able to write out the details as above.

Let's go back to *abstraction*. These *axioms* we wrote down above (multiplication distributes over addition, multiplication is commutative) are statements which you presumably agree are true for the integers. Of course, they are also true for other numbers—they are true for real numbers, or complex numbers. That means that the proof we wrote down works equally well for real numbers, or complex numbers. So you know, for instance, that

$$(4.5+6i+2)\times(4.5+6i+2)=(4.5+6i)\times(4.5+6i)+4\times(4.5+6i)+4$$

is a true statement. This is a second reason abstraction is important: it is a time- and memory-saving device. You can prove something once—or remember one fact—in an abstract setting and use it in many different concrete examples.

Next term, we'll give axiomatic definitions of a *group* and a *vector space*, and start proving theorems about abstract groups (and vector spaces). Here 'abstract' means we don't assume anything about the group except the axioms. This will seem painful and useless at first: you'll (by then) know a few concrete examples of groups and of vector spaces. It will usually be easier to see how to prove the theorems for the concrete examples. Usually you will have some idea already why the theorems should be true in the examples, while you won't have much intuition for how abstract groups behave. The natural response will be that you don't want to study abstract groups, you want to work with the concrete examples you know. But this is the **wrong reaction**. The reason is that you will then *only* learn about the concrete examples you already know, and you will suffer as soon as in future courses you see new examples of groups and are expected to immediately know a bunch of facts about them (and also in the exam, where we will likely test your ability to work with a new example of an abstract structure).

In this course, we need to work with *precise definitions* and *statements*, and you will need to know these. Not only will you need to know these, but you will have to understand them, and be able (through the use of them) to demonstrate that you understand them. Simply learning the definitions without understanding what they mean is not going to be adequate. I hope that these words of warning don't discourage you, but I think it's important to make it clear that this is a subject at a higher conceptual level than most of the mathematics you are likely to have studied before. This does not mean it is incredibly hard and you will struggle. It is not incredibly hard, and you are quite capable of doing well in this course (or you would not be here). It does mean, though, that if you are used to getting through school courses by memorising material without understanding it, then now is the time to change that (and, by the way, no-one will hire you for your memorisation ability—a computer does that better!).

In this course, you will learn how to *prove* mathematical statements precisely. This is a very different sort of mathematics from that which you will have encountered in many other mathematics courses you have previously taken, where the emphasis is on solving problems through *calculation*. In Abstract Mathematics, one has to be able to produce convincing mathematical arguments as to why a given mathematical statement is true or false. For example, a prime number is defined to be a positive integer greater than 1 that is only divisible by itself and the number 1 (so 7 is a prime number, but 8 is not). The statement "There are infinitely many prime numbers" is a mathematical statement, and it is either true (there are infinitely many prime numbers) or false (there are only a finitely many prime numbers). In fact, the statement is true. But why? There's no quick 'calculation' we can do to establish the truth of the statement. What is needed is a proof: a watertight, logical argument. This is the type of problem we consider in this course.

1.1.1 How to get the most out of this course (and all the other maths courses)

There are two theories about mathematical ability (and intelligence in general). One theory says that you have what you are born with. The other says that (just like strength or stamina) it's something you develop by practice. Various studies have shown that broadly similar number of students believe each theory, but the ones who believe ability is something you develop are consistently the ones who do better—and almost all academic mathematicians believe ability is something you learn and train.

Some people are faster than others, but speed is in the end not all that useful: no matter how fast you are, if you switch off and coast for a while, you will have trouble catching up with people who pay attention and work on understanding their courses. In particular—and this is different to school maths—we will always assume you understood the previous lectures and courses, and we will use things from those previous lectures and courses all the time. If you do understand the previous material—even if you are not so fast—you'll understand a good deal of the current lecture (maybe all of it, maybe not quite) in real time, and you won't need to spend much time after the lecture going over the material. If you don't really understand the previous material, you won't have a chance to understand large parts of the lecture and you'll have to do even more work afterwards to catch up.

In this course, all the theory will be introduced in the lectures, together with some examples. There will be extra examples sessions (which don't exist in most courses—don't expect them!), which you do not have to attend but which may well be useful. In the lectures and examples sessions, you should be trying to understand what is going on. Don't waste time copying things down which will appear on Moodle (which is essentially everything). Certainly don't waste time with a newspaper or games on your phone, which annoys me and distracts your classmates. No-one is taking attendance in the lectures; if you're not going to pay attention, go to a café instead. If you do not understand something I said or wrote, then probably either I didn't explain it properly or I made a mistake, so you should **ask questions** (louder, or put your hand up, if I don't hear). If I ask a question, **I really want an answer**. Probably you need to think about the question to answer it, so I will wait until someone does answer.

For many of you there will be some point in the lectures where you do not immediately understand what I say, and when you ask a question the answer is still not very useful. You should keep asking me to explain better in such a situation. It is possible that I will eventually say that I want to move on and you should think about it after the lecture. That doesn't mean I think you are stupid, it generally means I am failing to understand what exactly you don't understand, or maybe I do understand but cannot think of a good way to explain it on the spot. In either case, if you try to formulate clearly exactly what it is that you do not like (which will take time, which is why you should do it after the lecture), you will probably find that doing so also helps you figure out what is going on; once you understand something deeply in this way you will not forget it. But it would still be useful to tell me about it after the lecture, so that I can improve the lectures for next year (and if possible give some more explanation on Moodle directly).

There will also be problems set every week, some online (for which you'll see results immediately) and some which you will solve and hand in to your class teacher, who will mark them and discuss in the next class. **The marks you get do not affect your result in the course**. The purpose of the problems is for you to practice and check you really know what is going on. If you get stuck, hand in half a solution with 'I don't know what to do next' and your class teacher will tell you (either written on the work, or maybe many people were stuck in the same place and the class teacher will go over it in class; usually then there will be a short comment like 'Will discuss in class'). Then you learn something. If you don't hand anything in, or you only hand in the problems you could solve, you don't learn anything. The written comments on your work, and the explanations in class, are the most important piece of feedback you get—but you only get it if you show us something on which we can give feedback. On that note—please do not copy work from someone else (or from last year's solutions). Doing this is a waste of your time and ours.

Finally, there are office hours and the Maths Support Centre. If you don't understand something, you should first try to figure it out for yourself—if you manage, then you won't forget it (and you should be happy with yourself). But if you get stuck, then you should not wait and hope that it magically gets clear. It probably will not, and you will suffer because you don't understand something I am assuming you do understand in my lectures. So go to office hours or the Support Centre and ask questions. You have already paid for those office hours; use them. You can also try talking with your friends on the course and seeing if you can figure out what's going on—group work can be fun and productive.

You can, of course, also read books (in these notes you'll see references to a couple which might be useful). But you do not need to do this. If you really want even more problems to solve, then you can find them in textbooks, but you will likely feel you already have enough work. If you don't understand something I say in the lecture, and it doesn't get clear when you talk to friends or go to office hour or try to solve the week's problems, you might try reading a textbook to see if a different presentation helps. However this is really a last resort.

1.1.2 Aims

The course is designed to enable you to:

- develop your ability to think in a critical manner;
- formulate and develop mathematical arguments in a logical manner;
- improve your skill in acquiring new understanding and expertise;
- acquire an understanding of basic abstract mathematics, and the role of logical argument in mathematics.

1.1.3 Learning objectives

Having taken this subject, you should:

- have a knowledge of basic mathematical concepts in discrete mathematics, algebra, and real analysis;
- be able to use formal notation correctly and in connection with precise statements in English (or indeed any other natural language);
- be able to solve mathematical problems in discrete mathematics, algebra and real analysis;
- be able to find and formulate simple proofs.

1.1.4 Topics covered (first half of the course)

Descriptions of topics to be covered appear in the relevant chapters. However, it is useful to give a brief overview at this stage. These notes cover the first half of this course. Here, we are concerned primarily with proof, logic, and number systems. We will first investigate how precise mathematical statements can be formulated, and here we will use the language and symbols of mathematical logic. We will then study how one can prove or disprove mathematical statements. Next, we look at some important ideas connected with functions, relations, and numbers. For example, we will look at prime numbers and learn what special properties these important numbers have, and how one may prove such properties.

Some of this material is intended to help you prepare for the second half of this course; the rest is intended to prepare you for the second-year and later mathematics courses. All of it is examinable, with the exception of sections which are clearly marked 'non-examinable'. Just to be clear — some of the non-examinable material will be useful for understanding the course (and I'll probably talk about it in lectures), some is background which you will not need to understand the course (but which you might find interesting, and which I will probably not talk about in lectures). The way I choose what material is examinable and what is not, is I try to come up with a good exam question; if I can't, then I'll mark it as non-examinable. That means, anything in the course marked as examinable is material which I know how to test in an exam.

1.2 Moodle

All information and materials for this course are on Moodle:

`http://moodle.lse.ac.uk/course/view.php?id=1989`

On the course Moodle page, you will find assignments, solutions, lecture notes, and so on.

1.3 Reading

There are many books that would be useful for this subject, since abstract mathematics is a components of almost all university-level mathematics degree

programmes.

For the first half of the course (the part covered by these notes), the following two books are recommended.

☞ Biggs, Norman L., *Discrete Mathematics*, Second edition. (Oxford University Press, 2002). [ISBN 0198507178].

☞ Eccles, P.J., *An Introduction to Mathematical Reasoning: numbers, sets and functions*. (Cambridge University Press, 1997). [ISBN 0521597188].

There is one topic that neither of these covers, which is the topic of Complex Numbers. However, this is a topic that is well-covered in a number of other textbooks and I have included a fairly full treatment of it in these notes to compensate for the fact that it is not covered in these two recommended textbooks.

1.4 Activities and sample exercises

Throughout the chapters of these notes, you'll find 'activities'. These are things for you to do or think about as you read, just to reaffirm that you've understood the material.

At the end of each chapter of these notes you will find some sample exercises together with solutions. These are not the exercises that will be assigned for classes, but are *additional* to those. They are a very useful resource. You should try them once you think you have mastered a particular chapter. Really try them: don't just simply read the solutions provided. Make a serious attempt before consulting the solutions. Note that the solutions are often just sketch solutions, to indicate to you how to answer the questions.

2

Chapter 2
Mathematical statements, proof, logic, and sets

☞ Biggs, N.L. *Discrete Mathematics*. Chapters 1–3.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapters 1–4 and 6.

2.1 Introduction

In this course, we want to make precise mathematical statements and establish whether they are true or not—we want to *prove* things. But for that, we have to first understand what a proof is. We will look at fairly simple types of mathematical statement, in order to emphasise techniques of proof. Some of these statements are going to be interesting, others are not so interesting—bear in mind that what you are doing in this part of the course is learning the rules of the game: the play (and more of the fun) comes later.

In later chapters (such as those on numbers, analysis and algebra) we will use these proof techniques extensively. You might think that some of the things we prove in this chapter are very obvious and hardly merit proving, but proving even 'obvious' statements can be quite tricky sometimes, and it is good preparation for proving more complicated things later.

2.2 Mathematical statements and proof

To introduce the topics of mathematical statement and proof, we start by giving some explicit examples. Later in the chapter we give some general theory and principles. Our discussion of the general theory is limited because this is not a course in logic. We need enough logic to understand what mathematical statements mean and how we might prove or disprove them. We don't need to start talking about things like which statements are provable and which statements are true (and whether those are the same or not). There are interesting mathematical things to say there (and interesting philosophical things), but you don't need to know them in order to do mathematics.

2.2.1 Examples of Mathematical Statements

Consider the following statements (in which, you should recall that the natural numbers are the positive integers):

(a) 20 is divisible by 4.

(b) 21 is not divisible by 7.

(c) 21 is divisible by 4.

(d) 21 is divisible by 3 or 5.

(e) 50 is divisible by 2 and 5.

(f) n^2 is even.

(g) For every natural number n, the number $n^2 + n$ is even.

(h) There is a natural number n such that $2n = 2^n$.

(i) If n is even, then n^2 is even.

(j) For all odd numbers n, n^2 is odd.

(k) For natural numbers n, n^2 is even if and only if n is even.

(l) There are no natural numbers m and n such that $\sqrt{2} = m/n$.

These are all mathematical statements, of different sorts (all of which will be discussed in more detail in the remainder of this chapter).

Statements (a) to (e) are straightforward *propositions* about certain numbers, and these are either true or false. Statements (d) and (e) are examples of *compound statements*. Statement (d) is true precisely when *either one (or both)* of the statements '21 is divisible by 3' and '21 is divisible by 5' is true. Statement (e) is true precisely when *both* of the statements '50 is divisible by 2' and '50 is divisible by 5' are true.

Statement (f) is different, because the number n is not specified and whether the statement is true or false will depend on the value of the so-called 'free variable' n. Such a statement is known as a *predicate*.

Statement (g) makes an assertion about *all* natural numbers and is an example of a *universal statement*.

Statement (h) asserts the existence of a particular number and is an example of an *existential* statement.

Statement (i) can be considered as an assertion about all even numbers, and so it is a universal statement, where the 'universe' is all even numbers. But it can also be considered as an *implication*, asserting that *if* n happens to be even, *then* n^2 is even.

Statement (j) is a universal statement about all odd numbers. It can also be thought of (or rephrased) as an implication, for it says precisely the same as 'if n is odd, then n^2 is odd'.

Statement (k) is an 'if and only if' statement: what it says is that n^2 is even, for a natural number n, *precisely when* n is even. But this means two things: namely that n^2 is even if n is even, and n is even if n^2 is even. Equivalently, it means that n^2 is even if n is even and that n^2 is odd if n is odd. So statement (k) will be true precisely if (i) and (j) are true.

Statement (l) asserts the non-existence of a certain pair of numbers (m, n). Another way of thinking about this statement is that it says that for all choices of (m, n), it is *not* the case that $m/n = \sqrt{2}$. (This is an example of the general rule that a non-existence statement can be thought of as a universal statement, something to be discussed later in more detail.)

It's probably worth giving some examples of things that are *not* proper mathematical statements.

'6 is a nice number' is not a mathematical statement. This is because 'nice number' has no mathematical meaning. However, if, beforehand, we had *defined* 'nice number' in some way, then this would not be a problem. For example, suppose we said:

> Let us say that a number is *nice* if it is the sum of all the positive numbers that divide it and are less than it.

Then '6 is a nice number' would be a proper mathematical statement, and it would be true, because 6 has positive divisors $1, 2, 3, 6$ and $6 = 1 + 2 + 3$. But without defining what 'nice' means, it's not a mathematical statement. Definitions are important[1].

'$n^2 + n$' is not a mathematical statement, because it does not say anything about $n^2 + n$. It is not a mathematical statement in the same way that 'David Cameron' is not a sentence: it makes no assertion about what David Cameron is or does. However, '$n^2 + n > 0$' is an example of a *predicate* with free variable n and, for a particular value of n, this is a mathematical statement. Likewise, 'for all natural numbers n, $n^2 + n > 0$' is a mathematical statement.

2.2.2 Introduction to proving statements

We've seen, above, various types of mathematical statement, and such statements are either true or false. But how would we establish the truth or falsity of these?

We can, even at this early stage, prove (by which we mean establish the truth of) or disprove (by which we mean establish the falsity of) most of the statements given above. Before we do this, we need to be sure that we really know precisely what all the statements mean. We already said what we mean by the 'natural numbers', and I assume you know what the algebra means (i.e. that n^2 means n multipled by n, and so on). We haven't formally defined 'divisible', though, and you might not have seen this in school. So we need to do that:

Let us say that a natural number n is *divisible* by a natural number d if we can write $n = d \cdot k$ for some natural number k. We say that a natural number is *even* if it is divisible by 2, and *odd* if it is not.

Note that saying n is divisible by d is the same thing as saying that if we try to divide n by d we get no remainder. This definition is probably what you thought 'divisible' meant when you read the statements in the previous section—now you know you were right, and you know everyone else will (by definition!) agree with you. For the rest of your degree, we'll assume you know what 'divisible' means, and the meaning

[1] Usually we say that a natural number which is equal to the sum of all smaller positive numbers which divide it is *perfect*. The reason for using 'nice' in the text is because that term is not commonly defined!

will not be changed. We might say 'divisible means when we try to divide we get no remainder', or some other phrase which has the same mathematical meaning: the precise words aren't important. What is important is that the mathematical meaning is now fixed.

Now that we're all clear on exactly what the statements mean, let's prove them.

(a) 20 is divisible by 4.

This statement is true. Since $20 = 5 \times 4$, we see that (by the definition) 20 is divisible by 4. And that's a proof! It's utterly convincing, watertight, and not open to debate. Nobody can argue with it, not even a sociologist! Isn't this fun? Well, maybe it's not that impressive in such a simple situation, but we will certainly prove more impressive results later.

(b) 21 is not divisible by 7.

This is false. It's false because 21 *is* divisible by 7, because $21 = 3 \times 7$.

(c) 21 is divisible by 4.

This is false, as can be established in a number of ways. First, we note that if the natural number m satisfies $m \leq 5$, then $m \times 4$ will be no more than 20. And if $m \geq 6$ then $m \times 4$ will be at least 24. Well, any natural number m is either at most 5 or at least 6 so, for all possible m, we do not have $m \times 4 = 21$ and hence there is no natural number m for which $m \times 4 = 21$. In other words, 21 is not divisible by 4. Another argument (which is perhaps more straightforward, but which relies on properties of rational numbers rather than just simple properties of natural numbers) is to note that $21/4 = 5.25$, and this is not a natural number, so 21 is not divisible by 4. (This second approach is the same as showing that 21 has remainder 1, not 0, when we divide by 4.)

Most of you are probably completely happy with these proofs. Maybe one or two of you would like to know things like: why is there no natural number between 5 and 6? Do we need to prove it? We'll get to that in the next chapter.

(d) 21 is divisible by 3 or 5.

As we noted above, this is a compound statement. It is true precisely if one (or both) of the following statements is true:

(i) 21 is divisible by 3

(ii) 21 is divisible by 5.

Statement (i) is true, because $21 = 7 \times 3$. Statement (ii) is false. Because at least one of these two statements is true, statement (d) is true.

(e) 50 is divisible by 2 and 5.

This is true. Again, this is a compound statement and it is true precisely if *both* of the following statements are true:

(i) 50 is divisible by 2

(ii) 50 is divisible by 5.

Statements (i) and (ii) are indeed true because $50 = 25 \times 2$ and $50 = 10 \times 5$. So statement (e) is true.

(f) n^2 is even

As mentioned above, whether this is true or false depends on the value of n. For example, if $n = 2$ then $n^2 = 4$ is even, but if $n = 3$ then $n^2 = 9$ is odd. So, unlike the other statements (which are *propositions*), this is a *predicate* $P(n)$. The predicate will become a proposition when we assign a particular value to n to it, and the truth or falsity of the proposition can then be established. You probably implicitly assume that n has to be a natural number, but there isn't actually anything in the statement to tell you that—maybe n is a matrix, in which case it's not even clear what 'even' should mean for a matrix (we only defined 'even' for natural numbers). If we assume n is a natural number, then (i) and (j) cover all the possibilities.

(g) For every natural number n, the number $n^2 + n$ is even

Here's our first non-immediate, non-trivial, proof. How on earth can we prove this, if it is true, or disprove it, if it is false? Suppose it was false. How would you convince someone of that? Well, the statement says that *for every* natural number n, $n^2 + n$ is even. So if you managed (somehow!) to find a particular N for which $N^2 + N$ happened to be odd, you could prove the statement false by simply observing that 'When $n = N$, it is *not* the case that $n^2 + n$ is even.' And that would be the end of it. So, in other words, if a universal statement about natural numbers is false, you can prove it is false by showing that its conclusion is false for *some particular* value of n. But suppose the statement is true. How could you prove it. Well, you could prove it for $n = 1$, then $n = 2$, then $n = 3$, and so on, but at some point you would expire and there would still be numbers n that you hadn't yet proved it for. And that simply wouldn't do, because if you proved it true for the first 9999 numbers, it might be false when $n = 10000$. So what you need is a more sophisticated, *general* argument that shows the statement is true for any *arbitrary* n.

Now, it turns out that this statement is true. So we need a nice general argument to establish this. Well, here's one approach. We can note that $n^2 + n = n(n + 1)$. The numbers n and $n + 1$ are consecutive natural numbers. So one of them is odd and one of them is even. When you multiply any odd number and any even number together, you get an even number, so $n^2 + n$ is even. Are you convinced? Maybe not? We really should be more explicit. Suppose n is even. What that means is that, for some integer k, $n = 2k$. Then $n + 1 = 2k + 1$ and hence

$$n(n + 1) = 2k(2k + 1) = 2\left(k(2k + 1)\right).$$

Because $k(2k + 1)$ is an integer, this shows that $n^2 + n = n(n + 1)$ is divisible by 2; that is, it is even. We supposed here that n was even. But it might be odd, in which case we would have $n = 2k + 1$ for some integer k. Then

$$n(n + 1) = (2k + 1)(2k + 2) = 2\left((2k + 1)(k + 1)\right),$$

which is, again, even, because $(2k + 1)(k + 1)$ is an integer.

Right, we're really proving things now. This is a very general statement, asserting something about *all* natural numbers, and we have managed to prove it. I find that quite satisfying, don't you?

(h) There is a natural number n such that $2n = 2^n$.

This is an *existential statement*, asserting that *there exists* n with $2n = 2^n$. Before diving in, let's pause for a moment and think about how we might deal with such statements. If an existential statement like this is true we would need only to show that its conclusion (which in this case is $2n = 2^n$) holds for some particular n. That is, we need only find an n that works. If the statement is false, we have a lot more work to do in order to prove that it is false. For, to show that it is false, we would need to show that, for *no* value of n does the conclusion holds. Equivalently, for *every* n, the conclusion fails. So we'd need to prove a universal statement and, as we saw in the previous example, that would require us to come up with a suitably general argument.

In fact, this statement is true. This is because when $n = 1$ we have $2n = 2 = 2^1 = 2^n$; we're done.

We could also use $n = 2$ to prove this statement is true: we have $2n = 2 \cdot 2 = 4 = 2^2 = 2^n$. But to prove an existential statement to be true, it's enough to find one example; once we saw $n = 1$ is such an example, we don't need to care that $n = 2$ is also an example.

(i) If n is even, then n^2 is even

This is true. The most straightforward way to prove this is to assume that n is some (that is, *any*) even number and then show that n^2 is even. So suppose n is even. Then $n = 2k$ for some integer k (by definition) and hence $n^2 = (2k)^2 = 4k^2$. This is even because it is $2(2k^2)$ and $2k^2$ is an integer.

(j) For all odd numbers n, n^2 is odd.

This is true. The most straightforward way to prove this is to assume that n is *any* odd number and then show that n^2 is also odd. So suppose n is odd. Then $n = 2k + 1$ for some integer k and hence $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. To establish that this is odd, we need to show that it can be written in the form $2K + 1$ for some integer K. Well, $4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. This is indeed of the form $2K + 1$, where K is the integer $2k^2 + 2k$. Hence n^2 is odd.

Another way to prove this result is to prove that if n^2 is even then n must be even. We won't do that right now, because to do it properly requires a result we meet later concerning the factorisation of numbers into prime numbers. But think about the strategy for a moment. Suppose we were able to prove the following statement, which we'll call Q:

Q: *if* n^2 is even *then* n is even.

Why would that establish what we want (namely that if n is odd then n^2 is odd). Well, one way is to observe that Q is what's called the *contrapositive* of statement (j) that we're trying to prove, and the contrapositive is *logically equivalent* to the initial statement. (This is a bit of formal logic, and we will discuss this more later). But there's another way of thinking about it, which is perhaps easier to understand at this stage. Suppose we have proved statement Q and suppose that n is odd. Then it must be the case that n^2 is odd. For, if n^2 was not odd, it would be even and then Q would tell us that this means n is even. But we have assumed n is odd. It cannot be both even and odd, so we have reached a contradiction. By

assuming that the opposite conclusion holds (n^2 even) we have shown that something impossible happens. This type of argument is known as a *proof by contradiction* and it is often very powerful. We will see more about this later.

(k) For natural numbers n, n^2 is even if and only if n is even.

This is true. What we have shown in proving (i) and (j) is that if n is even then n^2 is even, and if n is odd then n^2 is odd. The first, (statement (i)) establishes that *if* n is even, then n^2 is even. The second of these (statement (j)) establishes that n^2 is even *only if* n is even. This is because it shows that n^2 is odd if n is odd, from which it follows that if n^2 is even, n must not have been odd, and therefore must have been even. 'If and only if' statements if this type are very important. As we see here, the proof of such statements breaks down into the proof of two 'If-then' statements.

(l) There are no natural numbers m and n such that $\sqrt{2} = m/n$.

This is, in fact, true, though we defer the proof for now, until we know more about factorisation of numbers into prime numbers. We merely comment that the easiest way to prove the statement is to use a proof by contradiction.

These examples hopefully demonstrate that there are a wide range of statements and proof techniques, and in the rest of this chapter we will explore these further.

Right now, one thing I hope comes out very clearly from these examples is that to prove a mathematical statement, you need to know precisely what it means. Well, that sounds obvious, but you can see how detailed we had to be about the meanings (that is, the *definitions*) of the terms 'divisible', 'even' and 'odd'. Definitions are very important.

2.3 Some basic logic

Mathematical statements can be true or false. Let's denote 'true' by T and 'false' by F. Given a statement, or a number of statements, it is possible to form other statements. This was indicated in some of the examples above (such as the compound statements). A technique known as the use of 'truth tables' enables us to define 'logical operations' on statements, and to determine when such statements are true. This is all a bit vague, so let's get down to some concrete examples.

2.3.1 Negation

The simplest way to take a statement and form another statement is to *negate* the statement. The *negation* of a statement P is the statement $\neg P$ (sometimes just denoted 'not P'), which is defined to be true exactly when P is false. This can be described in the very simple truth table, Table 2.1:

P	$\neg P$
T	F
F	T

Table 2.1: The truth table for 'negation' or 'not'

What does the table signify? Quite simply, it tells us that if P is true then $\neg P$ is false and if P is false then $\neg P$ is true.

> **Example 2.1** If P is '20 is divisible by 3' then $\neg P$ is '20 is not divisible by 3'. Here, P is false and $\neg P$ is true.

It has, I hope, been indicated in the examples earlier in this chapter, that to disprove a universal statement about natural numbers amounts to proving an existential statement. That is, if we want to disprove a statement of the form 'for all natural numbers n, property $p(n)$ holds' (where $p(n)$ is some predicate, such as 'n^2 is even') we need only produce some N for which $p(N)$ fails. Such an N is called a *counterexample*. Equally, to disprove an existential statement of the form 'there is some n such that property $p(n)$ holds', one would have to show that for *every* n, $p(n)$ fails. That is, to disprove an existential statement amounts to proving a universal one. But, now that we have the notion of the negation of a statement we can phrase this a little more formally. Proving that a statement P is false is equivalent to proving that the negation $\neg P$ is true. In the language of logic, therefore, we have the following:

- The negation of a universal statement is an existential statement.
- The negation of an existential statement is a universal statement.

More precisely,

- The negation of the universal statement 'for all n, property $p(n)$ holds' is the existential statement 'there is n such that property $p(n)$ does not hold'.
- The negation of the existential statement 'there is n such that property $p(n)$ holds' is the universal statement 'for all n, property $p(n)$ does not hold'.

We could be a little more formal about this, by defining the negation of a predicate $p(n)$ (which, recall, only has a definitive true or false value once n is specified) to be the predicate $\neg p(n)$ which is true (for any particular n) precisely when $p(n)$ is false. Then we might say that

- The negation of the universal statement 'for all n, the statement $p(n)$ is true' is the existential statement 'there is n such that $\neg p(n)$ is true'.
- The negation of the existential statement 'there is n such that $p(n)$ is true' is the universal statement 'for all n, the statement $\neg p(n)$ is true'.

Now, let's not get confused here. None of this is really difficult or new. We meet such logic in everyday life. If I say 'It rains every day in London' then either this statement is true or it is false. If it is false, it is because on (at least) one day it does not rain. The

negation (or disproof) of the statement 'On every day, it rains in London' is simply 'There is a day on which it does not rain in London'. The former is a universal statement ('On every day, . . . ') and the latter is an existential statement ('there is a day . . . '). Or, consider the statement 'There is a student who enjoys reading these lecture notes'. This is an existential statement ('There is . . . '). This is false if 'No student enjoys reading these lecture notes'. Another way of phrasing this last statement is 'Every student reading these lecture notes does not enjoy it'. This is a more awkward expression, but it emphasises that the negation of the initial, existential statement, is a universal one ('Every student . . . ').

The former is an existential statement ('there is something I will write that . . . ') and the latter is a universal statement ('everything I write will . . .). This second example is a little more complicated, but it serves to illustrate the point that much of logic is simple common sense.

2.3.2 Conjunction and disjunction

There are two very basic ways of combining propositions: through the use of 'and' (known as conjunction) and the use of 'or' (known as disjunction).

Suppose that P and Q are two mathematical statements. Then 'P and Q', also denoted $P \wedge Q$, and called the *conjunction* of P and Q, is the statement that is true precisely when *both* P and Q are true. For example, statement (e) above, which is

'50 is divisible by 2 and 5'

is the conjunction of the two statements

- 50 is divisible by 2
- 50 is divisible by 5.

Statement (e) is true because *both* of these two statements are true.

Table 2.2 gives the truth table for the conjunction P and Q:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2.2: The truth table for 'and'

What Table 2.2 says is simply that $P \wedge Q$ is true precisely when *both* P and Q are true (and in no other circumstances).

Suppose that P and Q are two mathematical statements. Then 'P or Q', also denoted $P \vee Q$, and called the *disjunction* of P and Q, is the statement that is true precisely when P, or Q, or both, are true. For example, statement (d) above, which is

'21 is divisible by 3 or 5'

is the disjunction of the two statements

- 21 is divisible by 3
- 21 is divisible by 5.

Statement (d) is true because at least one (namely the first) of these two statements is true.

Note one important thing about the mathematical interpretation of the word 'or'. It is *always* used in the 'inclusive-or' sense. So $P \vee Q$ is true in the case when P is true, or Q is true, or *both*. In some ways, this use of the word 'or' contrasts with its use in normal everyday language, where it is often used to specify a choice between mutually exclusive alternatives. (For example 'You're either with us or against us'.) But if I say 'Tomorrow I will wear brown trousers or I will wear a yellow shirt' then, in the mathematical way in which the word 'or' is used, the statement would be true if I wore brown trousers and any shirt, any trousers and a yellow shirt, and also if I wore brown trousers and a yellow shirt. You might have your doubts about my dress sense in this last case, but, logically, it makes my statement true.

Table 2.2 gives the truth table for the disjunction P and Q:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 2.3: The truth table for 'or'

What Table 2.3 says is simply that $P \vee Q$ is true precisely when *at least one of* P and Q is true.

2.4 If-then statements

It is very important to understand the formal meaning of the word 'if' in mathematics. The word is often used rather sloppily in everyday life, but has a very precise mathematical meaning. Let me give you an example. Suppose I tell you 'If it rains, then I wear a raincoat', and suppose that this is a true statement. Well, then, suppose it rains. You can certainly conclude I will wear a raincoat. But what if it does not rain? Well, you can't conclude anything. My statement only tells you about what happens *if* it rains. If it does not, then I might, or I might not, wear a raincoat: and whether I do or not does not affect the truth of the statement I made. You have to be clear about this: an 'if-then' statement only tells you about what follows *if* something particular happens.

More formally, suppose P and Q are mathematical statements (each of which can therefore be either true or false). Then we can form the statement denoted $P \Rightarrow Q$ ('P implies Q' or, equivalently, 'if P, then Q'), which has as its truth table Table 2.4. (This type of statement is known as an *if-then* statement or an *implication*.)

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

Table 2.4: The truth table for '$P \Rightarrow Q$'

Note that the statement $P \Rightarrow Q$ is false only when P is true but Q is false. (To go back to the previous example, the statement 'If it rains, I wear a raincoat' is false precisely if it does rain but I do not wear a raincoat.) This is tricky, so you may have to spend a little time understanding it. As I've suggested, perhaps the easiest way is to think about when a statement 'if P, then Q' is false.

The statement $P \Rightarrow Q$ can also be written as $Q \Leftarrow P$. There are different ways of describing $P \Rightarrow Q$, such as:

- if P then Q
- P implies Q
- P is sufficient for Q
- Q if P
- P only if Q
- Q whenever P
- Q is necessary for P.

All these mean the same thing. The first two are the ones I will use most frequently.

If $P \Rightarrow Q$ and $Q \Rightarrow P$ then this means that Q will be true precisely when P is. That is Q is true *if and only if* P is. We use the single piece of notation $P \Longleftrightarrow Q$ instead of the two separate $P \Rightarrow Q$ and $Q \Leftarrow P$. There are several phrases for describing what $P \Longleftrightarrow Q$ means, such as:

- P if and only if Q (sometimes abbreviated to 'P iff Q')
- P is equivalent to Q
- P is necessary and sufficient for Q
- Q is necessary and sufficient for P.

The truth table is shown in Table 2.5, where we have also indicated the truth or falsity of $P \Rightarrow Q$ and $Q \Rightarrow P$ to emphasise that $P \Longleftrightarrow Q$ is the same as the conjunction $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \iff Q$
T	**T**	T	T	**T**
T	**F**	F	T	**F**
F	**T**	T	F	**F**
F	**F**	T	T	**T**

Table 2.5: The truth table for '$P \iff Q$'

What the table shows is that $P \iff Q$ is true precisely when P and Q are either both true or both false.

> **Activity 2.1** Look carefully at the truth table and understand why the values for $P \iff Q$ are as they are. In particular, try to explain in words why the truth table is the way it is.

2.5 Logical equivalence

Two statements are *logically equivalent* if when either one is true, so is the other, and if either one is false, so is the other. For example, for statements P and Q, the statements $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent. We can see this from the truth table, Table 2.6, which shows that, in all cases, the two statements take the same logical value T or F). (This value is highlighted in bold.)

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$
T	T	T	**F**	F	F	**F**
T	F	T	**F**	F	T	**F**
F	T	T	**F**	T	F	**F**
F	F	F	**T**	T	T	**T**

Table 2.6: The truth tables for $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$

The fact that $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent is quite easy to understand. The statement $P \vee Q$ is true if and only if at least one of P, Q is true. The statement is therefore false precisely when *both* P and Q are false, which means $\neg P$ and $\neg Q$ are both true, which means $\neg P \wedge \neg Q$ is true. Again, we can understand these things fairly easily with some common sense. If I tell you 'I will wear brown trousers or I will wear a yellow shirt' then this is a false statement only if I *do not* wear brown trousers *and* I *do not* wear a yellow shirt.

Now that we know the meaning of $\iff$, we can see that to say that $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent is to say that $\neg(P \vee Q) \iff \neg P \wedge \neg Q$.

> **Activity 2.2** Show that the statements $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent. [This shows that the negation of $P \wedge Q$ is $\neg P \vee \neg Q$. That is, $\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$.]

2.6 Converse statements

Given an implication $P \Rightarrow Q$, the 'reverse' implication $Q \Rightarrow P$ is known as its *converse*. Generally, there is no reason why the converse should be true just because the implication is. For example, consider the statement 'If it is Tuesday, then I buy the Guardian newspaper.' The converse is 'If I buy the Guardian newspaper, then it is Tuesday'. Well, I might buy that newspaper on other days too, in which case the implication can be true but the converse false. We've seen, in fact, that if both $P \Rightarrow Q$ and $Q \Rightarrow P$ then we have a special notation, $P \Longleftrightarrow Q$, for this situation. Generally, then, the truth or falsity of the converse $Q \Rightarrow P$ has to be determined separately from that of the implication $P \Rightarrow Q$.

> **Activity 2.3** What is the converse of the statement 'if the natural number n divides 4 then n divides 12'? Is the converse true? Is the original statement true?

2.7 Contrapositive statements

The *contrapositive* of an implication $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$. The contrapositive is logically equivalent to the implication, as Table 2.7 shows. (The columns highlighted in bold are identical.)

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	**T**	F	F	**T**
T	F	**F**	F	T	**F**
F	T	**T**	T	F	**T**
F	F	**T**	T	T	**T**

Table 2.7: The truth tables for $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$.

If you think about it, the equivalence of the implication and its contrapositive makes sense. For, $\neg Q \Rightarrow \neg P$ says that if Q is false, P is false also. So, it tells us that we cannot have Q false and P true, which is precisely the same information as is given by $P \Rightarrow Q$.

So what's the point of this? Well, sometimes you might want to prove $P \Rightarrow Q$ and it will, in fact, be easier to prove instead the equivalent (contrapositive) statement $\neg Q \Rightarrow \neg P$. We will see many examples of this through your degree—for now, see Biggs, section 3.5 for an example.

2.8 What is a proof?

You should probably have some idea of what a proof is by now: you start with some statements you're assuming to be true (usually called *axioms*), from these statements you deduce others (using the rules of logic) and eventually you get to the statement

you wanted to prove. If you are being very formal, you should write down every single step.

If you write down every single step, you're in a great position if someone wants to argue with your proof. If someone doesn't agree with your conclusion—the statement you're proving—it's their problem to find a mistake in your proof. That means they have to point at some statement in your proof and say that they do not believe it. Now there are two sorts of statements in your proof: ones which follow logically from earlier statements, and your axioms. If the doubter says they don't believe something which follows logically from earlier statements, then they have to point at one of these earlier statements and say they don't like that one either (or they tell you they don't believe in logic, in which case you can safely stop listening). Eventually they will either be convinced you were right all along, or they will get back to one of your axioms and say they disagree with that. Now, if you have some strange non-standard axiom, then there might even be a good reason to argue. But if you stick to standard axioms, like 'addition of natural numbers is commutative', then no-one is going to argue—which means you will convince everyone that what you claim is true. This is the gold standard of proof.

The problem with writing down every single step is that it takes a very long time to actually get anywhere. Look back to the proof on page 8—it takes eight lines to do a piece of algebra which you would normally write out in one line, and even that proof skips the steps of proving from axioms that $2 \times 2 = 2 + 2 = 4$ (which we'll see how to do in the next chapter). You don't want to spend the next three years taking pages and pages to write out simple algebra, so we need to agree on a way to write proofs which is shorter. There are two ways to do this, and we will use both.

The first way is that, as we go through the course (and the degree) we will make for ourselves a library of true statements—ones which we already proved—and we will not repeat the proofs every time we want to use them. So, for example, we already proved that for every natural number n, the number $n^2 + n$ is even (We didn't really write out every single step—if you don't like that, try doing it yourself). Next time we want to know that $n^2 + n$ is even for some natural number n, we won't need to prove it, we can just say 'proved in MA103'. There's nothing much anyone can object to here—it's clear that we could have written out a gold standard proof just by copying-and-pasting in the proof from MA103.

The second way we will save time is by not writing out every single step. When you need to do a piece of algebra, do it just as you did in school, and we will assume you do know how to justify all the steps by going back to the axioms (or at least that you know where to look in order to find out how). We will also sometimes save steps by saying that something is 'obvious', or 'clear'. When you (or I) write 'obvious' or 'clear' in a proof, it is there to tell the reader that there are some steps missing, that you (or I) know what those steps are, and that the reader should have no trouble figuring out what the missing steps are. What this also means is: **if you cannot explain why a statement is true, then you cannot write that it is 'obvious' in a proof**. You will need to make a judgement of how many steps it is OK to skip.

You will quickly get used to what is and what is not acceptable as a proof—assuming you do the weekly exercises—because your class teacher will correct you. What you should keep in mind is that whatever you write as a proof should be something

which you could expand out to a gold standard proof if you were forced to, either from memory or because you know where to look for the missing pieces and previously proved statements.

As we go on, those 'missing pieces and previously proved statements' will get pretty long: there will be proofs you write later this year in a page or two which might take a hundred or more pages to write out in 'gold standard' style. For an example (which you shouldn't expect to understand when you read this the first time; but it will make sense when you're revising) think about how to prove that a piece of simple algebra with the rational numbers makes sense, in terms of the axioms for the natural numbers. We prove in this course that you can do it (which is enough—if I know something is possible, I don't have to actually do it to check it works)—but try actually doing it!

2.9 Working backwards to obtain a proof

As you will see in this course, it is not easy to prove statements. On occasion, you may be asked to prove some statement which you can simply look at and immediately an idea comes to your mind of what you have to write down to prove it. Usually, that's not going to be the case. You need to try different strategies. There isn't any universal method which works — at least, if there is humanity has not found it — but there are some strategies which can help. Here is one of them.

We've already seen, in the examples earlier in this chapter, how some statements may be proved directly. For example, in order to prove a universal statement 'for all n, $P(n)$' about natural numbers, we would need to provide a proof that starts by assuming that n is any given (that is, *arbitrary*) natural number and show the desired conclusion holds. To disprove such a statement (which is the same as proving its negation), we would simply need to find a single value of n for which $P(n)$ is false (and such an n is known as a *counterexample*).

However, some statements are difficult to prove directly. It is sometimes easier to 'work backwards'. Suppose you are asked to prove something, such as an inequality or equation. It might be easier to see how to do so if the end-result (the inequality or equation you are required to prove) is simplified, or expanded, or re-written in some way. Here's an example.

Example 2.2 Prove the statement that: 'if a, b are real numbers and $a \neq b$, then $ab < (a^2 + b^2)/2$'.

It's certainly not immediately obvious how to approach this. But let's start with what we want to prove. This is the inequality $ab < (a^2 + b^2)/2$, which can be rewritten as $a^2 + b^2 - 2ab > 0$. Now, this can be simplified as $(a - b)^2 > 0$ and maybe now you can see why it is true: the given fact that $a \neq b$ means that $a - b \neq 0$ and hence $(a - b)^2$ is a positive number. So we see why the statement is true. To write down a nice proof, we can now reverse this argument, as follows:

Proof Since $a \neq b$, $a - b \neq 0$ and, hence, $(a - b)^2 > 0$. But $(a - b)^2 = a^2 + b^2 - 2ab$. So we have $a^2 + b^2 > 2ab$ and, therefore, $ab < (a^2 + b^2)/2$, as required. □

There are a few things to note here. First, mathematics is a language and what you write has to make good sense. Often, it is tempting to make too much use of symbols rather than words. But the words used in this proof, and the punctuation, make it easy to read and give it a structure and an argument. You should find yourself using words like 'so, 'hence', 'therefore, 'since', 'because', and so on. *Do* use words and punctuation and, whatever you do, do not replace them by symbols of your own invention! Also do not use the symbols '$\therefore$' and '$\because$'. You may have seen these in school, but they make your work hard to read. Write the English words instead! A second thing to note is the use of the symbol '□'. There is nothing particularly special about this symbol: others could be used. What it achieves is that it indicates that the proof is finished. There is no need to use such a symbol, but you will find that textbooks do make much use of symbols to indicate when proofs have ended. It makes the reader's life easier: when you see the □ symbol, you know that you are meant to be convinced and that what follows will be a comment, or the next piece of material. Otherwise you might be left wondering whether the proof is finished yet.

The final, very important, thing to note is that even if you work backwards to get a proof, *you need to write it down forwards*. Otherwise you do *not* have a proof.

2.10 What is not a proof?

There are several common mistakes made by students when they are asked to prove something. Some of the most common are:

(1) The goose's mistake: 'proof by example'. In January, a goose hatches from an egg. Every day, the farmer feeds it. Towards the middle of December, the goose is sure that it will be fed every day forever...

Whenever you are supposed to prove 'for all...' statements, you need to do *all* the cases not one or two; whenever you want a counterexample to 'there exists...' statements, than means you have to show *all* the possibilities fail, not just that the most obvious one fails. This probably sounds obvious written out like this, but nevertheless probably about half of you will make the goose's mistake at some point.

(2) The ends justify the means. You are in a park and buy an ice-cream; a small child snatches it away from you. In the end, you will get your ice-cream back—explain how.

That means: write a story. The first and last lines are given: 'You are in a park and buy an ice-cream; a small child snatches it away from you' and 'You get your ice-cream back'. What's in the middle is important. Maybe it's 'You have a long discussion of comparative morality with the child. It realises the error of its ways'.

You're used to 'doing maths' meaning making a calculation, and the point of a calculation is to 'get the right answer'. Now, of course, it can happen that you make two mistakes in a calculation which happen to cancel out and you get the right answer even though you made mistakes—but you have to be really lucky for that to happen. Normally, if you make mistakes you get the wrong answer. So you're used to thinking (maybe subconsciously) that if the last line is right, then everything else was probably also good.

We're not doing calculations in this course, though, we're doing proofs. When you write a proof, you usually know the first and last lines before anything else: the first line is what you're assuming, and the last line is what you want to prove. What is important is actually what's in the middle which explains why the last line is true. If (when) you get a proof back from your class teacher marked as wrong even though 'the answer is right', before complaining, think: does it make a difference to the story if the middle line is instead 'You pull out your gun and shoot the child'?

(3) Working in reverse to obtain a proof but then not writing the proof out forwards. For example, consider trying to prove the following trigonometric identity: for all $x \in \mathbb{R}$, we have

$$(\cos x)^2 - \sin x = 1 - (\sin x)^2 + \sin x\,. \tag{2.1}$$

If you just work in reverse, your proof might be:

Proof.

We want	$(\cos x)^2 - \sin x = 1 - (\sin x)^2 + \sin x$		
so	$-\sin x = 1 - (\sin x)^2 + \sin x - (\cos x)^2$		subtracting $(\cos x)^2$
so	$(\sin x)^2 = \big(1 - (\sin x)^2 + \sin x - (\cos x)^2\big)^2$		squaring both sides
so	$0 = (1 - 1 + \sin x)^2 - (\sin x)^2 = 0$		adding $(\sin x)^2$,

where to get to the last line we used the identity $(\sin x)^2 + (\cos x)^2 = 1$, which holds for all $x \in \mathbb{R}$. The last line is true, so we are done. □

Note that normally you wouldn't write justifications for each line of simple algebra—it's obvious enough how we got from each line to the next—but I wanted to do this here for extra clarity.

This is *not* a valid proof—what it shows is that *if* the identity we want to prove, (2.1), holds, *then* $0 = 0$, which is a true statement. But a proof is supposed to *end* with the statement you want to prove, not start with it.

That might seem picky—after all, it looks pretty much like what we did in Example 2.2, just we didn't bother to reverse the argument so the statement we want is at the end. Well, let's try reversing it.

Proof, take 2. We have

	$0 = (1 - 1 + \sin x)^2 - (\sin x)^2$		
so	$(\sin x)^2 = (1 - 1 + \sin x)^2$		subtracting $(\sin x)^2$
so	$(\sin x)^2 = \big(1 - (\sin x)^2 + \sin x - (\cos x)^2\big)^2$		since $1 = (\sin x)^2 + (\cos x)^2$
so	$-\sin x = 1 - (\sin x)^2 + \sin x - (\cos x)^2$		taking square roots
so	$(\cos x)^2 - \sin x = 1 - (\sin x)^2 + \sin x$		adding $(\cos x)^2$

which is what we wanted to prove. □

Looks better—but wait! The first two 'so's are fine, but the third 'so', 'taking square roots', boils down to 'If $a^2 = b^2$ then $a = b$' — and that's not true; it could equally

well be that $a = -b$. There is a problem with the proof here — and the reason is that we are trying to prove a *false statement*! In fact,

$$(\cos \tfrac{\pi}{2})^2 - \sin \tfrac{\pi}{2} = 0^2 - 1 = -1 \quad \text{but} \quad 1 - (\sin \tfrac{\pi}{2})^2 + \sin \tfrac{\pi}{2} = 1 - 1^2 + 1 = 1\,.$$

so the 'identity' simply isn't true.

What you should learn from this example is that it is not being picky to insist on writing arguments (especially calculations with algebra) properly so that the statement to be proved comes at the end not the beginning. It is very easy to do some operation to both sides which is not reversible—in this example, squaring—without noticing and 'prove' a false statement. If you write a proof properly, i.e. forwards, then you are more likely to notice a potential problem.

2.11 Sets

2.11.1 Basics

You have probably already met some basic ideas about sets and there is not too much more to add at this stage, but they are such an important idea in abstract mathematics that they are worth discussing here.

Loosely speaking, a set may be thought of as a collection of objects. A set is usually described by listing or describing its *members*, or *elements*, inside curly brackets. For example, when we write $A = \{1, 2, 3\}$, we mean that the objects belonging to the set A are the numbers $1, 2, 3$ (or, equivalently, the set A consists of the numbers $1, 2$ and 3). Equally (and this is what we mean by 'describing' its members), this set could have been written as

$$A = \{n \mid n \text{ is a whole number and } 1 \leq n \leq 3\}.$$

Here, the symbol $\mid$ stands for 'such that'. Often, the symbol ':' is used instead, so that we might write

$$A = \{n : n \text{ is a whole number and } 1 \leq n \leq 3\}.$$

When x is an object in a set A, we write $x \in A$ and say 'x belongs to A', or 'x is in A', or 'x is a member of A'. If x is not in A we write $x \notin A$.

As another example, the set

$$B = \{x \in \mathbb{N} \mid x \text{ is even}\}$$

has as its members the set of positive even integers. Here we are specifying the set by *describing* the defining property of its members.

One point which is important is that it doesn't make sense to say that an object is in a set twice. It's either in or not, and this is the end. We'll avoid writing obvious repetitions, like $S = \{1, 2, 3, 1\}$. That *is* a set, and it is the same as the set $\{1, 2, 3\}$; whichever way I write it, it contains 1, 2 and 3 and nothing else. But sometimes it will be painful to write a description avoiding repetition.

Sometimes it is useful to give a *constructional* description of a set. For example, $C = \{n^2 \mid n \in \mathbb{N}\}$ is the set of natural numbers known as the 'perfect squares'.

We could also write $D = \{z^2 \mid z \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of all (not just positive) integers. The difference between C and D is simple: D contains 0 and C does not. That's the only difference. By definition $(-3)^2 = 9$ is in D, but it is also in C, because $3^2 = 9$ is by definition in C. It doesn't matter that our definition of D repeats some elements (like $9 = (-3)^2 = 3^2$).

The set which has no members is called the *empty set* and is denoted by $\emptyset$. The empty set may seem like a strange concept, but it is useful to define. Think about lengths—'zero centimetres' is a funny length, but if we didn't want to use it, we would have trouble with the question 'How much longer is a metre than 100 centimetres?'.

2.11.2 Subsets

We say that the set S is a *subset* of the set T, and we write $S \subseteq T$, if every member of S is a member of T. For example, $\{1, 2, 5\} \subseteq \{1, 2, 4, 5, 6, 40\}$. (Be aware that some texts use $\subset$ where we use $\subseteq$.) What this means is that the statement

$$x \in S \Rightarrow x \in T$$

is true.

A rather obvious, but sometimes useful, observation is that, given two sets A and B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. So to prove two sets are equal, we can prove that each of these two 'containments' holds. That might seem clumsy, but it is, in many cases, the best approach.

For any set A, the empty set, $\emptyset$, is a subset of A. You might think this is strange, because what it means is that 'every member of $\emptyset$ is also a member of A'. But $\emptyset$ has no members—how can that be true? Let's go back to the logic: 'every member of $\emptyset$ is also a member of A' means 'for each x, if x in $\emptyset$ then $x \in A$'. Check the truth table of if—then ($\Rightarrow$). The only way some x can be a counterexample to this statement is if x is in $\emptyset$ and not in A. But there is no x such that $x \in \emptyset$, by definition—so we proved $\emptyset \subseteq A$.

2.11.3 Health warning

It's very easy to get confused about what sets are equal, what are members and what are subsets of a set. I'm about to give an example, which right now will look like a deliberate attempt to trick you. But things like this will show up later, not as a trick, and you need to get it right.

Consider the set $S = \{0, 1, \{0, 1\}, \{2\}\}$. What are its members and subsets? Well, 0 is a member. And so is 1, and so is $\{0, 1\}$, and so is $\{2\}$. But 2 is not a member of S. Furthermore, $\{0, 1\}$ is a subset of S (because 0 and 1 are both members of S) and so is $\{\{0, 1\}\}$. These are two different sets — $\{0, 1\} \neq \{\{0, 1\}\}$. And there are some other subsets of S too — try to write them all out; you should get 16 in total.

If you don't like the statements above, maybe think of it this way. Any

(mathematical) object can go in a set, so the number 1 can go in, or a function can go in, or even another set. This is just the same thing as saying that you can put a (normal) object in a parcel, so an apple can go in a parcel, or an orange can go in a parcel, or a parcel full of sweets can go in another parcel, and so on. If you think a parcel containing a parcel full of sweets is the same as a parcel full of sweets (or it's the same as just having a lot of sweets), think back to childhood games of Pass-the-Parcel. Just like that game, it really matters how many of the { and } set brackets there are, and what exactly they go round.

2.11.4 Unions and intersections

Given two sets A and B, the *union* $A \cup B$ is the set whose members belong to A or B (or both A and B): that is,

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

Equivalently, to use the notation we've learned,

$$x \in A \cup B \iff (x \in A) \vee (x \in B).$$

Example 2.3 If $A = \{1, 2, 3, 5\}$ and $B = \{2, 4, 5, 7\}$, then $A \cup B = \{1, 2, 3, 4, 5, 7\}$.

Similarly, we define the *intersection* $A \cap B$ to be the set whose members belong to both A and B:

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

So,

$$x \in A \cap B \iff (x \in A) \wedge (x \in B).$$

2.11.5 Arbitrary unions and intersections

Often we will want to take the union of a lot of sets, for example $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. This is a pain to write out in this way, and if we wanted to take the union of infinitely many sets, we wouldn't be able to do it at all. So we define a notation which lets us write such a thing easily.

Suppose that I is a set, which we will call the *index set*, and that for each $i \in I$ we have some set A_i (so in the example above, $I = \{1, 2, 3, 4, 5\}$). Then we define the *arbitrary union*

$$\bigcup_{i \in I} A_i$$

for the set

$$\left\{x \mid x \in A_i \text{ for at least one } i \in I\right\}.$$

Similarly, we define the *arbitrary intersection*

$$\bigcap_{i \in I} A_i$$

for the set

$$\{x \mid x \in A_i \text{ for all } i \in I\}.$$

You should check for yourself that

$$\bigcup_{i \in \{1,2,3,4,5\}} A_i$$

really defines the same set as $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$, and similarly with the arbitrary intersection.

One final warning: what do these definitions mean if $I = \emptyset$? It's not very obvious, and we need to talk about *universal sets* to understand it. We'll get back to this later; for now, just think of $\bigcup$ as a convenient way to avoid writing a long string of $\cup$s.

2.11.6 Universal sets and complements

We've been a little informal about what the possible 'objects' in a set might be. In fact, we haven't been very clear about what exactly is and is not a set—this is a genuine difficulty. See Section 2.16 for a brief discussion of this. In this course, we will take the (not very rigorous!) point of view that anything we claim is a set, really is. In order for this to make some kind of sense, we will always work with respect to some 'universal set' E. For example, if we are thinking about sets of natural numbers, the universal set (the possible candidates for membership of the sets we might want to consider) is the set $\mathbb{N}$ of all natural numbers.

This might seem like an unnecessary complication, but it is essential. Suppose I tell you that the set A is the set of all even natural numbers. What are the objects that do not belong to A? Well, in the context of natural numbers, it is all odd natural numbers. The context is important (and it is this that is encapsulated in the universal set). Without that context (or universal set), then there are many other objects that we could say do not belong to A, such as negative integers, apples, bananas and elephants. (I could go on, but I hope you get the point!)

Given a universal set E and a subset A of E, the *complement* of A (sometimes called the *complement of A in E*) is denoted by $E \setminus A$ and is

$$E \setminus A = \{x \in E \mid x \notin A\}.$$

If the universal set is clear, the complement of A is sometimes denoted by $\bar{A}$ or A^c (with textbooks differing in their notation).

Suppose A is any subset of E. Because each member of E is either a member of A, or is not a member of A, it follows that

$$A \cup (E \setminus A) = E.$$

2.11.7 Sets and logic

There are a great many comparisons and analogies between set theory and logic. Using the shorthand notation for complements, one of the 'De Morgan' laws of complementation is that

$$\overline{A \cap B} = \bar{A} \cup \bar{B}.$$

This looks a little like the fact (observed in an earlier Learning Activity) that $\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$. And this is more than a coincidence. The negation operation, the conjunction operation, and the disjunction operation on statements behave entirely in the same way as the complementation, intersection, and union operations (in turn) on sets. In fact, when you start to prove things about sets, you often end up giving arguments that are based in logic.

For example, how would we prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$? We could argue as follows:

$$\begin{aligned} x \in \overline{A \cap B} &\iff x \notin A \cap B \\ &\iff \neg(x \in A \cap B) \\ &\iff \neg((x \in A) \wedge (x \in B)) \\ &\iff \neg(x \in A) \vee \neg(x \in B) \\ &\iff (x \in \bar{A}) \vee (x \in \bar{B}) \\ &\iff x \in \bar{A} \cup \bar{B}. \end{aligned}$$

What the result says is, in fact, easy to understand: if x is not in *both* A and B, then that's precisely because it fails to be in (at least) one of them.

For two sets A and B (subsets of a universal set E), the *complement of B in A*, denoted by $A \setminus B$, is the set of objects that belong to A but not to B. That is,

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Activity 2.4 Prove that $A \setminus B = A \cap (E \setminus B)$.

2.11.8 Cartesian products

For sets A and B, the *Cartesian product* $A \times B$ is the set of all *ordered pairs* (a, b), where $a \in A$ and $b \in B$. For example, if $A = B = \mathbb{R}$ then $A \times B = \mathbb{R} \times \mathbb{R}$ is the set of all ordered pairs of real numbers, usually denoted by $\mathbb{R}^2$.

There is often a confusion between sets of two elements and ordered pairs (or more generally ordered tuples, also called vectors). They're visually different: $\{a, b\}$ is a set with two elements (a and b, which are not the same) whereas (a, b) is the ordered pair whose first element is a and second element is b (and a and b might be the same, for example if you are to go 3 metres North and 3 metres East, i.e. follow the vector $(3, 3)$, units in metres). Usually people have no trouble remembering the difference when working with vectors in $\mathbb{R}^n$, but get the two confused when working with other things. If you are told that $\{\text{sugar}, \text{salt}\}$ are in jars in the cupboard, you know you don't need to go buy more. If you are told that there is $\{\text{salt}, \text{sugar}\}$ there, you've just been told the same thing again. You know you don't want to confuse $(\text{salt}, \text{sugar})$ and $(\text{sugar}, \text{salt})$, otherwise your tea will taste nasty. So if someone tells you that $\{\text{salt}, \text{sugar}\}$ are on the table, you'd probably ask which is which—is it $(\text{salt}, \text{sugar})$ from left to right, or $(\text{sugar}, \text{salt})$? In normal life you're happy with the idea that $\{\text{salt}, \text{sugar}\}$, $(\text{sugar}, \text{salt})$ and $(\text{salt}, \text{sugar})$ are three different things.

2.11.9 Power sets

For a set A, the set of all subsets of A, denoted $\mathcal{P}(A)$, is called the *power set* of A. Note that the power set is a set of sets. For example, if $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Activity 2.5 Write down the power set of the set $A = \{1, 2, 3, 4\}$.

Activity 2.6 Suppose that A has n members, where $n \in \mathbb{N}$. How many members does $\mathcal{P}(A)$ have?

2.12 Quantifiers

We have already met the ideas of universal and existential statements involving natural numbers. More generally, given any set E, a *universal statement* on E is one of the form 'for all $x \in E$, $P(x)$'. This statement is true if $P(x)$ is true for all x in E, and it is false if there is some x in E (known as a *counterexample*) such that $P(x)$ is false. We have a special symbol that is used in universal statements: the symbol '$\forall$' means 'for all'. So the typical universal statement can be written as

$$\forall x \in E,\ P(x).$$

(The comma is not necessary, but I think it looks better.) An *existential statement* on E is one of the form 'there is $x \in E$ such that $P(x)$', which is true if there is some $x \in E$ for which $P(x)$ is true, and is false if for every $x \in E$, $P(x)$ is false. Again, we have a useful symbol, '$\exists$', meaning 'there exists'. So the typical existential statement can be written as

$$\exists x \in E,\ P(x).$$

Here, we have omitted the phrase 'such that', but this is often included if the statement reads better with it. For instance, we could write

$$\exists n \in \mathbb{N},\ n^2 - 2n + 1 = 0,$$

but it would probably be easier to read

$$\exists n \in \mathbb{N} \text{ such that } n^2 - 2n + 1 = 0.$$

Often 'such that' is abbreviated to 's.t.'. (By the way, this statement is true because $n = 1$ satisfies $n^2 - 2n + 1 = 0$.)

We have seen that the negation of a universal statement is an existential statement and vice versa. In symbols, $\neg(\forall x \in E,\ P(x))$ is logically equivalent to $\exists x \in E,\ \neg P(x)$; and $\neg(\exists x \in E,\ P(x))$ is logically equivalent to $\forall x \in E,\ \neg P(x)$.

With these observations, we can now form the negations of more complex statements. Consider the statement

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m > n.$$

Activity 2.7 What does the statement $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m > n$ mean? Is it true?

What would the negation of the statement be? Let's take it gently. First, notice that the statement is

$$\forall n \in \mathbb{N}, (\exists m \in \mathbb{N}, m > n).$$

The parentheses here do not change the meaning. According to the rules for negation of universal statements, the negation of this is

$$\exists n \in \mathbb{N}, \neg(\exists m \in \mathbb{N}, m > n).$$

But what is $\neg(\exists m \in \mathbb{N}, m > n)$? According to the rules for negating existential statements, this is equivalent to $\forall m \in \mathbb{N}, \neg(m > n)$. What is $\neg(m > n)$? Well, it's just $m \leq n$. So what we see is that the negation of the initial statement is

$$\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, m \leq n.$$

We can put this argument more succinctly, as follows:

$$\begin{aligned} \neg\left(\forall n \in \mathbb{N}(\exists m \in \mathbb{N}, m > n)\right) &\iff \exists n \in \mathbb{N}, \neg(\exists m \in \mathbb{N}, m > n) \\ &\iff \exists n \in \mathbb{N}, \forall m \in \mathbb{N}, \neg(m > n) \\ &\iff \exists n \in \mathbb{N}, \forall m \in \mathbb{N}, m \leq n. \end{aligned}$$

2.12.1 Quantifiers and arbitrary unions and intersections; empty sets

Another way of defining arbitrary union is

$$\bigcup_{i \in I} A_i = \left\{x \mid \exists i \in I,\, x \in A_i\right\},$$

and the arbitrary intersection is

$$\bigcap_{i \in I} A_i = \left\{x \mid \forall i \in I,\, x \in A_i\right\}.$$

Check that you see these definitions agree with the ones we gave earlier!

Now, what exactly do we do if I is an empty set? Well, for union it is intuitively clear: the union of no sets had better be an empty set. That's what the definition above says. If I is empty, there is no $i \in I$, so whatever the condition after '$\exists i \in I$' is is irrelevant. The statement '$\exists X \in \emptyset$, $P(x)$' is False whatever $P(x)$ is. This looks obvious written like this, but if $P(x)$ is a statement that looks 'obviously true' you will be tempted to say that '$\exists X \in \emptyset$, $P(x)$' should be True, and then you will run into trouble.

For the arbitrary intersection, it is not so clear what the right answer should be — and in fact we will avoid using this notation — but what the answer should be is that

$$\bigcap_{i \in \emptyset} A_i = E$$

where E is the universal set we're working in. Why? Well, because '$\forall x \in \emptyset$, $P(x)$' is True whatever $P(x)$ is, so by definition every x we are considering is in the arbitrary intersection of no sets. This might sound strange, and for sets it is a bit funny. But it is important in logic: and again, if $P(x)$ is some statement that looks 'obviously false' then you will be tempted to say that '$\forall x \in \emptyset$, $P(x)$' should be False and get into trouble.

2.13 Proof by contradiction

We've seen a small example of proof by contradiction earlier in the chapter. Suppose you want to prove $P \Rightarrow Q$. One way to do this is by contradiction. What this means is that you suppose P is true but Q is false (in other words, that the statement $P \Rightarrow Q$ is false) and you show that, somehow, this leads to a conclusion that you know, definitely, to be false.

Here's an example.

> **Example 2.4** There are no integers m, n such that $6m + 8n = 1099$.

To prove this by contradiction, we can argue as follows:

Suppose that integers m, n *do* exist such that $6m + 8n = 1099$. Then since 6 is even, $6n$ is also even; and, since 8 is even, $8n$ is even. Hence $6m + 8n$, as a sum of two even numbers, is even. But this means $1099 = 6m + 8n$ is an even number. But, in fact, it is not even, so we have a contradiction. It follows that m, n of the type required do *not* exist. □

This sort of argument can be a bit perplexing when you first meet it. What's going on in the example just given? Well, what we show is that if such m, n exist, then something impossible happens: namely the number 1099 is both even and odd. Well, this can't be. If supposing something leads to a conclusion you know to be false, then the initial supposition must be false. So the conclusion is that such integers m, n do not exist.

Probably the most famous proof by contradiction is Euler's proof that there are infinitely many prime numbers. A prime number is a natural number greater than 1 which is only divisible by 1 and itself. Such numbers have been historically of huge importance in mathematics, and they are also very useful in a number of important applications, such as information security. The first few prime numbers are $2, 3, 5, 7, 11, \ldots$. A natural question is: does this list go on forever, or is there a largest prime number? In fact, the list goes on forever: there are infinitely many prime numbers. We'll mention this result again later. A full, detailed, understanding of the proof requires some results we'll meet later, but you should be able to get the flavour of it at this stage. So here it is, a very famous result:

There are infinitely many prime numbers.

Proof. (Informally written for the sake of exposition) Suppose *not*. That is, suppose there are only a finite number of primes. Then there's a largest one. Let's call it M. Now consider the number

$$X = (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times M) + 1,$$

which is the product of *all* the prime numbers (2 up to M), with 1 added. Notice that $X > M$, so X is not a prime (because M is the largest prime). If a number X is not prime, that means that it has a divisor p that is a prime number and which satisfies $1 < p < X$. [*This is the key observation: we haven't really proved this yet, but we will later.*] But p must therefore be one of the numbers $2, 3, 5, \ldots, M$. However, X is *not*

divisible by any of these numbers, because it has remainder 1 when divided by any of them. So we have reached a contradiction: on the one hand, X must be divisible by one of these primes, and on the other, it is not. So the initial supposition that there were *not* infinitely many primes simply must be wrong. We conclude there are infinitely many primes. □

This proof has been written in a fairly informal and leisurely way to help explain what's happening. It could be written more succinctly and a bit more formally:

Proof. Suppose the set of prime numbers is not infinite. Then there are t prime numbers, for some integer t. In other words, the set of prime numbers is $\{p_1, \ldots, p_t\}$. Consider the integer $N = (p_1 \times p_2 \times \cdots \times p_t) + 1$. Now N is bigger than any of $p_1, \ldots, p_t$, so (by our assumption that $p_1, \ldots, p_t$ are all the prime numbers) it cannot be prime. And by construction N is not divisible by any of $p_1, \ldots, p_t$ (if we divide by any of them we have a remainder of 1). And since 2 and 3 are prime, certainly N is at least 7, in particular it is bigger than 1. But any integer bigger than 1 is either prime or it is divisible by a prime number, which is a contradiction. □

This proof is still missing a few things—which you can see a bit more clearly because it's written formally. Why does the first sentence imply the second? Well, we didn't formally define the word 'infinite' yet. When we do, you'll see that the second sentence is just writing out the definition of 'not infinite', also known as 'finite'. And we still didn't prove the final sentence—but hopefully it is a bit more clear what exactly we do need to prove. It's worth thinking about this a little bit now—what exactly is missing? We defined a prime number to be an integer greater than 1 which is only divisible by 1 and itself. So we need to know what to do if we are given an integer bigger than 1 which is not prime.

The other point which we should be careful about is the following. Suppose that we take the first t prime numbers, multiply them together and add one. What we just proved is that *either* we will get a new prime number *or* what we get will be divisible by a prime number which isn't one of the first t primes. We don't have any idea which of these two things will happen. If you try this for the first few values of t, you see

$$\begin{aligned} 2 + 1 &= 3 \\ 2 \times 3 + 1 &= 7 \\ 2 \times 3 \times 5 + 1 &= 31 \\ 2 \times 3 \times 5 \times 7 + 1 &= 211 \\ 2 \times 3 \times 5 \times 7 \times 11 + 1 &= 2311 \end{aligned}$$

which are all prime. It's tempting to think this pattern will continue, but in fact

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$$

is not prime.

2.14 Some terminology

At this point, it's probably worth introducing some important terminology. When, in Mathematics, we prove a true statement, we often say we are proving a *Theorem*, or a

Proposition. (Usually the word 'Proposition' is used if the statement does not seem quite so significant as to merit the description 'Theorem'.) A theorem that is a preliminary result leading up to a Theorem is often called a *Lemma*, and a minor theorem that is a fairly direct consequence of, or special case of, a theorem is called a *Corollary*, if it is not significant enough itself to merit the title Theorem. For your purposes, it is important just to know that these words all mean true mathematical statements. You should realise that these terms are used subjectively: for instance, the person writing the mathematics has to make a decision about whether a particular result merits the title 'Theorem' or is, instead, merely to be called a 'Proposition'.

2.15 General advice

2.15.1 Introduction

Proving things is difficult. Inevitably, when you read a proof, in the textbooks or in these notes, you will ask 'How did the writer know to do that?' and you will often find you asking yourself 'How can I even begin to prove this?'. This is perfectly normal. This is where the key difference between abstract mathematics and more 'methods-based' mathematics lies. If you are asked to differentiate a function, you just go ahead and do it. It might be technically difficult in some cases, but there is no doubt about what approaches you should use. But proving something is more difficult. You might try to prove it, and fail. That's fine: what you should do in that case is try another attack. Keep trying until you crack it. (I suppose this is a little bit like integration. You'll know that there are various methods, but you don't necessarily know which will work on a particular integral, so you should try one, and keep trying until you manage to find the integral.) Abstract mathematics should always be done with a large pile of scrap paper at your disposal. You are unlikely to be able to write down a perfect solution to a problem straight away: some 'scratching around' to get a feel for what's going on might well be needed, and some false starts might be pursued first. If you expect to be able to envisage a perfect solution in your head and then write it down perfectly, you are placing too much pressure on yourself. You will only be able to do this for easy problems, and we aren't going to be doing easy problems. Your lecturers may give the impression of being able to produce perfect solutions effortlessly, but this is a result of lots of practice and doing the work in advance of the lecture (i.e. cheating). When we come across a problem we haven't seen before, we also try things which turn out not to work.

In this chapter I have tried to indicate that there are methodical approaches to proof (such as proof by contradiction, for example). What you have to always be able to do is to understand *precisely* what it is that you have to prove. That sounds obvious, but it is something the importance of which is often underestimated. Once you understand what you need to show (and, here, working backwards a little from that end-point might be helpful, as we've seen), then you have to try to show it. And you must know when you have done so! So it is inevitable that you will have to take a little time to think about what is required: you cannot simply 'dive in' like you might to a differentiation question.

All this becomes much easier as you practice it. You should attempt problems from

the textbooks (and also the problems below). Problems are a valuable resource and you are squandering this resource if you simply turn to the answers (should these be available). It is one thing to 'agree' with an answer, or to understand a proof, but it is quite a different thing to come up with a proof yourself. There is no point in looking at the answer before you have tried hard yourself to answer the problem. By trying (and possibly failing), you will learn more than simply by reading answers. Exam questions will be different from problems you have seen, so there is no point at all in 'learning' answers. You need to understand how to approach problems and how to answer them for yourself.

2.15.2 How to write mathematics

You should write mathematics **in English**!! You shouldn't think that writing mathematics is just using formulae. A good way to see if your writing makes sense is by reading it aloud (where you should only read what you really have written, not adding extra words). If it sounds like nonsense, a sequence of loose statements with no obvious relations, then you probably need to write it again.

Don't use more symbols than necessary.
Since many people seem to think that mathematics involves writing formulae, they often use symbols to replace normal English words. An eternal favourite is the double arrow "$\Longrightarrow$" to indicate that one thing follows from the other. As in:

$$x^2 = 1 \quad \Longrightarrow \quad x = 1 \text{ or } x = -1.$$

This is not only pure laziness, since it's just as easy to write:

$$x^2 = 1, \text{ hence } x = 1 \text{ or } x = -1.$$

But it is even probably not what was meant! The implication arrow "$\Longrightarrow$" has a logical meaning "if ..., then ...". So if you write "$x^2 = 1 \implies x = 1$ or $x = -1$", then that really means "**if** $x^2 = 1$, then $x = 1$ or $x = -1$". And hence this gives no real information about what x is. On the other hand, writing

$$\text{I know } x^2 = 1, \text{ hence } x = 1 \text{ or } x = -1,$$

means that now we know $x = 1$ or $x = -1$ and can use that knowledge in what follows.

Some other unnecessary symbols that are sometimes used are "$\therefore$" and "$\because$". They mean something like "therefore/hence" and "since/because". It is best not to use them, but to write the word instead. It makes things so much easier to read.

Provide all information required.
A good habit is to start by writing what information is given and what question needs to be answered. For instance, suppose you are asked to prove the following:

Problem 2.1 For any natural numbers a, b, c with $c \geq 2$, there is a natural number n such that $an^2 + bn + c$ is not a prime.

A good start to an answer would be:

Given : natural numbers a, b, c, with $c \geq 2$.
To prove : there is a natural number n such that $an^2 + bn + c$ is not a prime.

At this point you (and any future reader) has all the information required, and you can start thinking what really needs to be done.

2.15.3 How to do mathematics

In a few words : **by trying** and **by doing it yourself** !!

Try hard
The kind of questions you will be dealing with in this subject often have no obvious answers. There is no standard method to come to an answer. That means that you have to find out what to do yourself. And the only way of doing that is by trial and error.

So once you know what you are asked to do (plus all the information you were given), the next thing is to take a piece of paper and start writing down some possible next steps. Some of them may look promising, so have a better look at those and see if they will help you. Hopefully, after some (or a lot) of trying, you see how to answer the question. Then you can go back to writing down the answer. This rough working is a vital part of the process of answering a question (and, in an examination, you should make sure your working is shown). Once you have completed this part of the process, you will then be in a position to write the final answer in a concise form indicating the flow of the reasoning and the arguments used.

Keep trying
You must get used to the situation that not every question can be answered immediately. Sometimes you immediately see what to do and how to do it. But other times you will realise that after a long time you haven't got any further.

Don't get frustrated when that happens. Put the problem aside, and try to do another question (or do something else). Look back at the question later or another day, and see if it makes more sense then. Often the answer will come to you as some kind of "ah-ha" flash. But you can't force these flashes. Spending more time improves the chances they happen, though.

Don't get the idea that you are looking for 'the right answer'. That might seem funny—in every mathematics class you ever took so far, you were probably told that the point of mathematics is 'to find the right answer'. This is *not true*. We would like to know which statements are true and which are false—but usually there are lots of different correct ways to prove a statement is true. They are all 'right answers'. So don't be surprised if your answer to a problem is not the same as the model solution but it is marked as correct—that just means you found a different way to solve the problem, which is fine.

If you need a long time to answer certain questions, you can consider yourself in good company. For the problem known as "Fermat's Last Theorem", the time between when the problem was first formulated and when the answer was found was about 250 years.

Finally, you should not be unhappy if you find some problems you can't solve at all.

What about the following: Suppose I take the first t primes, multiply them together and add one (remember we saw this when we proved that there are infinitely many primes). We know the result is sometimes prime and sometimes not, depending on t (we saw examples of both). Are there infinitely many values of t such that we get a prime number? No-one knows the answer; that problem has been open for over 2 300 years.

Do it yourself
Here is one (of many possible) solutions to Problem 2.1:

Given : natural numbers a, b, c, with $c \geq 2$.
To prove : there is a natural number n such that $an^2 + bn + c$ is not a prime.
By definition, a natural number p is **prime** if $p \geq 2$ and the only divisors of p are 1 and p itself.
Hence to prove : there is a natural number n for which $an^2 + bn + c$ is smaller than 2 or it has divisors other than 1 or itself.
Let's take $n = c$. Then we have $an^2 + bn + c = ac^2 + bc + c$.
But we can write $ac^2 + bc + c = c\,(ac + b + 1)$, which shows that $ac^2 + bc + c$ has c and $ac + b + 1$ as divisors.
Moreover, it's easy to see that neither c nor $ac + b + 1$ can be equal to 1 or to $ac^2 + bc + c$.
We've found a value of n for which $an^2 + bn + c$ has divisors other than 1 or itself. □

The crucial step in the answer above is the one in which I choose to take $n = c$. Why did I choose that? Because it works. How did I get the idea to take $n = c$? Ah, that's far less obvious. Probably some rough paper and lots of trying was involved. In the final answer, no information about how this clever idea was found needs to be given.

You probably have no problems following the reasoning given above, and hence you may think that you understand this problem. But being able to follow the answer, and **being able to find the answer yourself** are two completely different matters. And it is the second skill you are suppose to acquire in this course. (And hence the skill that will be tested in the examination.) Once you have learnt how to approach questions such as the above and come up with the clever trick yourself, you have some hope of being able to answer other questions of a similar type.

But if you only study answers, you will probably never be able to find new arguments for yourself. And hence when you are given a question you've never seen before, how can you trust yourself that you have the ability to see the "trick" that that particular question requires ?

For many, abstract mathematics seems full of clever "tricks". But these tricks have always been found by people working very hard to get such a clever idea, not by people just studying other problems and the tricks found by other people.

2.15.4 How to become better in mathematics

One thing you might consider is doing more questions. The books are a good source of exercises. Trying some of these will give you extra practice.

But if you want to go beyond just being able to do what somebody else has written

down, you must try to explore the material even further. Try to understand the reason for things that are maybe not explicitly asked.

As an illustration of thinking that way, look again at the formulation of the example we looked at before :

For any natural numbers a, b, c with $c \geq 2$, there is a natural number n such that $an^2 + bn + c$ is not a prime.

Why is it so important that $c \geq 2$? If you look at the proof in the previous section, you see that that proof goes wrong if $c = 1$. (Since we want to use that c is a divisor different from 1.) Does that mean the statement is wrong if $c = 1$? (No, but a different proof is required.)

And what happens if we allow one or more of a, b, c to be zero or negative?

And what about more complicated expression such as $an^3 + bn^2 + cn + d$ for some numbers a, b, c, d with $d \geq 2$? Could it be possible that there is an expression like this for which all n give prime numbers ? If you found the answer to the original question yourself, then you probably immediately see that the answer has to be "no", since similar arguments as before work. But if you didn't try the original question yourself, and just studied the ready-made answer, you'll be less well equipped to answer more general or slightly altered versions.

Once you start thinking like this, you are developing the skills required to be good in mathematics. Trying to see beyond what is asked, asking yourself new questions and seeing which you can answer, is the best way to train yourself to become a mathematician.

2.16 Non-examinable: set theory—take 2

What is a set, exactly? It's supposed to be a mathematical object, which contains other mathematical objects. That sounds like a definition—why not just say that anything goes; put a bunch of objects in a bag and you have a set, which you can name (and in turn you can put it in further sets.

One of the properties we would rather like to have sets to have is that we can write things like

$$\{n \in \mathbb{N} : n \text{ is even}\}$$

and say that this too is a set. More generally, if we have some statement $P(s)$ (whose truth depends on s) and a set S, we would like to say that $\{s \in S : P(s) \text{ is true}\}$ is a set. We'll see that this kind of statement shows up continually throughout your degree programme.

Now, so far this looks fine—if 'anything goes' then certainly this is OK. But if 'anything goes', we can also ask about the set of all mathematical objects—this would also be a set, let's call it $\mathcal{U}$ for 'universe'. And we can write our favourite statement $P(s)$, for example $P(s)$ could be the statement 's is not a member of s'. In that case we get a set

$$X = \{s \in \mathcal{U} : P(s) \text{ is true}\}.$$

Now, you might notice this statement $P(s)$ is a bit funny—how can a set possibly be a member of itself? Well, actually if $\mathcal{U}$ is a set, it is a mathematical object so it has to contain itself. That might already raise a warning sign that strange things are going to happen, but it's not actually a logical contradiction; it's just a bit funny.

But what about this set X? Well, by definition X contains everything which is not a member of itself (and nothing else). So it certainly contains anything which isn't a set (because something which isn't a set doesn't contain anything at all, let alone itself). And it certainly contains a lot of sets, like $\emptyset$ and $\{1, 2, 53\}$. OK, does X contain X? Well, if not, then by definition it should. So X must contain X. But then by definition, X cannot contain X. That's a logical contradiction, pointed out by Bertrand Russell. It's really nothing more than a mathematical version of the 'Barber of Seville', who shaves everyone in Seville that doesn't shave themself. Who shaves the Barber?

What this logical contradiction tells us is that 'anything goes' is not OK. Some things are not sets. We need to give some rules which allow you to construct new sets from old sets; some *axioms of set theory*. This is what most mathematicians do (when we think about such things at all!), and usually we use some axioms called ZFC. These axioms don't, for instance, allow you to construct a 'set of everything'; in fact, they don't allow any set to contain itself (because you have to construct new sets from old sets you already have). These rules don't—as far as we know—lead to logical contradictions like Russell's. If you are worried about trying to explain everything in mathematics, then a good place to start is with ZFC set theory.

However, ZFC set theory is hard work; you spend a lot of time and energy proving things which look 'obvious', to an even greater extent than you'll see in the next chapter (where we discuss axioms for the natural numbers). We had to make a choice: do we spend all of MA103 building up the basics of mathematics from set theory, so that you have one (hopefully) consistent foundation for the rest of your degree? Or do we want to actually do some mathematics? We chose to do the latter, which means that in this course we are going to assume some things are true without proving them. In particular, we are going to assume statements like that there is such a thing as the set of natural numbers $\mathbb{N}$, that it makes sense to talk about sets of pairs such as $\{(a, b) : a, b \in \mathbb{N}\}$, and so on. All these are things which one can prove from the ZFC axioms, but we will not do so.

If you dislike this, you should go study ZFC set theory (in the summer, when you have time!). However don't expect it to be particularly easy, and don't expect it to be an 'answer to everything'. You'll still need to assume that ZFC set theory itself makes sense; there is no proof that it makes sense.

2.17 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- demonstrate an understanding of what mathematical statements are
- prove whether mathematical statements are true or false
- negate statements, including universal statements and existential statements

- construct truth tables for logical statements
- use truth tables to determine whether logical statements are logically equivalent or not
- demonstrate knowledge of what is meant by conjunction and disjunction
- demonstrate understanding of the meaning of 'if-then' statements and be able to prove or disprove such statements
- demonstrate understanding of the meaning of 'if and only if' statements and be able to prove or disprove such statements
- find the converse and contrapositive of statements
- prove statements by proving their contrapositive
- prove results by various methods, including directly, by the the method of proof by contradiction, and by working backwards
- demonstrate understanding of the key ideas and notations concerning sets
- prove results about sets
- use existential and universal quantifiers
- be able to negate statements involving several different quantifiers

2.18 Sample exercises

Exercise 2.1
Is the following statement about natural numbers n true or false? Justify your answer by giving a proof or a counterexample:

If n is divisible by 6 then n is divisible by 3.

What are the converse and contrapositive of this statement? Is the converse true? Is the contrapositive true?

Exercise 2.2
Is the following statement about natural numbers n true or false? Justify your answer by giving a proof or a counterexample:

If n is divisible by 2 then n is divisible by 4.

What are the converse and contrapositive of this statement? Is the converse true? Is the contrapositive true?

Exercise 2.3
Prove that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent. □

Exercise 2.4
Prove that the negation of $P \vee Q$ is $\neg P \wedge \neg Q$.

Exercise 2.5
Prove that for all real numbers a, b, c, $ab + ac + bc \leq a^2 + b^2 + c^2$.

Exercise 2.6
Prove by contradiction that there is no largest natural number.

Exercise 2.7
Prove that there is no smallest positive real number.

Exercise 2.8
Suppose A and B are subsets of a universal set E. Prove that

$$(E \times E) \setminus (A \times B) = ((E \setminus A) \times E) \cup (E \times (E \setminus B)).$$

Exercise 2.9
Suppose that $P(x, y)$ is a predicate involving two free variables x, y from a set E. (So, for given x and y, $P(x, y)$ is either true or false.) Find the negation of the statement

$$\exists x \in E, \forall y \in E, P(x, y)$$

2.19 Comments on selected activities

Learning activity 2.2 We can do this by constructing a truth table. Consider Table 2.8. This proves that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are equivalent.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
T	T	T	**F**	F	F	**F**
T	F	F	**T**	F	T	**T**
F	T	F	**T**	T	F	**T**
F	F	F	**T**	T	T	**T**

Table 2.8: The truth tables for $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$

Learning activity 2.3 The converse is 'if n divides 12 then n divides 4'. This is false. For instance, $n = 12$ is a counterexample. This is because 12 divides 12, but it does not divide 4. The original statement is true, however. For, if n divides 4, then for some $m \in \mathbb{Z}$, $4 = nm$ and hence $12 = 3 \times 4 = 3nm = n(3m)$, which shows that n divides 12.

Learning activity 2.4 We have

$$\begin{aligned} x \in A \setminus B &\iff (x \in A) \wedge (x \notin B) \\ &\iff (x \in A) \wedge (x \in E \setminus B) \\ &\iff x \in A \cap (E \setminus B). \end{aligned}$$

Learning activity 2.5 $\mathcal{P}(A)$ is the set consisting of the following sets:

$$\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\},$$

$$\{1,2,3\}, \{2,3,4\}, \{1,3,4\}, \{1,2,4\}, \{1,2,3,4\}.$$

Learning activity 2.6 The members of $\mathcal{P}(A)$ are all the subsets of A. A subset S is determined by which of the n members of A it contains. For each member x of A, either $x \in S$ or $x \notin S$. There are therefore two possibilities, for each $x \in A$. It follows that the number of subsets is $2 \times 2 \times \cdots \times 2$ (where there are n factors, one for each element of A). Therefore $\mathcal{P}(A)$ has 2^n members.

Learning activity 2.7 The statement means that if we take any natural number n there will be some natural number m greater than n. Well, this is true. For example, $m = n + 1$ will do.

2.20 Solutions to exercises

Solution to exercise 2.1

The statement is true. For, suppose n is divisible by 6. Then for some $m \in \mathbb{N}$, $n = 6m$, so $n = 3(2m)$ and since $2m \in \mathbb{N}$, this proves that n is divisible by 3.

The converse is 'If n is divisible by 3 then n is divisible by 6'. This is false. For example, $n = 3$ is a counterexample: it is divisible by 3, but not by 6.

The contrapositive is 'If n is not divisible by 3 then n is not divisible by 6'. This is true, because it is logically equivalent to the initial statement, which we have proved to be true.□

Solution to exercise 2.2

The statement is false. For example, $n = 2$ is a counterexample: it is divisible by 2, but not by 4.

The converse is 'If n is divisible by 4 then n is divisible by 2'. This is true. For, suppose n is divisible by 4. Then for some $m \in \mathbb{N}$, $n = 4m$, so $n = 2(2m)$ and since $2m \in \mathbb{N}$, this proves that n is divisible by 2.

The contrapositive is 'If n is not divisible by 4 then n is not divisible by 2'. This is false, because it is logically equivalent to the initial statement, which we have proved to be false. Alternatively, you can see that it's false because 2 is a counterexample: it is not divisible by 4, but it *is* divisible by 2.

Solution to exercise 2.3

This can be established by using the truth table constructed in Learning activity 2.2. See the solution above.

Solution to exercise 2.4

This is established by Table 2.6. That table shows that $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. This is the same as saying that the negation of $P \vee Q$ is $\neg P \wedge \neg Q$.

Solution to exercise 2.5

We work backwards, since it is not immediately obvious how to begin. We note that what we're trying to prove is equivalent to

$$a^2 + b^2 + c^2 - ab - ac - bc \geq 0.$$

This is equivalent to

$$2a^2 + 2b^2 + 2c^2 - 2ab - 2ac - 2bc \geq 0,$$

which is the same as

$$(a^2 - 2ab + b^2) + (b^2 - 2bc + c^2) + (a^2 - 2ac + c^2) \geq 0.$$

You can perhaps now see how this is going to work, for $(a^2 - 2ab + b^2) = (a - b)^2$ and so on. Therefore the given inequality is equivalent to

$$(a - b)^2 + (b - c)^2 + (a - c)^2 \geq 0.$$

We know this to be true because squares are always non-negative. If we wanted to write this proof 'forwards' we might argue as follows. For any a, b, c, $(a - b)^2 \geq 0$, $(b - c)^2 \geq 0$ and $(a - c)^2 \geq 0$, so

$$(a - b)^2 + (b - c)^2 + (a - c)^2 \geq 0$$

and hence

$$2a^2 + 2b^2 + 2c^2 - 2ab - 2ac - 2bc \geq 0,$$

from which we obtain

$$a^2 + b^2 + c^2 \geq ab + ac + bc,$$

as required. □

Solution to exercise 2.6

Let's prove by contradiction that there is no largest natural number. So suppose there is a largest natural number. Let us call it N. (What we want to do now is somehow show that a conclusion, or something we know for sure must be false, follows.) Well, consider the number $N + 1$. This is a natural number. But since N is the largest natural number, we must have $N + 1 \leq N$, which means that $1 \leq 0$, and that's nonsense. So it follows that we must have been wrong in supposing there is a largest natural number. (That's the only place in this argument where we could have gone wrong.) So there is *no* largest natural number. We could have argued the contradiction slightly differently. Instead of using the fact that $N + 1 \leq N$ to obtain the absurd statement that $1 \leq 0$, we could have argued as follows: $N + 1$ is a natural number. But $N + 1 > N$ and this contradicts the fact that N is the largest natural number.

Solution to exercise 2.7

We use a proof by contradiction. Suppose that there is a smallest positive real number and let's call this r. Then $r/2$ is also a real number and $r/2 > 0$ because $r > 0$. But $r/2 < r$, contradicting the fact that r is the smallest positive real number. (Or, we could argue: because $r/2$ is a positive real number and r is the smallest such number, then we must have $r/2 \geq r$, from which it follows that $1 \geq 2$, a contradiction.)

Solution to exercise 2.8

We need to prove that

$$(E \times E) \setminus (A \times B) = ((E \setminus A) \times E) \cup (E \times (E \setminus B)).$$

Now,

$$\begin{aligned}
(x,y) \in (E \times E) \setminus (A \times B) &\iff \neg((x,y) \in A \times B) \\
&\iff \neg((x \in A) \wedge (y \in B)) \\
&\iff \neg(x \in A) \vee \neg(y \in B) \\
&\iff (x \in E \setminus A) \vee (y \in E \setminus B) \\
&\iff ((x,y) \in (E \setminus A) \times E) \vee ((x,y) \in E \times (E \setminus B)) \\
&\iff (x,y) \in ((E \setminus A) \times E) \cup (E \times (E \setminus B)).
\end{aligned}$$

Solution to exercise 2.9

We deal first with the existential quantifier at the beginning of the statement. So, the negation of the statement is

$$\forall x \in E, \neg(\forall y \in E, P(x,y))$$

which is the same as

$$\forall x \in E, \exists y \in E, \ \neg P(x,y).$$

Chapter 3
Mathematical structures, natural numbers and proof by induction

☞ Biggs, N. L. *Discrete Mathematics*. Chapter 4.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapters 1–4 and 6.

3.1 Introduction

In this chapter we will discuss what is meant by a 'mathematical structure', and explore some of the properties of one of the most important mathematical structures: the natural numbers. These will not be new to you, but they shall be explained a little more formally. The chapter also studies a very powerful proof method, known as *proof by induction*. This enables us to prove many universal statements about natural numbers that would be extremely difficult to prove by other means.

Along the way, we are going to see the first 'real' example of Abstract Maths: what some standard axioms are and what they are good for.

3.2 Mathematical structures

A mathematical structure is a precisely specified object which one can study. We already saw, informally, several examples in the course:

(1) The natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ which come with the operations $+$ and $\times$, and the relation $<$.

(2) The integers $\mathbb{Z}$ which come with the operations $+$ and $\times$, and the relation $<$.

(3) The rational numbers $\mathbb{Q}$ (intuitively, the fractions; numbers which you can write as $\frac{a}{b}$ where a and b are integers and b is not zero), which again come with the operations $+$ and $\times$, and the $<$ relation.

(4) The real numbers $\mathbb{R}$ (intuitively: points on the number line) which again come with the operations $+$ and $\times$, and the $<$ relation.

(5) The complex numbers $\mathbb{C}$ which are numbers of the form $a + bi$, where i is a special symbol representing $\sqrt{-1}$. Again you can add and multiply these, but it's not clear what $<$ should be, so we leave it out.

All these examples are structures where you can do arithmetic as you're used to it. Here are another couple of examples. Don't worry if you haven't seen these before. We won't try to study them just yet; you'll study them more later this year.

(6) The 'clock numbers' $\mathbb{Z}_{24}$, which are the integers $\{0, 1, 2, \ldots, 23\}$ on a 24-hour clock, where you add and multiply as you would on a clock; if you get 24 you replace it with 0, if you get 25 you replace it with 1, and so on.

(7) The 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are real numbers. Here too we can define addition and multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \quad \text{and}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}.$$

These still look like structures where you can 'do arithmetic as you're used to it'. But you have to be a little careful now. In $\mathbb{Z}_{24}$ we have $4 \times 5 = 20 = 4 \times 11$. So what should we say $20/4$ is? You're used to the idea that 'division by zero' doesn't make sense, but in $\mathbb{Z}_{24}$ 'division by four' also doesn't make sense. When you work with 2×2 matrices, then multiplication turns out not to be commutative:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \quad \text{but} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Here is a rather different example.

(8) The set of social networks, where a social network consists of a (finite) collection of people and a relation 'friends' between pairs of people.

Think of taking a snapshot of the Facebook network at some moment: there are something like 1 000 000 000 people in the network, and if I look at any particular pair I will find they are either friends or they are not. That's a social network (by the definition we gave); if we let some time pass, some people join or leave, some pairs of people friend or de-friend each other, we get a different social network.

It's not clear what $+$ or $\times$ should mean here—how can we multiply social networks? But I probably don't have to convince you that there are interesting things to study here; and in fact the (results of the) mathematical study of networks ('Graph Theory') turns out to be very important in today's technology. We're not going to go further into this in MA103; the point of giving this example is to show you that we can be interested as mathematicians in things which don't involve arithmetic.

More or less, any time you find a precise, unambiguous definition of something, then you have a mathematical structure which you can start studying. Mathematics is a much broader area than the arithmetic you saw in school. **A lot of mathematics is not about numbers.** Of course, not everything interesting is mathematics—you (maybe) find politics interesting, but you will not be able to come up with a definition of 'left-wing' or 'economically good' which is generally agreed on, let alone one which

is precise and unambiguous. We'll have to leave politics to the political scientists. The flip side of this is: it's (more or less) true that all mathematicians agree that all of mathematics is correct, which keeps fights to a minimum. That's certainly not true for political scientists, who (sometimes) write books whose messages boil down to 'My idea is right', 'You're wrong', 'Am not!', 'Wrongy wrongy wrong!'... and so on.

If you're thinking carefully, you might notice that the structures we mentioned above aren't really very clearly defined. What are 'the points on the number line'? In fact, what are 'the natural numbers'? We probably all feel we know what is meant by a positive integer, how to add and multiply them, and that all of us will get the same answers if we try it. But that's not good enough. It would be very embarrassing if it turned out that some of us made different assumptions to others about the natural numbers, and we started arguing about what statements are true. So let's find a way to avoid that right away.

3.3 Natural numbers: an axiomatic approach

In order to clearly and unambiguously define what we mean by 'the natural numbers', we are going to write down a collection of simple statements which we can all agree are true for the natural numbers—which we call *axioms* for the natural numbers—and then we will prove that there is really only one mathematical structure which satisfies all of these statements. Of course, this course is in English, so the natural numbers start 'one, two,...' and so on; if it was in German I would write 'eins, zwei,...'. But these are really the same thing; I just need a dictionary to tell me that 'mal' is 'times' and 'siebenundzwanzig' is 'twenty-seven'. So what we will need to prove is that any two mathematical structures which satisfy all our axioms are basically the same; there is a dictionary-style correspondence between them.

At this stage, you probably either don't see how this can be possible, or you don't see where there could be any problem. So let's state the axioms for the natural numbers, and then try to explain them. Before you get worried—I do **not** expect you to learn these axioms, if you need them for the exam then they will be printed on the exam (as you can see on last year's paper). You will need to know how to use these axioms, but learning them is a waste of time (because you do already know how to do arithmetic!).

($\mathbb{N}\mathbf{1}$) For all $a, b \in \mathbb{N}$ we have $a + b \in \mathbb{N}$. [Closure under Addition]

($\mathbb{N}\mathbf{2}$) For all $a, b \in \mathbb{N}$ we have $a + b = b + a$. [Commutative Law for Addition]

($\mathbb{N}\mathbf{3}$) For all $a, b, c \in \mathbb{N}$ we have $(a + b) + c = a + (b + c)$. [Associative Law for Addition]

($\mathbb{N}\mathbf{4}$) For all $a, b \in \mathbb{N}$ we have $a \times b \in \mathbb{N}$. [Closure under Multiplication]

($\mathbb{N}\mathbf{5}$) For all $a, b \in \mathbb{N}$ we have $a \times b = b \times a$. [Commutative Law for Multiplication]

($\mathbb{N}\mathbf{6}$) For all $a, b, c \in \mathbb{N}$ we have $(a \times b) \times c = a \times (b \times c)$. [Associative Law for Multiplication]

(ℕ**7**) For all $a, b, c \in \mathbb{N}$ we have $a \times (b + c) = (a \times b) + (a \times c)$. [Distributive Law]

(ℕ**8**) There is a special element of $\mathbb{N}$, denoted by 1, which has the property that for all $n \in \mathbb{N}$ we have $n \times 1 = n$.

(ℕ**9**) For all $a, b, c \in \mathbb{N}$, if $a + c = b + c$, then $a = b$. [Additive Cancellation]

(ℕ**10**) For all $a, b, c \in \mathbb{N}$, if $a \times c = b \times c$, then $a = b$. [Multiplicative Cancellation]

(ℕ**11**) For all $a, b \in \mathbb{N}$, $a < b$ if and only if there is some $c \in \mathbb{N}$ with $a + c = b$.

(ℕ**12**) For all $a, b \in \mathbb{N}$, exactly one of the following is true: $a = b$, $a < b$, $b < a$.

(ℕ**13**) For any non-empty subset S of $\mathbb{N}$, there exists $a \in S$ such that $a \leq b$ for every $b \in S$. [Well-ordering principle]

Before we go on to work with these axioms, let's try to say a little bit about them. You should read the first three axioms as saying 'addition works the way I think it does'. These three axioms are also true if you replace the natural numbers $\mathbb{N}$ with for example the real numbers $\mathbb{R}$, or the complex numbers $\mathbb{C}$, or the 'clock numbers' $\mathbb{Z}_{24}$, or for adding up 2×2 matrices. Of the list of structures in Section 3.2, the only one we ruled out with these axioms is the social networks, because they don't have an 'addition'.

The next three axioms say the same thing for multiplication, and axiom (ℕ**7**) says that addition and multiplication work together the way you learnt years ago in school. Again, these would all be true for $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_{24}$, as well as for $\mathbb{N}$. But we just saw that 2×2 matrix multiplication is *not* commutative.

So with these first seven axioms, we certainly haven't yet given an unambiguous definition of the natural numbers. But some possibilities have been ruled out, for example what we are trying to describe cannot be 2×2 matrices. The more axioms we add, the more possibilities are ruled out.

Let's move on to axiom (ℕ**8**). This says that there is at least one element in the set $\mathbb{N}$ we're trying to describe (and multiplying by that element doesn't change anything)—if you think about it, the empty set trivially satisfies all of the previous axioms too, just because there don't exist any elements to provide a counterexample. But now the empty set is ruled out. However there are still lots of mathematical structures left which satisfy (ℕ**1**)–(ℕ**8**), for example $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

The axioms (ℕ**9**) through (ℕ**12**) again simply say that addition and multiplication behave the way you expect; and that they interact with $<$ the way you think positive numbers should. It's worth pointing out that these axioms together rule out all the structures we mentioned above except $\mathbb{N}$, because (ℕ**11**) isn't true for the rest ($1 + (-1) = 0$ but 1 is not smaller than 0). But still there are structures left which are not $\mathbb{N}$ but which satisfy (ℕ**1**)–(ℕ**12**), for example the positive real numbers (and there are more).

Finally we put in the axiom (ℕ**13**) which says that any non-empty set of natural numbers has a least element. This axiom is a bit more complicated than the rest, so let's check that we understand it intuitively. Suppose I have in mind a set S of natural numbers. If you want to find out whether it is empty or not, and if not what its least

element is, you can ask:

$$\begin{aligned} &\text{Is } 1 \text{ in the set } S?\\ \text{Is } 1+1 =&2 \text{ in the set } S?\\ \text{Is } 2+1 =&3 \text{ in the set } S?, \end{aligned}$$

and so on. I might say 'No' to the first few questions, but as soon as I say 'Yes' you will tell me 'OK, then that's the least element of S' (and you don't need to know what else might be in S). If I keep saying 'No' forever, then it must mean S is the empty set. This should justify (intuitively, not formally) that the natural numbers really satisfy ($\mathbb{N}$**13**).

Now, this axiom rules out the positive real numbers. There are sets of positive real numbers which don't have a least element—can you find one?

Activity 3.1 Think of a set of real numbers that has no least member.

But are we done? Maybe there are still some funny structures which are not the natural numbers but satisfy all the axioms. Hopefully you agree it isn't obvious what the answer is; just because you and I can't think of such a structure doesn't mean it doesn't exist. We'll get to that later in the chapter.

The proof we gave back on page 8 uses some of these axioms. But we also assumed $2+2=4$ and $2\times 2=4$, without proving them. Just for completeness, let's see how we can prove those two statements. To begin with, we need to explain what '2' is. Well, 2 is short-hand for $1+1$. And 3 is short-hand for $2+1$, which in turn really means $(1+1)+1$, and so on. Now we can prove $2+2=4$.

Proof of $2+2=4$**.**

$$\begin{aligned} 2+2 &= 2+(1+1) && \text{by definition of } 2\\ &= (2+1)+1 && \text{by axiom } (\mathbb{N}\mathbf{3})\\ &= 3+1 && \text{by definition of } 3\\ &= 4 && \text{by definition of } 4. \end{aligned}$$

□

That was a pain, and you probably don't want to see why $2\times 2=4$. It's a good exercise though.

Activity 3.2 Prove using the axioms that $2\times 2=4$.

Other properties of the natural numbers follow from these axioms. (That is, they can be proved assuming these axioms.)

For example, we can prove the following.

(P1) For all $a,b,c\in\mathbb{N}$, $(a+b)\times c=(a\times c)+(b\times c)$.

(P2) If $a,b\in\mathbb{N}$ satisfy $a\times b=a$, then $b=1$.

(P3) For $a,b,c\in\mathbb{N}$, if $a<b$ and $b<c$, then $a<c$. [Transitivity]

(P4) For $a, b, c \in \mathbb{N}$, if $a < b$ then $a + c < b + c$ and $a \times c < b \times c$.

(P5) 1 is the least element of $\mathbb{N}$.

(P6) 1 is not equal to $1 + 1$.

We don't need to add these to the axioms because they follow from the axioms we already have. (We can **prove** them just from the axioms above.) We'll come back to this later in the chapter.

In general, we can prove that all the properties of arithmetic which you are used to are true using these axioms. However, **we are not going to do this**. It is fiddly and time-consuming, and you will not learn anything new by doing it. If you are interested, or worried about whether you are really doing arithmetic right, then you can find these proofs in books on 'foundations of mathematics'.

You probably think all the above statements are obvious — but if someone asked you *why* 1 is the smallest natural number, how would you answer? Whatever you say, it has to be some argument which relies on specifically the properties of the natural numbers (as opposed to, say, the integers or the positive real numbers, for which 1 is not the smallest element!).

Let me try to be clear about what you are supposed to learn from working with these axioms. You are supposed to learn how to write proofs about mathematical structures using the axioms rather than from your intuition about 'how that structure should work'. The reason is that later on in your degree course (starting next term in MA103 and continuing), you will need to write proofs using similar axioms about structures about which *you, and I, do not have any intuition*, such as 'groups'. Then you have no choice but to write a proof from the axioms, and you do not want to have to learn how to do that from scratch with a complicated and unintuitive structure. So learn it now, using your intuition as a check. And we will try to get to interesting statements—ones which you didn't already know from school—as fast as possible; it won't take long.

3.3.1 Greatest and least elements

Let S be a subset of $\mathbb{N}$. We say ℓ is a *least element* or *least member* of S if $\ell \in S$ and for all $s \in S$ we have $\ell \leq s$. Similarly, we say g is a *greatest element* or *greatest member* of S if $g \in S$ and for all $s \in S$ we have $g \geq s$.

It's obvious that some subsets of $\mathbb{N}$ do not have a greatest element—for example $\mathbb{N}$ itself doesn't have a greatest element, nor does the set of even natural numbers, nor the set of primes (which is, more or less, what we proved in the last chapter). And by definition the empty set $\emptyset$ doesn't have either a least or a greatest element: it doesn't have any elements at all. But axiom ($\mathbb{N}$**13**), the Well-Ordering Principle, says that every non-empty subset of $\mathbb{N}$ has a least element. For this reason, the Well-Ordering Principle is sometimes also called the Least Element Principle. It's a rather special property of the natural numbers, which doesn't hold for many other structures, such as the real numbers.

3.4 The principle of induction

3.4.1 Proof by induction

One particularly useful principle that follows from the axioms of the natural numbers given above is the following one, known as the *Induction Principle*.

The Induction Principle: Suppose $P(n)$ is a statement involving natural numbers n. Then $P(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $P(1)$ is true; ('Base case')

(ii) For all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$. ('Induction step')

We'll **prove** this later in the chapter. Intuitively, the idea is as follows. Suppose you can prove two things:

$$P(1) \text{ is true,} \quad \text{and} \quad \forall k \in \mathbb{N},\ P(k) \Rightarrow P(k+1).$$

Then: because $P(1) \Rightarrow P(2)$ and $P(1)$ is true, we must have that $P(2)$ is true. Now, because $P(2) \Rightarrow P(3)$ and $P(2)$ is true, we must have $P(3)$ is true, and so on. So $P(n)$ has to be true for all $n \in \mathbb{N}$.

Let's give an example. If you have an infinitely tall ladder, you could let $P(n)$ be the statement 'I can climb to the nth rung'. So $P(1)$ is 'I can climb to the first rung'. Presumably you can show that's true, for example by standing on the first rung. That is proving the base case. Now, the induction step, in this example, is 'For all $k \in \mathbb{N}$, if I can climb to the kth rung then I can climb to the $(k+1)$st rung'. For any given k, it's clear this is true — if you can climb to the kth rung, then you just need to climb one more step to get to the $(k+1)$st rung. So this proves the induction step, and what you can conclude is that you can climb to any rung you like. This is all that induction is, but it turns out to be very useful.

Before we prove the Induction Principle properly (using the axioms) later in this chapter, let's think about how we can use it.

Suppose you want to prove $\forall n \in \mathbb{N}, P(n)$. This looks tricky: we need to show something is true for every natural number n. For each individual n, perhaps it is not so hard—a simple calculation might do the job for $P(1)$, $P(2)$,...—but probably the calculation gets harder as you try to check larger numbers, and you can't see how to write down a calculation with a general n in it. But you can check $P(1)$ is true. At this point you're stuck. You might think: perhaps it would help me to know $P(k)$ is true in order to prove $P(k+1)$. Well, let's assume it is and try to prove $P(k+1)$. What you're doing is proving the statement '$\forall k,\ P(k) \Rightarrow P(k+1)$', and when you've finished it you are done by the Principle of Induction. Let's see a few concrete examples.

3.4.2 An example

Here's an example of how we might prove by induction a result we proved directly earlier, in the previous chapter, namely:

$$\forall n \in \mathbb{N},\ n^2 + n \text{ is even.}$$

Let $P(n)$ be the statement '$n^2 + n$ is even'. Then $P(1)$ is true, because $1^2 + 1 = 2$, and this is even. (Establishing $P(1)$ is known as proving the *base case* or the *induction basis*.) Next we show that $P(k) \Rightarrow P(k+1)$ for any $k \in \mathbb{N}$. So we show that if $P(k)$ is true, so will be $P(k+1)$. To do this we assume that $P(k)$ is true and show that $P(k+1)$ is then also true. (The assumption that $P(k)$ is true is known as the *inductive hypothesis*.) So suppose $P(k)$ is true, which means that $k^2 + k$ is even. What we need to do now is show that this means that $P(k+1)$ is also true, namely that $(k+1)^2 + (k+1)$ is even. So we need somehow to relate the expression $(k+1)^2 + (k+1)$ to the one we are assuming we know something about, $k^2 + k$. Well,

$$(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + (2k + 2).$$

Now, by the 'inductive hypothesis' (the assumption that $P(k)$ is true), $k^2 + k$ is even. But $2k + 2 = 2(k+1)$ is also even, so $(k+1)^2 + (k+1)$ is an even number, in other words $P(k+1)$ is true. So we have shown that $\forall k, P(k) \Rightarrow P(k+1)$. It now follows, by the Principle of Induction, that for all $n \in \mathbb{N}$, $P(n)$ is true.

Once we get used to this technique, we can make our proofs more succinct.

The basic way of proving a result $\forall n \in \mathbb{N},\ P(n)$ by induction is as follows:

- **[The Base Case]** Prove $P(1)$ is true.
- **[The Induction Step]** Prove that, for any $k \in \mathbb{N}$, assuming $P(k)$ is true (the 'inductive hypothesis'), then $P(k+1)$ is also true.

And that's all you need to do! The principle of induction then establishes that $P(n)$ is true for all $n \in \mathbb{N}$.

3.4.3 Induction: why be careful?

At least for now, I'm going to insist that when you write a proof by induction, you really need to write it out formally as in the examples in this chapter. I want to see the words 'base case' appearing with a proof of the base case, I want to see the words 'induction step' appearing with a proof of the induction step, and then I want to see a final line like 'so by the principle of induction,... '.

This is not (just) because I am picky; it is because induction is an easy thing to mess up and 'prove' something which isn't true. Furthermore, later on you may well write a long complicated proof that uses induction in two or three different places, and writing it out formally like this gives you some structure and lets you see clearly where you are using induction and when you are done.

You may get worried about why induction works—it can get confusing, when you have some complicated statement which you are trying to prove, and especially if

you are using some variants of induction (see below). Keep in mind that eventually every induction proof is basically saying that if you can get to the first rung of the ladder, and you can always climb up to the next step, then you can climb the ladder.

You may alternatively begin to feel that induction is obvious and it's not clear why you need all the careful formalities; the examples we will see next mainly look like 'calculate the first case, then just keep doing the same calculation over and over again'. Why can't we simply write in a proof 'and now keep doing this calculation forever'? The answer is that it is easy to write down something which looks convincing, where the 'calculation you do forever' works for the first one or two times, but then it stops working because you missed some difficulty which doesn't show up in the first one or two cases. Induction is nothing more than 'and now keep doing this calculation forever', except that writing out the formalities forces you to say in detail exactly what calculation you will do and check it really works.

3.4.4 Variants

Suppose N is some particular natural number and that $P(n)$ is a statement involving natural numbers n. Then $P(n)$ is true for all $n \geq N$ if the following two statements are true:

(i) $P(N)$ is true;

(ii) For all $k \in \mathbb{N}, k \geq N$, $P(k) \Rightarrow P(k+1)$.

This is a version of the Induction Principle obtained from the standard one by 'changing the base case'. It can be used to prove a result like the following:

$$\forall n \geq 4, n^2 \leq 2^n.$$

(The inequality $n^2 \leq 2^n$ is false when $n = 3$, so it does not hold for all $n \in \mathbb{N}$.)

Activity 3.3 Prove that $\forall n \geq 4, n^2 \leq 2^n$.

In terms of the ladder intuition, this is simply saying that instead of calling the rungs of the ladder 'rung 1', 'rung 2' and so on, you paint N on the lowest rung, $N+1$ on the next lowest, and so on. Still, if you can get on the lowest rung (prove $P(N)$) and you can always climb from each rung to the next, then you can climb the ladder (i.e. you can get to every rung from the lowest, labelled N, up).

Another variant of the Induction Principle is the following, known as the Strong Induction Principle:

The Strong Induction Principle: Suppose $P(n)$ is a statement involving natural numbers n. Then $P(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $(P(s)$ true $\forall s \leq k) \Rightarrow P(k+1)$.

The name is misleading, because, in fact, the strong induction principle follows from the standard induction principle.

Activity 3.4 Try to understand why the strong induction principle follows from the induction principle. Hint: consider $Q(n)$, the statement '$\forall s \leq n,\ P(s)$ is true'. [This is difficult, so you may want to omit this activity at first.]

Again, in terms of the ladder intuition, what the induction step is now saying is not the "for every k, if I can climb to rung k then I can climb to rung $k+1$" of normal induction, but "for every k, if I can climb to rung k and I climbed on all the lower rungs on the way, then I can climb to rung $k+1$". Phrased like that, it's "obvious" that it doesn't really make a difference and still I can conclude that I can climb the ladder. What's not obvious is why such a thing might be useful. As we shall see, though, it is often useful when it comes to proving results about sequences that are defined 'recursively'.

In general, you won't know when you start trying to solve a problem that the Principle of Induction is a good tool to try using. Rather, you will get stuck in some logic and notice, 'hey, it would really help if I could assume the previous case is true.' Similarly, you don't always know from the outset when the strong induction principle is going to be handy. Rather, your thought when stuck will be 'hey, it would be great if I could assume some smaller case is (or a whole bunch of smaller cases are) true.'

3.5 Summation formulae

Suppose $a_1, a_2, a_3, \ldots$ is a sequence (an infinite, ordered, list) of real numbers. Then the sum $\sum_{r=1}^{n} a_r$ is the sum of the first n numbers in the sequence. It is useful to define these sums 'recursively' or 'by induction', as follows:

$$\sum_{r=1}^{1} a_r = a_1 \quad \text{and} \quad \text{for } n \in \mathbb{N},\ \sum_{r=1}^{n+1} a_r = \left(\sum_{r=1}^{n} a_r\right) + a_{n+1}.$$

With this observation, we can use proof by induction to prove many results about the values and properties of such sums. Here is a simple, classical, example.

Example 3.1 For all $n \in \mathbb{N}$, $\sum_{r=1}^{n} r = \frac{1}{2}n(n+1)$. This is simply the statement that the sum of the first n natural numbers is $n(n+1)/2$.

Proof. We prove the result by induction. Let $P(n)$ be the statement that $\sum_{r=1}^{n} r = \frac{1}{2}n(n+1)$. Then $P(1)$ states that $1 = \frac{1}{2} \times 1 \times 2$, which is true. So the base case $P(1)$ is true. Now let's do the induction step. Suppose that $k \in \mathbb{N}$ and that

(the inductive hypothesis) $\sum_{r=1}^{k} r = \frac{1}{2}k(k+1)$ holds. Consider $\sum_{r=1}^{k+1} r$. We have

$$\begin{aligned}
\sum_{r=1}^{k+1} r &= \sum_{r=1}^{k} r + (k+1) \\
&= \tfrac{1}{2}k(k+1) + (k+1) \text{ by the induction hypothesis} \\
&= \tfrac{1}{2}(k^2 + k + 2k + 2) \\
&= \tfrac{1}{2}(k^2 + 3k + 2) \\
&= \tfrac{1}{2}(k+1)(k+2) \\
&= \tfrac{1}{2}(k+1)((k+1)+1).
\end{aligned}$$

This establishes that $P(k+1)$ is true (for $P(k+1)$ is precisely the statement that $\sum_{r=1}^{k+1} r = (k+1)((k+1)+1)/2$.) Therefore, by induction, for all $n \in \mathbb{N}$, $\sum_{r=1}^{n} r = \frac{1}{2}n(n+1)$.

Note how the the induction hypothesis was used. In the induction step, you always prove $P(k+1)$ to be true assuming $P(k)$ is. (Unless you do so, it isn't a proof by induction.)

Activity 3.5 Prove by induction that the sum of the first n terms of an arithmetic progression with first term a and common difference d is $n(2a + (n-1)d)/2$.

3.6 Recursively defined sequences

Sequences of numbers are often defined 'recursively' or 'by induction'.

For example, suppose that the sequence x_n is given by $x_1 = 9$, $x_2 = 13$ and, for $n \geq 3$, $x_n = 3x_{n-1} - 2x_{n-2}$. We can prove by induction (using the strong induction principle) that, for all $n \in \mathbb{N}$, $x_n = 5 + 2^{n+1}$. Here's how:

Since the inductive definition for x_n only applies for $n \geq 3$, the base step of our proof is to verify the result for the cases $n = 1$ and $n = 2$. Now, when $n = 1$, $5 + 2^{n+1} = 9$, which is indeed x_1; and when $n = 2$, $5 + 2^{n+1} = 13$, which equals x_2, so these hold. Assume inductively that $k \in \mathbb{N}$ and that, for all $s \leq k$, $x_s = 5 + 2^{s+1}$. (Note that, here, we use strong induction. This is because x_{k+1} depends not only on x_k but on x_{k-1} too.) In particular, therefore, we have $x_k = 5 + 2^{k+1}$ and $x_{k-1} = 5 + 2^k$. So,

$$\begin{aligned}
x_{k+1} &= 3x_k - 2x_{k-1} \\
&= 3(5 + 2^{k+1}) - 2(5 + 2^k) \\
&= 15 - 10 + 3(2^{k+1}) - 10 - 2(2^k) \\
&= 5 + 3(2^{k+1}) - 2(2^k) \\
&= 5 + 6(2^k) - 2(2^k) \\
&= 5 + 4(2^k) \\
&= 5 + 2^{k+2} \\
&= 5 + 2^{(k+1)+1},
\end{aligned}$$

which is exactly what we need. So the formula for x_n holds for all n.

3.7 Using the axioms for the natural numbers

Earlier, we said that the following results follow from the axioms for $\mathbb{N}$.

(P1) For all $a, b, c \in \mathbb{N}$, $(a + b) \times c = (a \times c) + (b \times c)$.

(P2) If $a, b \in \mathbb{N}$ satisfy $a \times b = a$, then $b = 1$.

(P3) For $a, b, c \in \mathbb{N}$, if $a < b$ and $b < c$, then $a < c$. [Transitivity]

(P4) For $a, b, c \in \mathbb{N}$, if $a < b$ then $a + c < b + c$ and $a \times c < b \times c$.

(P5) 1 is the least element of $\mathbb{N}$.

(P6) 1 is not equal to 1+1.

Let's see why.

Proof of (P1) For all $a, b, c \in \mathbb{N}$, $(a + b) \times c = (a \times c) + (b \times c)$.

$$\begin{aligned} (a+b) \times c &= c \times (a+b) && \text{by } (\mathbb{N}\mathbf{5}) \text{ [Commutative]} \\ &= (c \times a) + (c \times b) && \text{by } (\mathbb{N}\mathbf{7}) \text{ [Distributive]} \\ &= (a \times c) + (b \times c) && \text{by } (\mathbb{N}\mathbf{5}) \text{ [Commutative]} \end{aligned}$$ □

Proof of (P2) If $a, b \in \mathbb{N}$ satisfy $a \times b = a$, then $b = 1$.

Suppose $a \times b = a$. Then, since (by ($\mathbb{N}$**8**)), $a = a \times 1$, so we have $a \times b = a \times 1$. By ($\mathbb{N}$**5**) [Commutative], it follows that $b \times a = 1 \times a$. But now by ($\mathbb{N}$**10**) [Cancellation], we conclude $b = 1$. □

Proof of (P3) For $a, b, c \in \mathbb{N}$, if $a < b$ and $b < c$, then $a < c$. [Transitivity]

If $a < b$ and $b < c$ then, by ($\mathbb{N}$**11**), there are $x, y \in \mathbb{N}$ such that $a + x = b$ and $b + y = c$. Then we have

$$\begin{aligned} a + (x + y) &= (a + x) + y && \text{by } (\mathbb{N}\mathbf{3}) \text{ [Associativity]} \\ &= b + y = c\,, && \text{by definition of } b \text{ and } c \end{aligned}$$

Now by ($\mathbb{N}$**1**) [Closure], we have $x + y \in \mathbb{N}$, so by ($\mathbb{N}$**11**), we have $a < c$. □

Proof of (P4) For $a, b, c \in \mathbb{N}$, if $a < b$ then $a + c < b + c$ and $a \times c < b \times c$.

If $a < b$ then (by ($\mathbb{N}$**11**)) this means $\exists d \in \mathbb{N}$ with $a + d = b$.

(i) We prove $a + c < b + c$. We have:

$$\begin{aligned} (a + c) + d &= d + (a + c) && \text{by } (\mathbb{N}\mathbf{2}) \\ &= (d + a) + c && \text{by } (\mathbb{N}\mathbf{3}) \\ &= (a + d) + c && \text{by } (\mathbb{N}\mathbf{2}) \\ &= b + c\,. \end{aligned}$$

This shows $a + c < b + c$ by ($\mathbb{N}$**11**).

(ii) We prove $a \times c < b \times c$. We have:
$(a \times c) + (d \times c) = (a + d) \times c$. This is **(P1)** from above.
So, since $a + d = b$, we have $(a \times c) + (d \times c) = b \times c$.

Since $d \times c \in \mathbb{N}$ by ($\mathbb{N}$**4**), we have a natural number $z = d \times c$ such that $(a \times c) + z = (b \times c)$. So, by ($\mathbb{N}$**11**), we conclude $a \times c < b \times c$. □

Proof of (P5) 1 is the least element of $\mathbb{N}$.

By ($\mathbb{N}$**13**) [Well-ordering], $\mathbb{N}$ has a least member. Call it a. Suppose $a \neq 1$.
Axiom ($\mathbb{N}$**12**) says $a < 1$ or $a = 1$ or $1 < a$. We are assuming $a \neq 1$ and can't have $1 < a$, because otherwise 1 is smaller than a, which is a contradiction to our assumption that a is a least element of $\mathbb{N}$. So $a < 1$. Now we have By **(P4)**, we have $a \times a < 1 \times a$. But by ($\mathbb{N}$**5**) [Commutativity] and by ($\mathbb{N}$**8**), we get $1 \times a = a \times 1 = a$. So we can conclude:

$$a \times a < a.$$

But $a \times a \in \mathbb{N}$ by ($\mathbb{N}$**4**) [Closure], and this contradicts the assumption that a is a least element of $\mathbb{N}$. □

Proof of (P6) 1 is not equal to $1 + 1$.

($\mathbb{N}$**11**) says $a < b$ if and only if there is some $c \in \mathbb{N}$ with $a + c = b$. So $1 < 1 + 1$.

But ($\mathbb{N}$**12**) says that for all $a, b \in \mathbb{N}$, exactly one of the following is true: $a = b$, $a < b$, $b < a$. So we do not have $1 = 1 + 1$. □

3.7.1 Why do we give proofs from the axioms?

We already explained that one reason to prove statements about the natural numbers using only the axioms is to make sure everyone is going to agree about which statements are provably true—everyone agrees on the axioms, and if anyone can prove some statement true, we will all accept it. But you might well feel this is taking it a bit far—after all, we also all agree on how arithmetic with the natural numbers works without writing down axioms.

Another reason is that we will often find that we can prove a statement using only some of the axioms. Go back to the proof on page 8—you'll see that although we are using some of the axioms of the natural numbers, we are not using all of them. The axioms we are using define a *commutative semiring*. (You don't need to remember that name for later—it isn't one you are likely to need to know in your degree course.) There are many examples of commutative semirings in mathematics. Some are ones you already have some intuition for (like the natural numbers, or the real numbers), some you probably are less comfortable with (like the complex numbers) and most of them you never heard of (like bounded distributive lattices). But even without knowing what a bounded distributive lattice is, you already know some things you can do with one.

The more mathematics you learn, the more often you will find that when a new area is introduced to you, even though the concrete structures you have to work with are unfamiliar, you know a lot about these structures already because they are examples

of abstract (defined by axioms) structures which you study in MA103 and its successor courses. At least, that's true if you are willing to put the effort in in this course and learn how to work with axiomatic definitions and write proofs using axioms—otherwise, you'll need to learn everything from scratch and remember it separately every time you come across a new concrete structure.

Finally, and most concretely, we are studying the axioms for the natural numbers so that you get used to writing axiomatic proofs of facts which you already know are true, and for which you basically understand why those facts are true. That way you only have to learn one difficult thing now, and when you come to the abstract algebra in Lent Term, you will only have to learn one difficult thing, namely what one can do with the axioms of a vector space or of a group, instead of trying to learn that and how to write an axiomatic proof at the same time.

3.8 Why the Principle of Induction works

We can now **Prove** the Principle of Induction from our axioms for the natural numbers (including the least element axiom).

Theorem 3.1 (The Induction Principle) Suppose

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$.

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

Proof. Suppose it's not the case that $P(n)$ is true for all $n \in \mathbb{N}$. Then the set S of $n \in \mathbb{N}$ for which it is not true is non-empty and, by the Least Element Axiom ($\mathbb{N}$**13**), has a least member a. Now, $a \neq 1$ because $P(1)$ is true. And we can't have $a < 1$ because by **(P5)** 1 is the least member of $\mathbb{N}$. So, by ($\mathbb{N}$**12**) we have $1 < a$. Consider $a - 1$: this is a natural number less than a and is therefore not in S. So $P(a-1)$ is true. But since $P(k) \Rightarrow P(k+1)$ for all k, it follows that $P(a)$ is true, meaning $a \notin S$, a contradiction. □

You might not be entirely satisfied with that proof. It used $a - 1$ but we haven't defined subtraction! Here's another way of explaining the last bit:

Since $1 < a$, by ($\mathbb{N}$**11**) there is some $c \in \mathbb{N}$ such that $1 + c = a$. By ($\mathbb{N}$**2**) [Commutativity] we have $c + 1 = a$, which, by ($\mathbb{N}$**11**) means $c < a$. So, because a is the least element of S we have $c \notin S$ and hence $P(c)$ is true. But $P(c) \Rightarrow P(c+1)$ and hence $P(a)$ is true, a contradiction.

3.9 Non-examinable: There's only one $\mathbb{N}$.

Dedekind proved that there is really only one mathematical structure which satisfies the axioms ($\mathbb{N}$**1**)–($\mathbb{N}$**13**). Remember that what that means is that if you give me two structures which satisfy the axioms, then I should be able to find a dictionary-style

correspondence between them, such as between the natural numbers written in English and in German.

In this section, we are going to explain how to find that correspondence and prove (or at least, prove the interesting part of) the fact that it works.

Proof. Suppose that $\mathbb{N}$ and $\mathbb{M}$ are two different mathematical structures which both satisfy axioms ($\mathbb{N}$**1**)–($\mathbb{N}$**13**). Let's assume that $\mathbb{N}$ is the natural numbers you learnt about in school.

To start with, we claim that in $\mathbb{N}$ there is only one element 1 which satisfies ($\mathbb{N}$**8**). To see that this is true, suppose for a contradiction that there is another element $1'$ which also satisfies ($\mathbb{N}$**8**), i.e. for every $n \in \mathbb{N}$ we have $n \times 1' = n$. But then we have

$$1' = 1' \times 1 = 1 \times 1' = 1$$

where we used ($\mathbb{N}$**5**) [Commutativity] for the middle equality, and the other two equalities are because both 1 and $1'$ are assumed to satisfy ($\mathbb{N}$**8**). So we have $1 = 1'$, which is a contradiction and so our claim is proved.

Let's call the element of $\mathbb{M}$ which satisfies ($\mathbb{N}$**8**) 'one' (just to make it visually different from 1). There is only one such element by the proof above—that proof applies equally well to $\mathbb{M}$ as to $\mathbb{N}$ (because it only uses the axioms, and $\mathbb{M}$ satisfies the axioms). So now we have the first entry in our correspondence dictionary: 1 in $\mathbb{N}$ corresponds to 'one' in $\mathbb{M}$.

Now we can extend it: recall we defined 2 to be shorthand for $1 + 1$, and by **(P6)** we know 2 is not equal to 1. Similarly, we can define 'two' to be shorthand for 'one plus one' in $\mathbb{M}$, and **(P6)** also shows that 'two' is not equal to 'one' (because it only uses the axioms, and $\mathbb{M}$ satisfies the axioms). So that's our next entry in the dictionary: 2 corresponds to 'two'. And we can keep going like this; we can let $3 = 2 + 1$ correspond to 'three', defined to be shorthand for 'two plus one', and so on. One can show that all these numbers are different, but we are going to skip this because it is basically the same as proving **(P6)**.

It is not too hard (but it is time-consuming, because there are lots of things to check) to show that $+$, $\times$ and $<$ in $\mathbb{N}$ do the same as 'plus', 'times' and 'less than' in $\mathbb{M}$ using the axioms. We are going to skip this part too.

What is left is to prove that the correspondence we defined so far is really everything—that is, there are no elements in $\mathbb{N}$ which don't have a corresponding element in $\mathbb{M}$, and vice versa. Now, it might look obvious—how could it be otherwise? To see why there is still something to do, you should check that everything we did so far would have worked equally well if $\mathbb{M}$ was the set of positive real numbers. In that case, what we would have found is a correspondence between $\mathbb{N}$ and the positive integers within the positive real numbers—but there are many positive real numbers which are not integers, like 1.5437.

So suppose that the correspondence is not everything. There are two possibilities. First, there are some elements of $\mathbb{N}$ which don't have a corresponding element of $\mathbb{M}$. Second, there are some elements of $\mathbb{M}$ which don't have a corresponding member of $\mathbb{N}$.

To deal with the first case, let S be the set of elements of $\mathbb{N}$ which don't have a corresponding element in $\mathbb{M}$. By assumption, S is not the empty set, so by ($\mathbb{N}$**13**), the

set S has a least element s. Now s is not equal to 1, because 1 does have a corresponding member 'one' in $\mathbb{M}$. As in the proof of the Principle of Induction, that means there is some $c \in \mathbb{N}$ such that $c + 1 = s$, and we have $c < s$. But by definition of S that means c does have a corresponding member in $\mathbb{M}$, call it 'cee'. And by the way we constructed the correspondence, that means $c + 1 = s$ corresponds to 'cee plus one'. But this is a contradiction—we assumed s does not have a corresponding member in $\mathbb{M}$.

The second case is very similar. Let T be the set of elements of $\mathbb{M}$ which don't have a corresponding element in $\mathbb{N}$. By assumption, T is not the empty set, so by ($\mathbb{N}$**13**) (which also applies to $\mathbb{M}$..!) the set T has a least element, call it 'tee'. We know 'tee' is not 'one', because 'one' corresponds to 1. So there is an element 'dee' in $\mathbb{M}$ such that 'dee plus one' equals 'tee' (using the same axioms as in the first case). Since 'dee' is less than 'tee', it has a corresponding element d in $\mathbb{N}$. But then again we see 'tee', which is equal to 'dee plus one', corresponds to $d + 1$—a contradiction. □

If you want to see the parts we skipped, either work out for yourself how to prove them, or you can look them up in books on 'foundations of mathematics'. In the latter case, you should be aware that the axioms we gave for the natural numbers are not the usual ones, called the 'Peano axioms'. There are fewer Peano axioms than we have, and they are simpler (but a bit strange). The reason for giving you a longer and more complicated list of axioms is that you will see very similar axioms repeatedly in your degree course; your practice with these axioms will help you in the rest of your degree course. That wouldn't be the case with the Peano axioms.

3.10 Non-examinable philosophical interlude

If you are especially sceptical, you might notice we did make an assumption in this chapter. We proved that any two structures which satisfy ($\mathbb{N}$**1**)–($\mathbb{N}$**13**) are basically the same, in that there is a dictionary correspondence between them (the usual word for this is *isomorphic*). But we didn't actually prove that there *is* a structure which satisfies these axioms, so a more accurate title would be 'There is at most one $\mathbb{N}$'. You can find ways to avoid this; for example there is a standard set of axioms for set theory, called ZFC, which you can use to prove that there is such a thing as $\mathbb{N}$. But then you are assuming there is actually such a thing as set theory... In the end, you will always have some assumption (most mathematicians, if we think about this at all, assume ZFC set theory makes sense and stop there).

The problem is this: it might happen that there is some statement P about the natural numbers which you can prove true from the axioms, and also you can prove $\neg P$. This is a contradiction, which would make the axioms *inconsistent*; it means they don't actually describe anything—then we would say the natural numbers do not exist. I'll give an example of what this might look like at the end of this section, by giving a set of axioms (for something else, not the natural numbers) which does turn out to be inconsistent.

We believe the natural numbers are consistent: the natural numbers are something you have intuition about from the real world and we don't expect to find a logical contradiction in reality. But there have been axioms seriously proposed before (for

other, much more complicated structures about which we don't really have any intuition) which turned out to be inconsistent, and it's hard to argue that we have any intuition about natural numbers which are so enormous that all the particles in the known universe are too few to write them down.

What one might hope (and logicians did hope around 1900) is that you might be able to find some way of proving that the axioms (or at least some useful set of axioms) are consistent: perhaps all you really need to assume to do mathematics are the rules of logic. Around the same time, logicians also believed that perhaps every problem in mathematics can be solved: for every statement, you can either find a proof or a counterexample.

But these hopes turn out to be wrong. Gödel showed that any (finite) collection of axioms which describe an interesting structure (interesting enough to do arithmetic) cannot prove its own consistency. And what is more, there will be some statements which one cannot prove to be either true or false. These theorems are central parts of the area called 'foundations of mathematics'. But most mathematicians do not worry about it. We don't believe that there will turn out to be a contradiction in the mathematics we do, and we know that no matter how much we try we can't hope to improve belief to a certainty, so we don't think too much about it.

In your degree course, we are going to stick to what most mathematicians believe and do, meaning we will not spend time worrying about whether the natural numbers exist (and so on). And in fact, from the end of this chapter we will also stick to assuming that arithmetic in $\mathbb{N}$ works the way you know it does, rather than proving it using the axioms.

However, we will try to avoid making more assumptions. You were probably pretty much convinced, long before you started this course, that the natural numbers exist: i.e. there is no contradiction in the axioms; there is no calculation which you can do that will end up telling you $0 = 1$. If I asked you why, you'd probably say something about intuition from real world counting. Do you still have an intuition for how the integers (positive, negative and zero) behave? Well, probably you feel you do; on the other hand, it's a bit more removed from the real world—you will never count -3 apples. What about the rational numbers? or the real numbers? You probably will say you still have an intuition here from reality, but later in this course you'll see a few results which might convince you your intuition isn't as good as you think now. What about the complex numbers? Sure, they are needed to describe physical reality, but if you think your experience of the real world tells you that the complex numbers make sense, then you're fooling yourself.

Let's go into that in a little more detail. The complex numbers, if you saw them in school, were probably introduced more or less as follows. We start with the real numbers, which you know you can do algebra with as you're used to (they satisfy axioms ($\mathbb{N}\mathbf{1}$)–($\mathbb{N}\mathbf{8}$), for example). Then we add a symbol i, which is defined to solve the equation $x^2 + 1 = 0$ (or maybe is defined to be $\sqrt{-1}$). Then you write numbers like $2 + 4.3i$, and you can still do algebra as you're used to (just remember that whenever you see i^2 you can replace it with -1). Probably the justification given is more or less 'we want to have solutions to all equations, and sometimes we need to invent a new kind of number to make that true'.

This is a nice game; let's invent a new number system $\mathbb{E}$. It would be nice to be able to

divide by zero; so let's define a new symbol E, which should solve the equation $x \times 0 = 1$ (or equivalently, let $E = 1/0$). Presumably we can write numbers like $2 + 4.3E$, and do algebra as we're used to. It looks pretty similar to the complex numbers: what could possibly go wrong? Let's try a calculation.

$$\begin{aligned}
&\text{We have} && 0 = 0 + 0 \\
&\text{so} && E \times 0 = E \times (0 + 0) \\
&\text{so} && E \times 0 = E \times 0 + E \times 0 \\
&\text{so} && 1 = 1 + 1 \qquad .
\end{aligned}$$

Here the first line is obviously true (it's a statement about the integers, not our new number system). The second line is just multiplying both sides of the first line by E; no problem there. To get the third line we use the distributive law, which is algebra as we're used to. And for the final line we're just using the definition of E. But the final line is a false statement about the integers. So something is wrong.

What is wrong is that this new number system does *not* exist; we cannot have both a symbol E satisfying $E \times 0 = 1$ and the usual laws of arithmetic. It's not that there is a problem with writing down axioms: we can do that. Here is one possible set of axioms which the new number system we wanted should satisfy:

(**$\mathbb{E}$1**) For all $a, b \in \mathbb{E}$ we have $a + b \in \mathbb{E}$.

(**$\mathbb{E}$2**) For all $a, b \in \mathbb{E}$ we have $a + b = b + a$.

(**$\mathbb{E}$3**) For all $a, b, c \in \mathbb{E}$ we have $(a + b) + c = a + (b + c)$.

(**$\mathbb{E}$4**) For all $a, b \in \mathbb{E}$ we have $a \times b \in \mathbb{E}$.

(**$\mathbb{E}$5**) For all $a, b \in \mathbb{E}$ we have $a \times b = b \times a$.

(**$\mathbb{E}$6**) For all $a, b, c \in \mathbb{E}$ we have $(a \times b) \times c = a \times (b \times c)$.

(**$\mathbb{E}$7**) For all $a, b, c \in \mathbb{E}$ we have $a \times (b + c) = (a \times b) + (a \times c)$.

(**$\mathbb{E}$8**) For all $a, b, c \in \mathbb{E}$, if $a + c = b + c$ then $a = b$.

(**$\mathbb{E}$9**) There is an element 0 of $\mathbb{E}$ which satisfies $a + 0 = a$ for all $a \in \mathbb{E}$.

(**$\mathbb{E}$10**) There is an element 1 of $\mathbb{E}$, not equal to 0, which satisfies $a \times 1 = a$ for all $a \in \mathbb{E} \setminus \{0\}$.

(**$\mathbb{E}$11**) There is an element E of $\mathbb{E}$, which satisfies $E \times 0 = 1$.

Just to be clear, there is no difficulty with the first ten of these axioms. Those axioms are satisfied by lots of structures which you're happy with, like the integers, the rational numbers, the real numbers and the complex numbers. But if we add (**$\mathbb{E}$11**) we obtain a collection of axioms which are inconsistent: there is no structure satisfying all of them. The calculation we did above proves this, once we check that (using these axioms) we do not have $1 = 1 + 1$. Let's check that: by (**$\mathbb{E}$10**) we have $0 \neq 1$, and so by Axiom (**$\mathbb{E}$8**) we have $0 + 1 \neq 1 + 1$. By (**$\mathbb{E}$2**) we have $0 + 1 = 1 + 0$, and by Axiom (**$\mathbb{E}$9**) we have $1 + 0 = 1$. So indeed $1 \neq 1 + 1$.

If we replaced (**$\mathbb{E}$11**) with

(**𝔼11′**) There is an element i of $\mathbb{E}$, which satisfies $i^2 + 1 = 0$.

then the system of axioms would be satisfied by the complex numbers (among other structures). What's the difference: why is one collection of axioms inconsistent and the other is not? Do we need to assume that, and if so why should we actually believe it? We'll get to that later in the course.

3.11 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- understand what it means to say that a given structure satisfies some axioms, and why the axiomatic viewpoint is useful
- understand how the natural numbers can be defined by axioms and understand that other properties of natural numbers can be proved from the axioms, and know how to construct such proofs.
- state what is meant by a greatest and least member of a set of natural numbers and know what is meant by the well-ordering principle (or least element axiom)
- state and prove the Induction Principle and its variants
- use Proof by Induction to prove a range of statements, including those involving summation and recursive sequences

3.12 Sample exercises

Exercise 3.1
Prove by induction that, for all $n \in \mathbb{N}$, $2^n \geq n + 1$.

Exercise 3.2
Prove by induction that the sum $a + ar + ar^2 + \cdots + ar^{n-1}$ of the first n terms of a geometric progression with first term a and common ratio $r \neq 1$ is $a(1 - r^n)/(1 - r)$. □

Exercise 3.3
Prove by induction that for all $n \in \mathbb{N}$,

$$\sum_{r=1}^{n} r^2 = \frac{1}{6} n(n+1)(2n+1).$$

Exercise 3.4
Prove by induction that $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

Exercise 3.5
Suppose the sequence x_n is given by $x_1 = 7$, $x_2 = 23$ and, for $n \geq 3$, $x_n = 5x_{n-1} - 6x_{n-2}$. Prove by induction that, for all $n \in \mathbb{N}$, $x_n = 3^{n+1} - 2^n$.

Exercise 3.6
Prove by induction that, for all $n \in \mathbb{N}$, $2^{n+2} + 3^{2n+1}$ is divisible by 7.

Exercise 3.7
For a sequence of numbers $x_1, x_2, x_3, \ldots$, and for $n \in \mathbb{N}$, the number $\prod_{r=1}^{n} x_r$ is the product of the first r numbers of the sequence. It can be defined inductively as follows:

$$\prod_{r=1}^{1} x_r = x_1, \quad \text{and} \quad \text{for } k \geq 1, \prod_{r=1}^{k+1} x_r = \left(\prod_{r=1}^{k} x_r \right) x_{k+1}.$$

Suppose that $x \neq 1$. Prove that

$$\prod_{r=1}^{n} (1 + x^{2^{r-1}}) = \frac{1 - x^{2^n}}{1 - x}.$$

3.13 Comments on selected activities

Learning activity 3.1 As written, this activity is easy—for example, the set of all real numbers obviously doesn't have a least member. How can we prove this? Well, the easy way is by contradiction. Suppose for a contradiction that there is a least real number, call it a. But then $a - 1$ is a real number, and it is less than a; this is a contradiction and we are done.

But of course I really wanted to have a set of *positive* real numbers which doesn't have a least member. Actually, this is pretty easy too—especially once we saw the proof above. Let's just take the set of all positive real numbers. Suppose that has a least member b, for a contradiction. But then $b/2$ is a positive real number, and it's smaller than b, which is a contradiction and we're done.

Learning activity 3.3 When $n = 4$, $n^2 = 16$ and $2^n = 2^4 = 16$, so in this base case, the statement is true. Suppose we make the inductive hypothesis that for some $k \geq 4$, $k^2 \leq 2^k$. We want to show

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

We have

$$(k+1)^2 = k^2 + 2k + 1 \leq 2^k + 2k + 1$$

(by the inductive hypothesis). So we'll be done if we can show that $2k + 1 \leq 2^k$. This will follow from $2k + 1 \leq k^2$ and the assumed fact that $k^2 \leq 2^k$. Now,

$$2k + 1 \leq k^2 \iff k^2 - 2k - 1 \geq 0 \iff (k-1)^2 \geq 2,$$

which is true for $k \geq 4$. So, finally,

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

as required. So the result is true for all $n \geq 4$.

Learning activity 3.4 Let $Q(n)$ be the statement '$\forall s \leq n,\ P(s)$ is true'. Then $Q(1)$ is true if and only if $P(1)$ is true. The statement $Q(k) \Rightarrow Q(k+1)$ is the same as

$$(P(s) \text{ true } \forall s \leq k) \Rightarrow (P(s) \text{ true } \forall s \leq k+1).$$

But if $P(s)$ is true for all $s \leq k$ then its truth for all $s \leq k+1$ follows just from its truth when $s = k+1$. That is, $Q(k) \Rightarrow Q(k+1)$ is the same as
$(P(s)$ true $\forall s \leq k) \Rightarrow P(k+1)$. The (standard) Induction Principle applied to the statement $Q(n)$ tells us that: $Q(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $Q(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $Q(k) \Rightarrow Q(k+1)$.

What we've established is that (i) and (ii) can be rewritten as:

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $(P(s)$ true $\forall s \leq k) \Rightarrow P(k+1)$.

We deduce that: $P(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $(P(s)$ true $\forall s \leq k) \Rightarrow P(k+1)$.

This is exactly the Strong Induction Principle. So the Strong Induction Principle follows from the standard one and is, therefore, not really 'stronger'.

Learning activity 3.5 Let $P(n)$ be the statement that the sum of the first n terms is $(n/2)(2a + (n-1)d)$. The base case is straightforward. The first term is a, and the formula $(n/2)(2a + (n-1)d)$ gives a when $n = 1$. Suppose that $P(k)$ holds, so the sum of the first k terms is $(k/2)(2a + (k-1)d)$. Now, the $(k+1)$st term is $a + kd$, so the sum of the first $k+1$ terms is therefore

$$\begin{aligned} a + kd + \frac{k}{2}(2a + (k-1)d) &= a + kd + ak + \frac{k(k-1)}{2}d \\ &= (k+1)a + \frac{k(k+1)}{2}d \\ &= \frac{(k+1)}{2}(2a + kd) \\ &= \frac{(k+1)}{2}(2a + ((k+1)-1)d), \end{aligned}$$

so $P(k+1)$ is true. The result follows for all n by induction.

3.14 Solutions to exercises

Solution to exercise 3.1

Let $P(n)$ be the statement '$2^n \geq n+1$'. When $n = 1$, $2^n = 2$ and $n+1 = 2$, so $P(1)$ is true. Suppose $P(k)$ is true for some $k \in \mathbb{N}$. Then $2^k \geq k+1$. It follows that

$$2^{k+1} = 2.2^k \geq 2(k+1) = 2k+2 \geq k+2 = (k+1)+1,$$

so $P(k+1)$ is also true. Hence, by induction, for all $n \in \mathbb{N}$, $2^n \geq n+1$. □

Solution to exercise 3.2
Let $P(n)$ be the statement that the sum of the first n terms is $a(1-r^n)/(1-r)$. $P(1)$ states that the first term is $a(1-r^1)/(1-r) = a$, which is true. Suppose $P(k)$ is true. Then the sum of the first $k+1$ terms is the sum of the first k plus the $(k+1)$st term, which is ar^k, so this sum is

$$\begin{aligned}\frac{a(1-r^k)}{1-r} + ar^k &= \frac{a(1-r^k)+(1-r)ar^k}{1-r} \\ &= \frac{a-ar^k+ar^k-ar^{k+1}}{1-r} \\ &= \frac{a(1-r^{k+1})}{1-r},\end{aligned}$$

which shows that $P(k+1)$ is true. Hence, for all $n \in \mathbb{N}$, $P(n)$ is true, by induction. □

Solution to exercise 3.3
Let $P(n)$ be the statement that

$$\sum_{r=1}^{n} r^2 = \frac{1}{6}n(n+1)(2n+1).$$

Then $P(1)$ states that $1 = 1(2)(3)/6$, which is true. Suppose $P(k)$ is true for $k \in \mathbb{N}$. Then

$$\sum_{r=1}^{k} r^2 = \frac{1}{6}k(k+1)(2k+1)$$

and $P(k+1)$ is the statement that

$$\sum_{r=1}^{k+1} r^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1) = \frac{1}{6}(k+1)(k+2)(2k+3).$$

We have

$$\begin{aligned}\sum_{r=1}^{k+1} r^2 &= (k+1)^2 + \sum_{r=1}^{k} r^2 \\ &= (k+1)^2 + \frac{1}{6}k(k+1)(2k+1) \quad \text{(by the induction hypothesis)} \\ &= \frac{1}{6}(k+1)\left[6(k+1)+k(2k+1)\right] \\ &= \frac{1}{6}(k+1)\left(2k^2+7k+6\right) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3),\end{aligned}$$

so $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Solution to exercise 3.4
Let $P(n)$ be the statement that $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$. Then $P(1)$ states that $\dfrac{1}{1\times 2} = \dfrac{1}{1+1}$, which is true. Suppose $P(k)$ is true for $k \in \mathbb{N}$. Then

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

and $P(k+1)$ is the statement that

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

Now,

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

so $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Solution to exercise 3.5

Let $P(n)$ be the statement that $x_n = 3^{n+1} - 2^n$. We use the Strong Induction Principle to prove $P(n)$ is true for all $n \in \mathbb{N}$. The base cases are $n = 1$ and $n = 2$. When $n = 1$, $x_1 = 7$ and $3^{n+1} - 2^n = 9 - 2 = 7$. When $n = 2$, $x_2 = 23$ and $3^{n+1} - 2^n = 27 - 4 = 23$, so these are true. Suppose that $k \geq 2$ and that for all $s \leq k$, $P(s)$ is true. In particular, $P(k)$ and $P(k-1)$ are true and so

$$\begin{aligned}
x_{k+1} &= 5x_k - 6x_{k-1} \\
&= 5(3^{k+1} - 2^k) - 6(3^k - 2^{k-1}) \\
&= 5(3^{k+1}) - 5(2^k) - 6(3^k) + 6(2^{k-1}) \\
&= 15(3^k) - 6(3^k) - 10(2^{k-1}) + 6(2^{k-1}) \\
&= 9(3^k) - 4(2^{k-1}) \\
&= 3^{k+2} - 2^{k+1} \\
&= 3^{(k+1)+1} - 2^{k+1},
\end{aligned}$$

so $P(k+1)$ is true. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. □

Solution to exercise 3.6

Let $P(n)$ be the statement that $2^{n+2} + 3^{2n+1}$ is divisible by 7. When $n = 1$, $2^{n+2} + 3^{2n+1} = 8 + 27 = 35$ and this is a multiple of 7 because $35 = 5 \times 7$. Suppose $P(k)$ is true, which means that for some $m \in \mathbb{N}$, $2^{k+2} + 3^{2k+1} = 7m$. Now, when we take

$n = k+1$,

$$\begin{aligned} 2^{n+2} + 3^{2n+1} &= 2^{k+3} + 3^{2k+3} \\ &= 2(2^{k+2}) + 9(3^{2k+1}) \\ &= 2(2^{k+2} + 3^{2k+1}) + 7(3^{2k+1}) \\ &= 14m + 7(3^{2k+1}) \\ &= 7\left(2m + 3^{2k+1}\right), \end{aligned}$$

which is a multiple of 7. So the statement is true for $P(k+1)$. This proves $P(k) \Rightarrow P(k+1)$, the induction step, and hence, by induction, for all $n \in \mathbb{N}$. □

Solution to exercise 3.7

Let $P(n)$ be the statement

$$\prod_{r=1}^{n}(1 + x^{2^{r-1}}) = \frac{1 - x^{2^n}}{1 - x}.$$

When $n = 1$, the left hand side is $1 + x^{2^0} = 1 + x$ and the right hand side is $(1 - x^2)/(1 - x) = 1 + x$, so $P(1)$ is true. Suppose $P(k)$ is true, so that

$$\prod_{r=1}^{k}(1 + x^{2^{r-1}}) = \frac{1 - x^{2^k}}{1 - x}.$$

Then

$$\begin{aligned} \prod_{r=1}^{k+1}(1 + x^{2^{r-1}}) &= (1 + x^{2^{(k+1)-1}}) \times \prod_{r=1}^{k}(1 + x^{2^{r-1}}) \\ &= (1 + x^{2^k})\frac{1 - x^{2^k}}{1 - x} \quad \text{(by the induction hypothesis)} \\ &= \frac{1 - (x^{2^k})^2}{1 - x} \quad \text{(where we've used } (1+y)(1-y) = 1 - y^2) \\ &= \frac{1 - x^{2^k \times 2}}{1 - x} \\ &= \frac{1 - x^{2^{k+1}}}{1 - x}, \end{aligned}$$

which shows that $P(k+1)$ is true. So $P(n)$ is true for all $n \in \mathbb{N}$, by induction.

Chapter 4
Functions and counting

☞ Biggs, N. L. *Discrete Mathematics*. Chapters 5 and 6.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapter 10, Sections 10.1 and 10.2, and Chapter 11.

4.1 Introduction

In this chapter we look at the theory of functions, and we see how the idea of the 'size' of a set can be formalised.

4.2 Functions

4.2.1 Basic definitions

You have worked extensively with functions in your previous mathematical study. Chiefly, you will have worked with functions from the real numbers to the real numbers, these being the primary objects of interest in calculus.

You are probably used to writing a function down by writing a formula, something like '$f(x) = x^2 + \sin x$'. This is *not* the approach we are going to take, because it's too restrictive. For a very simple example, take the function $g(x)$ which is defined as follows:

$$g(x) = \begin{cases} 0 & \text{if } x \leq 11850\,, \\ \frac{1}{5}(x - 11850) & \text{if } 11851 \leq x \leq 46350 \text{ and} \\ \frac{2}{5}(x - 46350) + 6900 & \text{if } x \geq 46351\,. \end{cases}$$

This is a perfectly good function, but finding a single formula for it is a bit tricky. Furthermore, once you find it you'll notice that the formula is much less helpful than the definition above. This function was actually an important function (at least in the UK): it's the (in 2018) income tax you pay on income £x.

Activity 4.1 Find a single formula which gives the function $g(x)$ above.

So we do not want to think of 'function' as meaning 'defined by a formula'. In fact, we don't want to think about how to go from the input x to the output $f(x)$ at all—we will think of a function as a 'black box' which takes in a number and spits out a number; the only rule is that we insist that it always spits out the same number.

Actually, even that is too restrictive; we don't want to insist that the input or output is a number. Maybe we would like the input or output to be 'Yes', or 'No', or a colour, or a social network... we need a definition which allows any of these possibilities. The only thing we want to stick to is: if we give the function the same input twice, we should get the same output each time. Here is the definition which formalises this.

Definition 4.1 Suppose that X and Y are sets. Then a *function* (also known as a *mapping*) from X to Y is a rule that associates a unique member of Y to each member of X. We write $f : X \to Y$. The set X is called the *domain* of f and Y is called the *codomain*.

The element of Y that is assigned to $x \in X$ is denoted by $f(x)$ and is called the *image* of x. We can write $x \mapsto f(x)$ to indicate that x maps to $f(x)$.

There are lots of examples of functions you already know, such as $\sin x$, or $g(x)$ defined above. Another example function is Drink, with domain $\{\text{Beer}, \text{Milk}\}$ and codomain $\{\text{Yes}, \text{No}, \text{Maybe}\}$ which is defined by $\text{Drink}(\text{Milk}) = \text{Maybe}$ and $\text{Drink}(\text{Beer}) = \text{Yes}$. If you have a social network, then that social network contains a number of friendships (i.e. pairs of people who are friends); that defines a function from social networks to the integers, which given a social network returns the total number of friendships. If you have a road map of some country, then there may or there may not be a way to drive through all the villages without ever having to return to a village you already visited. That defines a function from road maps to $\{\text{Yes}, \text{No}\}$. You can also generate your own personal function as follows. Throw a die 1 000 000 times, and write down the numbers in order that you get—that defines you a function from $\{1, \ldots, 1\,000\,000\}$ to $\{1, \ldots, 6\}$. (It's extremely unlikely anyone ever wrote down your personal function before. Of course, the next time you try this you are very likely to get a different function..!)

Some of these functions are easier to work with, or more interesting, than others. You know $\sin x$ shows up a lot in real-world calculations (in engineering, for example), and you know how to do algebra and calculus with it. The Drink function describes your lecturer's preferences—it might not be very interesting, but at least it's easy to describe. What about the road map function? If you're a fraudster, you need to keep moving on, and you probably care a lot about not going back to villages where you already conned people—but how do you actually work out, for a given road map with maybe 50 000 villages, whether the answer is 'Yes' or 'No'? It's an interesting function, but it's very hard to work with. Finally, what about one of these generated-by-dice functions? It's not easy to describe—you don't want to read a list a million characters long—and it's not clear what it should be useful for. Often (but certainly not all the time), we are really only interested in functions which we can describe in some useful way.

There are various ways of describing a function. If X has only finitely many members, we can simply list the images of the members of X. You're used to seeing a function defined by giving a formula for the function. For instance, $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is the function that maps each real number a to the real number $2a$.

Sometimes a function can be defined *recursively*. For example, we might define $f : \mathbb{N} \to \mathbb{N}$ by

$$f(1) = 1 \quad \text{and} \quad f(n) = 2 + 3f(n-1), \quad \text{for } n \geq 2\,.$$

(You can see that the sequence of numbers $f(1), f(2), f(3), \ldots$ is therefore given by a first order difference equation.)

What does it mean to say that two functions f and g are equal? Well, first, they must have the same domain X and codomain Y. Then, for each $x \in X$, we must have $f(x) = g(x)$. For example, if $\mathbb{R}^+$ is the set of positive real numbers, then the function $f : \mathbb{R}^+ \to \mathbb{R}$ given by $f(x) = x^2$ and the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ are *not* equal because their domains are different.

You might think it is picky to say that, for example, the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$ and the function $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $g(x) = x^2$ are different (The set $\mathbb{R}_{\geq 0}$ is the non-negative real numbers). After all, what you can put into both functions is the same, and what comes out is also the same—the only difference is that the codomains of f and g are different. However, it turns out often to be important what the codomain is—for example, we'll see later that only one of f and g is a bijection.

Finally, we define one very basic function. For any set X, the *identity* function $\mathbb{1} : X \to X$ is given by $\mathbb{1}(x) = x$.

4.2.2 Composition of functions

Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Then the *composition* $g \circ f$, also denoted by gf, is the function from X to Z given by

$$(g \circ f)(x) = g\big(f(x)\big) \quad \text{for} \quad x \in X\,.$$

If X and Z are distinct sets, there is only one way we can compose f and g. For example, given the function RightTime : $\{\text{Morning}, \text{Evening}\} \to \{\text{Beer}, \text{Milk}\}$ defined by RightTime(Morning) = Milk and RightTime(Evening) = Beer, it makes sense to talk about Drink $\circ$ RightTime. I think that in the morning it's the right time for milk, and in the evening it's the right time for beer. So if we put Morning into the composition Drink $\circ$ RightTime, then we can see that I will Maybe have a drink in the morning. It doesn't make sense to consider RightTime $\circ$ Drink, because whatever input from $\{\text{Beer}, \text{Milk}\}$ we put into Drink the output is something not in the domain of RightTime; that function doesn't know what to do with an input Maybe.

If $X = Z$, then both $f \circ g$ and $g \circ f$ make sense—but they are generally *not* the same function: the order is important. A further point to be careful about is that the notation fg can cause confusion. For example, suppose $X = Y = Z = \mathbb{R}$. Then you might be tempted to think that gf denotes the *product* function $x \to g(x)f(x)$. But this would be wrong. It should always be clear from the context whether gf should be interpreted as a composition. If I need to talk about the product of the functions f and g I will denote this by $f(x)g(x)$. The notation $g \circ f$ leads to less confusion, but it is not used in all textbooks.

> **Example 4.1** Suppose $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$ are given by $f(x) = x^2 + 1$ and $g(x) = (x+1)^2$. Then,
>
> $$(f \circ g)(x) = f\big(g(x)\big) = f\big((x+1)^2\big) = \big((x+1)^2\big)^2 + 1 = (x+1)^4 + 1.$$

And,

$$(g \circ f)(x) = g\big(f(x)\big) = g\big(x^2+1\big) = \big((x^2+1)+1\big)^2 = (x^2+2)^2.$$

4.3 Bijections, surjections and injections

There are three very important properties that a function might possess:

Definition 4.2 (Surjection) Suppose f is a function with domain X and codomain Y. Then f is said to be a *surjection* (or '*f is surjective*') if every $y \in Y$ is the image of some $x \in X$; that is, f is a surjection if and only if $\forall y \in Y, \exists x \in X, \text{s.t. } f(x) = y$.

Definition 4.3 (Injection) Suppose f is a function with domain X and codomain Y. Then f is said to be an *injection* (or '*f is injective*') if every $y \in Y$ is the image of *at most one* $x \in X$. In other words, the function is an injection if different elements of X have different images under f. Thus, f is an injection if and only if

$$\forall x, x' \in X, x \neq x' \Rightarrow f(x) \neq f(x')$$

or (equivalently, taking the contrapositive), if and only if

$$\forall x, x' \in X, f(x) = f(x') \Rightarrow x = x'.$$

This latter characterisation often provides the easiest way to verify that a function is an injection.

Definition 4.4 (Bijection) Suppose f is a function with domain X and codomain Y. Then f is said to be a *bijection* (or '*f is bijective*) if it is *both* an injection and a surjection. So this means two things: each $y \in Y$ is the image of some $x \in X$, and each $y \in Y$ is the image of no more than one $x \in X$. Well, of course, this is equivalent to: each $y \in Y$ is the image of *precisely one* $x \in X$.

Example 4.2 $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = 2x$ is not a surjection, because there is no $n \in \mathbb{N}$ such that $f(n) = 1$. (For, $2n = 1$ has no solution where $n \in \mathbb{N}$.) However, it is an injection. To prove this, suppose that $m, n \in \mathbb{N}$ and $f(m) = f(n)$. Then $2m = 2n$, which implies $m = n$.

Activity 4.2 Prove that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is a bijection.

4.3.1 An example

Let $X = \mathbb{R}$, the set of real numbers, and let Y be the interval $(-1, 1)$, the set of real numbers x such that $-1 < x < 1$. Then the function $f : X \to Y$ given by

$$f(x) = \frac{x}{1+|x|}$$

is a bijection from X to Y.

First, we prove f is **injective.** To do this, we prove that $f(x) = f(y)$ implies $x = y$. So, suppose $f(x) = f(y)$. Then

$$\frac{x}{1+|x|} = \frac{y}{1+|y|}.$$

So

$$x + x|y| = y + y|x|.$$

Because $x/(1+|x|) = y/(1+|y|)$, x and y are *both* non-negative or *both* negative. For, otherwise, one of $x/(1+|x|)$ and $y/(1+|y|)$ will be negative and the other one will be non-negative, which cannot be the case since they are equal. So, $x|y| = y|x|$, both being xy if $x, y \geq 0$ and $-xy$ if $x, y < 0$. So, we have $x = y$.

Next, we show f is **surjective.** We need to prove that, for each $y \in (-1, 1)$, there's $x \in \mathbb{R}$ such that $x/(1+|x|) = y$. Consider separately the case in which $y \geq 0$ and the case in which $y < 0$.

Suppose $y \geq 0$. Then, to have $x/(1+|x|) = y$, we need $x \geq 0$. So $|x| = x$ and we need to solve $x/(1+x) = y$. This has solution $x = y/(1-y)$, which is well-defined because we know $y < 1$.

Suppose $y < 0$. Then we'll need to have $x < 0$ and the equation to solve is $x/(1-x) = y$, for a solution $x = y/(1+y)$; this is also well-defined, since $y > -1$.

4.4 Inverse functions

4.4.1 Definition, and existence

Suppose we are given a function $f : X \to Y$. Then $g : Y \to X$ is an *inverse function* of f if $(g \circ f)(x) = x$ for all $x \in X$ and $(f \circ g)(y) = y$ for all $y \in Y$. An equivalent characterisation is that $y = f(x) \iff x = g(y)$.

The following theorem tells us precisely when a function has an inverse. It also tells us that if an inverse exists, then there is only one inverse. For this reason we can speak of *the* inverse function, and give it a specific notation, namely f^{-1}.

Theorem 4.1 $f : X \to Y$ has an inverse function if and only if f is a bijection. When f is bijective, there is a unique inverse function.

First, we prove:

$f : X \to Y$ has an inverse $\iff$ f is bijective.

Proof. This is an $\iff$ theorem, so there are two things to prove: the $\Leftarrow$ and the $\Rightarrow$.

First, we show: $f : X \to Y$ has an inverse $\Leftarrow$ f is bijective.

Suppose f is a bijection. For each $y \in Y$ there is exactly one $x \in X$ with $f(x) = y$. Define $g : Y \to X$ by $g(y) = x$. Then this is an inverse of f. Check this!

Next, we show: $f : X \to Y$ has an inverse $\Rightarrow$ f is bijective.

Suppose f has an inverse function g. We know that for any $y \in Y$,

$f(g(y)) = (f \circ g)(y) = y$, so there is some $x \in X$ (namely $x = g(y)$) such that $f(x) = y$. So f is surjective.

Now suppose $f(x) = f(x')$. Then $g(f(x)) = g(f(x'))$. But $g(f(x)) = (g \circ f)(x) = x$ and, similarly, $g(f(x')) = x'$. So: $x = x'$ and f is injective.

Now we prove that when f is bijective, the inverse is unique.

Suppose that g and h are inverses of f. Then both have domain Y and codomain X, and we just need to check that $g(y) = h(y)$ for every $y \in Y$. Well, $h \circ f$ is the identity function on X and $f \circ g$ is the identity function on Y. So, for any $y \in Y$ we have

$$g(y) = (h \circ f)\big(g(y)\big) = \big((h \circ f) \circ g\big)(y) = \big(h \circ (f \circ g)\big)(y) = h\big((f \circ g)(y)\big) = h(y)\,,$$

so $g = h$. □

Note that if $f : X \to Y$ is a bijection, then its inverse function (which exists, by Theorem 4.1) is also a bijection.

Again, you need to be a bit careful with the notation if your function is (for example) from $\mathbb{R}$ to $\mathbb{R}$. Do *not* confuse f^{-1}, the inverse function, with the function $x \to \big(f(x)\big)^{-1} = 1/f(x)$.

4.4.2 Examples

Example 4.3 The function $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = 3x + 1$. Find the inverse function.

To find a formula for f^{-1}, we use: $y = f(x) \iff x = f^{-1}(y)$. Now,

$$y = f(x) \iff y = 3x + 1 \iff x = (y - 1)/3,$$

so

$$f^{-1}(y) = \frac{1}{3}(y - 1).$$

Let $\mathbb{Z}$ denote the set of all integers (positive, zero, and negative).

Example 4.4 The function $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is defined as follows:

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -2n - 1 & \text{if } n < 0. \end{cases}$$

Prove that f is a bijection and determine a formula for the inverse function f^{-1}.

First, we prove that f is **injective**: Suppose $f(n) = f(m)$. Since $2n$ is even and $-2n - 1$ is odd, either (i) $n, m \geq 0$ or (ii) $n, m < 0$. (For otherwise, one of $f(n), f(m)$ is odd and the other even, and so they cannot be equal.)

In case (i), $f(n) = f(m)$ means $2n = 2m$, so $n = m$.

In case (ii), $f(n) = f(m)$ means $-2n - 1 = -2m - 1$, so $n = m$. Therefore f is injective.

Next, we prove that f is **surjective**: We show that $\forall m \in \mathbb{N} \cup \{0\}, \exists n \in \mathbb{Z}$ such that $f(n) = m$. Consider separately the case m even and the case m odd.

Suppose m is even. Then $n = m/2$ is a non-negative integer and $f(n)$ is $2(m/2) = m$).

If m odd, then $n = -(m+1)/2$ is a negative integer and

$$f(n) = f(-(m+1)/2) = -2\left(-\frac{(m+1)}{2}\right) - 1 = m.$$

The proof that f is surjective reveals to us what the inverse function is. We have

$$f^{-1}(m) = \begin{cases} m/2 & \text{if } m \text{ even} \\ -(m+1)/2 & \text{if } m \text{ odd.} \end{cases}$$

Finally, let's give an important non-example.

Example 4.5 Let $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be defined by $f(x) = x^2$, and let $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be defined by $g(x) = \sqrt{x}$.

It's tempting to think that g is the inverse function of f, and indeed $(f \circ g)(x) = x$ for all $x \in \mathbb{R}_{\geq 0}$. But $(g \circ f)(-1) = g(1) = 1$, because $\sqrt{x}$ means the *non-negative* square root of x. If you check Theorem 4.1 you'll see that in fact f doesn't have an inverse function: it is not a bijection. For example $f(1) = 1 = f(-1)$. It's a somewhat common mistake in basic algebra to assume $\sqrt{x^2} = x$; as we just saw it's not true when $x < 0$. We saw essentially this error as mistake (3) in Section 2.10.

4.5 Functions on sets

Suppose we have a function $f : X \to Y$. It is very common that, given some $S \subset X$, we want to talk about the set $\{f(x) : x \in S\}$. To make this easier, we define

$$f(S) = \{f(x) : x \in S\}.$$

Note that $f(\emptyset) = \emptyset$, and for any single $x \in X$ we have $f(\{x\}) = \{f(x)\}$. It's important to remember that $\{f(x)\}$ is *not* the same as $f(x)$ (in the same way that an apple in a box is not the same as an apple).

We also define, for *any* function $f : X \to Y$ and any $T \subset Y$, the set

$$f^{-1}(T) = \{x \in X : f(x) \in T\}.$$

Again, it's important to remember that for $y \in Y$, the set $f^{-1}(\{y\})$ is a set of elements in X, and it always exists, in contrast to $f^{-1}(y)$ which is a member of X and is only defined if f is an invertible function.

If f is invertible, then for every $y \in Y$ the set $f^{-1}(\{y\})$ contains exactly one element, namely $f^{-1}(y)$. However if f is not invertible, then by Theorem 4.1 either there will

be some $y \in Y$ such that $f^{-1}(\{y\}) = \emptyset$ (i.e. f is not surjective) or there will be some $y \in Y$ such that $f^{-1}(\{y\})$ has two or more elements (i.e. f is not injective), or both.

Given a function $f : X \to Y$, the set $f(X)$ is sometimes called the *image of* f. The image $f(X)$ of f is always a subset of the codomain Y (by definition!). It might be that $f(X) = Y$, or it might not be—by definition, $f(X) = Y$ if and only if f is surjective.

4.6 Counting as a bijection

What does it mean to say that a set has three objects? Well, it means that I can take an object from the set, and call that 'Object 1', then I can take a different object from the set and call that 'Object 2', and then I can take a different object from the set and call that 'Object 3', and then I have named all the objects in the set. Obvious, I know, but this is the fundamental way in which we can abstractly define what we mean by saying that a set has m members.

For $m \in \mathbb{N}$, let $\mathbb{N}_m$ be the set $\{1, 2, \ldots, m\}$ consisting of the first m natural numbers. Then we can make the following formal definition:

Definition 4.5 A set S has m members if there is a bijection from $\mathbb{N}_m$ to S.

So, the set has m members if to each number from 1 to m, we can assign a corresponding member of the set S, and all members of S are accounted for in this process. This is like the attachment of labels 'Object 1', etc, described above.

Note that an entirely equivalent definition is to say that S has m members if there is a bijection from S to $\mathbb{N}_m$. This is because if $f : \mathbb{N}_m \to S$ is a bijection, then the inverse function $f^{-1} : S \to \mathbb{N}_m$ is a bijection also. In fact, because of this, we can simply say that S has m members if there is a bijection 'between' $\mathbb{N}_m$ and S. (Eccles uses the definition that involves a bijection from $\mathbb{N}_m$ to S and Biggs uses the definition that involves a bijection from S to $\mathbb{N}_m$.)

For $m \in \mathbb{N}$, if S has m members, we say that S has *cardinality* m (or *size* m). The cardinality of S is denoted by $|S|$, so we would usually simply write $|S| = m$ for 'S has cardinality m'.

4.7 The pigeonhole principle

4.7.1 The principle

The 'pigeonhole principle' is something that you might find obvious, but it is very useful.

Informally, what it says is that says is that if you have n letters and you place them into m pigeonholes in such a way that no pigeonhole contains more than one letter, then $n \leq m$. Equivalently, if $n > m$ (so that you have more letters than pigeonholes), then some pigeonhole will end up containing more than one letter. This is very intuitive. Obvious as it may be, however, can you think about how you would

actually prove it? We shall prove it below. But let's state the principle more formally, first. Recall that, for $r \in \mathbb{N}$ we have $\mathbb{N}_r = \{1, 2, \ldots, r\}$.

Theorem 4.2 (Pigeonhole Principle (PP)) The following statement is true for all $n \in \mathbb{N}$: For all natural numbers m, if there is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$.

Proof. We prove this by induction. The statement we want to prove is the statement $P(n)$: 'if there is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$.' The base case, $n = 1$, is true because (since $m \in \mathbb{N}$), $1 \leq m$. Suppose $P(k)$ is true. We now want to show that $P(k+1)$ is also true. So suppose there is an injection $f : \mathbb{N}_{k+1} \to \mathbb{N}_m$. (What we want to show is that $k + 1 \leq m$.) Since $k \geq 1$, we have $k + 1 \geq 2$. Now we do not have $m = 1$, because if $m = 1$ then $\mathbb{N}_m = \{1\}$ and so the only possibility is $f(1) = f(2) = 1$, contradicting the assumption that f is an injection. Because m is a natural number, it follows that $m \geq 2$.

Since $m \geq 2$ we can write m as $m = s + 1$ where $s \in \mathbb{N}$. Now, either there is some $x \in \mathbb{N}_k = \{1, 2, \ldots, k\}$ with $f(x) = s + 1$, or there is not. Let's examine each case separately.

- Suppose, then, first, that for no $x \in \mathbb{N}_k$ do we have $f(x) = s + 1$. Then define $f_* : \mathbb{N}_k \to \mathbb{N}_s$ by $f_*(x) = f(x)$ for $x \in \mathbb{N}_k$. Then, because f is an injection, so too is f_*. So there is an injection (namely, f_*) from $\mathbb{N}_k$ to $\mathbb{N}_s$. By the induction hypothesis (applied to s instead of m), $k \leq s$ and hence $k + 1 \leq s + 1 = m$, as required.
- Now suppose that there is some $j \in \mathbb{N}_k$ such that $f(j) = s + 1$. Then the value $y = f(k + 1)$ must be different from $s + 1$ and therefore $y \in \mathbb{N}_s$. Define $f_{**} : \mathbb{N}_k \to \mathbb{N}_s$ by $f_{**}(j) = y$ and $f_{**}(x) = f(x)$ if $x \in \mathbb{N}_k \setminus \{j\}$. Then f_{**} maps from $\mathbb{N}_k$ to $\mathbb{N}_m$ and, furthermore, it is an injection. So, by the induction hypothesis, $k \leq s$ and hence $k + 1 \leq s + 1 = m$.

□

A consequence of this is:

Theorem 4.3 Suppose n, m are two natural numbers. If there is a bijection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n = m$.

Proof. Suppose $f : \mathbb{N}_n \to \mathbb{N}_m$ is a bijection. Then f is an injection. So from Theorem PP, $n \leq m$.

But there is an inverse function $f^{-1} : \mathbb{N}_m \to \mathbb{N}_n$ and this is also a bijection. In particular, f^{-1} is an injection from $\mathbb{N}_m$ to $\mathbb{N}_n$, and hence $m \leq n$.

Now we have both $n \leq m$ and $m \leq n$, hence $n = m$. □

A slightly more general form of the pigeonhole principle, easy to prove from that above is:

Theorem 4.4 Suppose that A and B are sets with $|A| = n$ and $|B| = m$, where $m, n \in \mathbb{N}$. If there is an injection from A to B, then $n \leq m$.

Proof. From the definition of counting, there are bijections $g : \mathbb{N}_n \to A$ and $h : \mathbb{N}_m \to B$. We also have an inverse bijection $h^{-1} : B \to \mathbb{N}_m$.

Suppose there is an injection $f : A \to B$. Consider the composite function $h^{-1} f g : \mathbb{N}_n \to \mathbb{N}_m$. If we can prove that this is an injection, then from Theorem 4.2 it follows that $n \leq m$.

So, let us prove injectivity. Suppose $a, b \in \mathbb{N}_n$ with $a \neq b$. Since g is a bijection $g(a), g(b) \in A$ with $g(a) \neq g(b)$. Since f is an injection, there are $f(g(a)), f(g(b)) \in B$ with $f(g(a)) \neq f(g(b))$. Since h^{-1} is a bijection, $h^{-1}(f(g(a)))$ and $h^{-1}(f(g(b)))$ belong to $\mathbb{N}_m$, and $h^{-1}(f(g(a))) \neq h^{-1}(f(g(b)))$. This last inequality is what we need. □

The pigeonhole principle is remarkably useful (even in some very advanced areas of mathematics). It has many applications. For most applications, it is the contrapositive form of the principle that is used. This states:

If $m < n$ and $f : \mathbb{N}_n \to \mathbb{N}_m$ is any function, then f is not an injection..

So, if $m < n$, and f is *any* function $f : \mathbb{N}_n \to \mathbb{N}_m$, then there are $x, y \in \mathbb{N}_n$ with $x \neq y$ such that $f(x) = f(y)$.

The name 'pigeonhole principle' comes from this last formulation. If you have m pigeonholes (named slots into which post is placed in a university) and n letters to put in them, where $n > m$, then there must be at least one pigeonhole into which two or more letters are placed.

4.7.2 What will be on the exam?

We've just seen our first 'long' proof which is examinable, the proof of the Pigeonhole Principle. You might be tempted to make a tactical guess that I will not ask you to reproduce this proof in the exam (which is correct, I won't ask it) and hence skip it. And you might think that it is too obvious to be interesting.

This would be an error. The proof is in the course for a reason: it's the first proof you have seen which uses 'abstract information' in a serious way, and I can and quite possibly will ask questions on the exam which test your ability to do something similar, maybe in a simpler scenario (the proof of PP is a bit too long for an exam question, and would be too hard if you hadn't seen it before).

You can break down the proof of the Pigeonhole Principle into several steps. The first is to try doing a proof by induction at all, and that the induction is on n (rather than m or some other parameter). It's not obvious why one should do that — but it works.

Once you think of induction on n, then it's obvious that the base case is true — we don't need to think at all about the condition 'if there is an injection from $\mathbb{N}_1$ to $\mathbb{N}_m$' at all, because $1 \leq m$ is true for all natural numbers m.

So the difficulty is to prove the induction step. Now, it is not obvious how to do this — it is certainly not the case that a Real Mathematician instantly sees how to do it. What we do is look for something more we can say, ideally something that will let us use our induction hypothesis. There is one more thing we can easily say. We are given that there is an injection from $\mathbb{N}_{k+1}$ to $\mathbb{N}_m$; in particular $k + 1$ is at least 2, and we can immediately rule out the possibility $m = 1$. Note we do *not* use the induction hypothesis to do this (even though we are in the middle of the induction step). That lets us write $m = s + 1$ for some natural number s, and the reason this is helpful is we

can now prove $k+1 \leq m$ by proving $k \leq s$.

Why is this helpful? Because the conclusion $k \leq s$ is what we would get from our induction hypothesis, if we could find an injection from $\mathbb{N}_k$ to $\mathbb{N}_s$. Now, in fact, most of what we just discussed is not really obvious; it's something you get to by trial and error (and experience, i.e. trying to solve problems, helps). But now we are at a point where there is really only one way to proceed.

We have an injection from $\mathbb{N}_{k+1}$ to $\mathbb{N}_{s+1}$, and we need to get from it an injection from $\mathbb{N}_k$ to $\mathbb{N}_s$. To start with, we *give a name* to the injection we are given, so we don't have to keep saying 'the injection from $\mathbb{N}_{k+1}$ to $\mathbb{N}_{s+1}$' but can just say f. (Note: It doesn't really matter what letter we use!)

Now, somehow f has to tell us how to write down an injection from $\mathbb{N}_k$ to $\mathbb{N}_s$. This f is *abstract information*: you don't know any function values of f, any concrete information, but you know it has this property 'injective'. You have to get used to the idea that you can still work with such a thing even without knowing anything about it. And often the way to do this is to learn more about f.

In this example, you learn more about f by asking yourself whether f in fact immediately gives you an injection from $\mathbb{N}_k$ to $\mathbb{N}_s$ — that happens if $f(1), \ldots, f(k)$ are all in $\mathbb{N}_s$. Well, if that would happen then you know how to write down the injection you wanted. But if it does not happen, there is a reason: the reason has to be that $f(j) = s+1$ for some $1 \leq j \leq k$. And now you learned a piece of (more) concrete information about f; you can try to use the extra information you learned to come up with the injection you want.

Putting this last paragraph into one sentence, the idea is: Maybe I have what I want — and if not, I learn something more about the abstract function that can help me complete the proof.

This kind of understanding is what I want you to get from the proof of PP. For all the longer proofs in these notes, I would like you to get an idea of why the proof works and what ideas you are being shown that you can use elsewhere in your own proofs; this is why these proofs are there.

4.7.3 Some applications of the Pigeonhole Principle

We now prove some theorems using the pigeonhole principle.

We start with an easy example.

Theorem 4.5 In any group of 13 or more people, there are two persons whose birthday is in the same month.

Proof. Consider the function that maps the people to their months of birth. Since $13 > 12$, this cannot be a bijection, so two people are born in the same month. □

This next one is not hard, but perhaps not immediately obvious.

Theorem 4.6 In a room full of people, there will always be at least two people who have the same number of friends in the room.

Proof. Let X be the set of people in the room and suppose $|X| = n \geq 2$. Consider the function $f : X \to \mathbb{N} \cup \{0\}$ where $f(x)$ is the number of friends x has in the room.

Let's assume that a person can't be a friend of themselves. (We could instead assume that a person is always friendly with themselves: we simply need a convention one way or the other.)

Then $f(X) = \{f(x) : x \in X\} \subseteq \{0, 1, \ldots, n-1\}$. But there can't be x, y with $f(x) = n-1$ and $f(y) = 0$. **Why?** Well, such an x would be a friend of all the others, including y, which isn't possible since y has no friends in the room.

So either $f(X) \subseteq \{0, 1, \ldots, n-2\}$ or $f(X) \subseteq \{1, \ldots, n-1\}$. In each case, since $f(x)$ can take at most $n-1$ values, there must, by PP, be at least two $x, y \in X$ with $f(x) = f(y)$. And that's what we needed to prove. □

Here's an interesting geometrical example. For two points (x_1, y_1), (x_2, y_2) in the plane, the **midpoint** of (x_1, y_1) and (x_2, y_2) is the point

$$\left(\tfrac{1}{2}(x_1 + x_2),\ \tfrac{1}{2}(y_1 + y_2)\right)$$

(the point on the middle of the line connecting (x_1, y_1) to (x_2, y_2)).

Theorem 4.7 If we have a set A of five or more points in the plane with **integer** coordinates, then there are two points in A whose midpoint has integer coordinates.

Proof. For two integers a, b, $\frac{1}{2}(a + b)$ is an integer if and only if $a + b$ is even, so if and only if a, b are both even or are both odd.

So the midpoint of $(x_1, y_1), (x_2, y_2)$ has both coordinates integer if and only if x_1, x_2 are **both** even or **both** odd, **and also** y_1, y_2 are **both** even or **both** odd.

Let's label each of the points (a, b) of A with one of "(even,even)", "(even,odd)", "(odd,even)" or "(odd,odd)".

Since $|A| \geq 5$, there will be at least two points which receive the same label. Hence these two points have the same parity (odd or even) for the first coordinate, and the same parity for the second coordinate. This means the midpoint of these two points must be integer as well. □

By the way, this result would not necessarily hold if we only had four points in the set. Consider $(0, 0)$, $(1, 0)$, $(1, 0)$ and $(1, 1)$.

Here's a very interesting number theory application (with a very sneaky proof). It uses the notion of remainders on division by n, which we'll cover properly soon: for now, all we need is that, for every natural number m, the "remainder, r, upon division by n" is one of the numbers $0, 1, \ldots, n-1$, and that $m - r$ is divisible by n.

Theorem 4.8 Let $a_1, a_2, \ldots, a_n$ be n integers (where $n \geq 2$). Then there exists a non-empty collection of these integers whose sum is divisible by n.

Proof. Consider the numbers $s_0, s_1, \ldots, s_n$ given by

$$s_0 = 0,$$

$$s_1 = a_1,$$

$$s_2 = a_1 + a_2,$$

$$s_3 = a_1 + a_2 + a_3,$$

etc., until

$$s_n = a_1 + a_2 + \cdots + a_n.$$

(It is not obvious, at all, why we should do this, but it will work!)

For each of these s_i, consider the remainder upon division by n. Since there are $n+1$ numbers s_i, but only n possible remainders $(0, 1, \ldots, n-1)$, two of the s_i will have the same remainder upon division by n.

So suppose s_k and s_ℓ have the same remainder, where $k < \ell$. Then $s_\ell - s_k$ is divisible by n. But since $s_\ell - s_k = a_{k+1} + a_{k+2} + \cdots + a_\ell$, this means that the sum $a_{k+1} + a_{k+2} + \cdots + a_\ell$ is divisible by n. Se we have proved the result. □

In fact we proved something even stronger than what we set out to prove:
Let $a_1, a_2, \ldots, a_n$ be a list of n integers (where $n \geq 2$). Then there exists a non-empty collection of **consecutive** numbers from this list $a_{k+1}, a_{k+2}, \ldots, a_\ell$ whose sum is divisible by n.

The theorem isn't true if we have fewer than n integers. For instance, if for any $n \geq 2$ we take the numbers $a_1, \ldots, a_{n-1}$ all equal to 1, then it's impossible to find a sum that adds up to something divisible by n.

4.8 A generalised form of PP

We state without proof the following more general version of the PP. Again, it's rather obvious. Isn't it?

Theorem 4.9 Suppose $f : A \to B$ and that $|A| > k|B|$ where $k \in \mathbb{N}$. Then there is some element of B that is the image of at least $k+1$ elements of A.

I should maybe point out why the proof of this is not in the course. First, it is something you can find or generate for yourself fairly easily if you want. More importantly, it won't show you any new ideas; you wouldn't learn anything you didn't already see earlier.

Last year, 241 students were registered for this course. I knew, before marking the exams, that at least three of them would get the same exam mark.

Why? Well, apply the theorem, with A being the students, B being the set $\{0, 1, \ldots, 100\}$ of all possible marks (which is of size 101) and $f(x)$ the mark of student x. Since $232 > 2(101)$, there's some mark y such that at least $2 + 1 = 3$ students will have $y = f(x)$, which means they get the same mark.

4.9 Infinite sets

We say that a set A is *finite* when there is some $n \in \mathbb{N}$ such that $|A| = n$. Otherwise, A is said to be *infinite*.

For example, the set of natural numbers is infinite. You might think that's obvious, but how would you prove it? (Remember that the formal definition that a set A has cardinality n is that there is a bijection between $\mathbb{N}_n$ and A.)

One way to show this is to use a proof by contradiction. Suppose (for a contradiction) that $\mathbb{N}$ is finite, of cardinality $n \in \mathbb{N}$, and that $f : \mathbb{N}_n \to \mathbb{N}$ is a bijection. Consider the number $N = f(1) + f(2) + \cdots + f(n)$. Since each $f(i)$ is a natural number, for all $i \in \mathbb{N}_n$, N is also a natural number. But $N > f(i)$ for all $i \in \mathbb{N}_n$. So here is a natural number, N, that is not equal to $f(i)$ for any $i \in \mathbb{N}_n$. But that contradicts the fact that f is a bijection, because if it's a bijection then it's certainly a surjection and there should be some $i \in \mathbb{N}_n$ with $f(i) = N$.

4.10 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- describe precisely what is meant by a function
- describe precisely what it means to say a function is a surjection, an injection and a bijection, and be able to determine whether a given function has these properties
- state the definition of the composite function $g \circ f$
- establish whether a function has an inverse or not
- demonstrate that you understand the formal definition of the cardinality of a finite set
- state and use the pigeonhole principle
- state what it means to say that a set is infinite; and be able to prove that a set is infinite.

4.11 Sample exercises

Exercise 4.1
Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Prove that if f and g are injections, so is the composition $g \circ f$. Prove also that if f and g are surjections, then so is the composition $g \circ f$.

Exercise 4.2
Let $\mathbb{Z}$ be the set of all integers and suppose that $f : \mathbb{Z} \to \mathbb{Z}$ is given, for $x \in \mathbb{Z}$, by

$$f(x) = \begin{cases} x + 1 & \text{if } x \text{ is even} \\ -x + 3 & \text{if } x \text{ is odd.} \end{cases}$$

Determine whether f is injective. Determine also whether f is surjective.

Exercise 4.3
Suppose that X, Y, Z are sets, and we have functions $f : X \to Y$, $g : Y \to Z$, and $h : Y \to Z$. Suppose that the compositions $h \circ f$ and $g \circ f$ are equal, and also that f is surjective. Prove that $g = h$. □

Exercise 4.4
Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Prove that if the composition $g \circ f$ is injective, then f is injective. Prove that if $g \circ f$ is surjective, then g is surjective. □

Exercise 4.5
Suppose that A and B are non-empty finite sets and that they are disjoint (i.e. $A \cap B = \emptyset$). Prove, using the formal definition of cardinality, that $|A \cup B| = |A| + |B|$. □

Exercise 4.6
Suppose that X, Y are any two finite sets. By using the fact that

$$X \cup Y = (X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y),$$

together with the result of Exercise 4.5, prove that

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Exercise 4.7
Suppose $n \in \mathbb{N}$ and that $f : \mathbb{N}_{2n+1} \to \mathbb{N}_{2n+1}$ is a bijection. Prove that there is some odd integer $k \in \mathbb{N}_{2n+1}$ such that $f(k)$ is also odd. (State clearly any results you use.) □

4.12 Comments on selected activities

Learning activity 4.1 To get started, observe that we can describe the function $h(x)$ defined by $h(x) = 0$ for $x < 0$ and $h(x) = 2x$ for $x \geq 0$ using the formula $h(x) = x + |x|$, where $|x|$ is (as is usual) the *absolute value of* x, i.e. the function $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. (We could also write $|x| = \sqrt{x^2}$). It follows that

$$g(x) = \tfrac{1}{10}\big((x - 11850) + |x - 11850|\big) + \tfrac{1}{10}\big((x - 46350) + |x - 46350|\big).$$

Would that formula be more or less useful to you than the description we gave to define it?

Learning activity 4.2 Given any $y \in \mathbb{R}$, let $x = y/2$. Then $f(x) = 2(y/2) = y$. This shows that f is surjective. Also, for $x, y \in \mathbb{R}$,

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y,$$

which shows that f is injective. Hence f is a bijection.

4.13 Solutions to exercises

Solution to exercise 4.1

Suppose f and g are injective. Then, for $x, y \in X$,

$$\begin{aligned}(g \circ f)(x) = (g \circ f)(y) &\Rightarrow g(f(x)) = g(f(y)) \\ &\Rightarrow f(x) = f(y) \text{ (because } g \text{ is injective)} \\ &\Rightarrow x = y \text{ (because } f \text{ is injective).}\end{aligned}$$

This shows that $g \circ f$ is injective.

Suppose that f and g are surjective. Let $z \in Z$. Then, because g is surjective, there is some $y \in Y$ with $g(y) = z$. Because f is surjective, there is some $x \in X$ with $f(x) = y$. Then

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

so z is the image of some $x \in X$ under the mapping gf. Since z was any element of Z, this shows that $g \circ f$ is surjective. □

Solution to exercise 4.2

Suppose one of x, y is even and the other odd. Without any loss of generality, we may suppose x is even and y odd. ('Without loss of generality' signifies that there is no need to consider also the case in which x is odd and y is even, because the argument we'd use there would just be the same as the one we're about to give, but with x and y interchanged.) So $f(x) = x + 1$ and $f(y) = -y + 3$. But we cannot then have $f(x) = f(y)$ because $x + 1$ must be an odd number and $-y + 3$ an even number. So if $f(x) = f(y)$, then x, y are both odd or both even. If x, y are both even, this means $x + 1 = y + 1$ and hence $x = y$. If they are both odd, this means $-x + 3 = -y + 3$, which means $x = y$. So we see that f is injective.

Is f surjective? Let $z \in \mathbb{Z}$. If z is odd, then $z - 1$ is even and so $f(z - 1) = (z - 1) + 1 = z$. If z is even, then $3 - z$ is odd and so $f(3 - z) = -(3 - z) + 3 = z$. So for $z \in \mathbb{Z}$ there is $x \in \mathbb{Z}$ with $f(x) = z$ and hence f is surjective.

Solution to exercise 4.3

Suppose f is surjective and that $h \circ f = g \circ f$. Let $y \in Y$. We show $g(y) = h(y)$. Since y is any element of Y in this argument, this will establish that $g = h$. Because f is surjective, there is some $x \in X$ with $f(x) = y$. Then, because $h \circ f = g \circ f$, we have $h(f(x)) = g(f(x))$, which means that $h(y) = g(y)$. So we've achieved what we needed.

Solution to exercise 4.4

Suppose $g \circ f$ is injective. To show that f is injective we need to show that $f(x) = f(y) \Rightarrow x = y$. Well,

$$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y))$$

by definition of a function. Now $g(f(x)) = (g \circ f)(x)$, and similarly for y; this is what $\circ$ means. And

$$(g \circ f)(x) = (g \circ f)(y) \Rightarrow x = y,$$

because $g \circ f$ is injective. So we proved

$$f(x) = f(y) \Rightarrow x = y\,,$$

i.e. f is injective.

Now suppose $g \circ f$ is surjective. So for all $z \in Z$ there is some $x \in X$ with $(g \circ f)(x) = z$. So $g(f(x)) = z$. Denoting $f(x)$ by y, we therefore see that there is $y \in Y$ with $g(y) = z$. Since z was any element of Z, this shows that g is surjective. □

Solution to exercise 4.5

Suppose $|A| = m$ and $|B| = n$. We need to show that $|A \cup B| = m + n$ which means, according to the definition of cardinality, that we need to show there is a bijection from $\mathbb{N}_{m+n}$ to $A \cup B$. Because $|A| = m$, there is a bijection $f : \mathbb{N}_m \to A$ and because $|B| = n$, there is a bijection $g : \mathbb{N}_n \to B$. Let us define $h : \mathbb{N}_{m+n} \to A \cup B$ as follows:

$$\text{for } 1 \leq i \leq m,\ h(i) = f(i) \quad \text{and for } m+1 \leq i \leq m+n,\ h(i) = g(i-m).$$

Then h is injective. We can argue this as follows: if $1 \leq i, j \leq m$ then

$$h(i) = h(j) \Rightarrow f(i) = f(j) \Rightarrow i = j,$$

because f is injective. If $m+1 \leq i, j \leq m+n$ then

$$h(i) = h(j) \Rightarrow g(i-m) = g(j-m) \Rightarrow i - m = j - m \Rightarrow i = j,$$

because g is injective. The only other possibility is that one of i, j is between 1 and m and the other between $m+1$ and $m+n$. In this case, the image under h of one of i, j belongs to A and the image of the other to B and these cannot be equal because $A \cap B = \emptyset$. So h is indeed an injection. It is also a surjection. For, given $a \in A$, because f is a surjection, there is $1 \leq i \leq m$ with $f(i) = a$. Then $h(i) = a$ also. If $b \in B$ then there is some $1 \leq j \leq n$ such that $g(j) = b$. But then, this means that $h(m+j) = g((m+j) - m) = b$, so b is the image under h of some element of $\mathbb{N}_{m+n}$. So h is a bijection from $\mathbb{N}_{m+n}$ to $A \cup B$ and hence $|A \cup B| = m + n$.

Solution to exercise 4.6

Note first that the two sets $(X \setminus Y) \cup (Y \setminus X)$ and $X \cap Y$ are disjoint. Therefore,

$$|X \cup Y| = |(X \setminus Y) \cup (Y \setminus X)| + |X \cap Y|.$$

Now, $(X \setminus Y)$ and $(Y \setminus X)$ are disjoint, so

$$|(X \setminus Y) \cup (Y \setminus X)| = |(X \setminus Y)| + |(Y \setminus X)|$$

and therefore

$$|X \cup Y| = |(X \setminus Y)| + |(Y \setminus X)| + |X \cap Y|.$$

Now, the sets $X \setminus Y$ and $X \cap Y$ are disjoint and their union is X, so

$$|X| = |(X \setminus Y) \cup (X \cap Y)| = |X \setminus Y| + |X \cap Y|.$$

A similar argument shows that

$$|Y| = |(Y \setminus X) \cup (X \cap Y)| = |Y \setminus X| + |X \cap Y|.$$

These mean that

$$|X \setminus Y| = |X| - |X \cap Y| \text{ and } |Y \setminus X| = |Y| - |X \cap Y|.$$

So we have

$$\begin{aligned} |X \cup Y| &= |(X \setminus Y)| + |(Y \setminus X)| + |X \cap Y| \\ &= (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| \\ &= |X| + |Y| - |X \cap Y|. \end{aligned}$$

Solution to exercise 4.7

Let E be the set of even integers, and O the set of odd integers, in the range $\{1, 2, \ldots, 2n+1\}$. Then $|E| = n$ and $|O| = n+1$. If f was such that $f(k)$ was even for all $k \in O$, then $f^* : O \to E$ given by $f^*(x) = f(x)$ would be an injection. But, by the pigeonhole principle, since $|O| > |E|$, such an injection cannot exist. Hence there is some odd k such that $f(k)$ is odd. □

Chapter 5
Equivalence relations and the integers

☞ Biggs, N. L. *Discrete Mathematics*. Chapter 7.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapter 22.

5.1 Introduction

In this chapter of the notes we study the important idea of an *equivalence relation*, a concept that is central in abstract mathematics. As an important example, we look at how the integers can be defined from the natural numbers through the use of an equivalence relation. We also study some of the important properties of the integers.

5.2 Equivalence relations

5.2.1 Relations in general

The idea of a *relation* is quite a general one. For example, consider the set of natural numbers $\mathbb{N}$ and let us say that two natural numbers m, n are related, denoted by $m \, R \, n$, if $m + n$ is even. So we have, for instance, $6 \, R \, 2$ and $7 \, R \, 5$, but that 6 and 3 are not related. This relation has some special properties. For one thing, since $2n$ is even for all $n \in \mathbb{N}$, $n \, R \, n$ for all $n \in \mathbb{N}$. (We say such a relation is *reflexive*.) Also, if $m \, R \, n$, then $m + n$ is even. But $m + n = n + m$ and hence, also, $n \, R \, m$. (We say such a relation is *symmetric*.) It is because $m \, R \, n \iff n \, R \, m$ that we can simply say that 'm and n are related' rather than 'm is related to n' or 'n is related to m'. The relation R has other important properties that we will come back to later.

Formally, a relation R on a set X is a subset of the Cartesian product $X \times X$ (which, recall, is the set of all ordered pairs of the form (x, y) where $x, y \in X$). You should just keep in mind that $x \, R \, y$ is a true-or-false statement; if you're not told any more about the relation, there's not much more you can say—maybe for some x and y you are told $x \, R \, y$ is true, but it doesn't tell you whether or not $y \, R \, x$ is true, for example.

> **Example 5.1** Suppose R is the relation on $\mathbb{R}$ given by $x \, R \, y \iff x > y$. Regarded as a subset of $\mathbb{R} \times \mathbb{R}$, this is the set $\{(x, y) \mid x > y\}$. This relation does not possess the reflexive and symmetric properties we met in the example above. For no $x \in \mathbb{R}$ do we have $x \, R \, x$ because x is not greater than x. Furthermore, if $x \, R \, y$ then $x > y$, and we cannot therefore also have $y \, R \, x$, for that would imply the contradictory statement that $y > x$.

In many cases, we use special symbols for relations. For instance '$=$' is a relation, as is $>$. It is often convenient to use a symbol other than R: for instance, many textbooks use $x \sim y$ rather than $x\,R\,y$ as a symbol for 'some relation'.

5.2.2 The special properties of equivalence relations

There are three special properties that a relation might have (two of which we saw in one of the earlier examples):

Definition 5.1 Suppose that R is relation on a set X. Then

- **[The reflexive property]** R is said to be *reflexive* if, for all $x \in X$, $x\,R\,x$.
- **[The symmetric property]** R is said to be *symmetric* if, for all $x, y \in X$, $x\,R\,y$ implies $y\,R\,x$ (equivalently, for all $x, y \in X$, $x\,R\,y \iff y\,R\,x$).
- **[The transitive property]** R is said to be *transitive* if, for all $x, y, z \in X$, whenever $x\,R\,y$ and $y\,R\,z$, we also have $x\,R\,z$; that is, $(x\,R\,y) \wedge (y\,R\,z) \Rightarrow xRz$.

A relation that has all three of these properties is called an *equivalence relation*.

Definition 5.2 A relation is an *equivalence relation* if is reflexive, symmetric and transitive.

Example 5.2 We saw earlier that the relation on $\mathbb{N}$ given by

$$m\,R\,n \iff m + n \text{ is even}$$

is reflexive and symmetric. It is also transitive. To prove that, suppose x, y, z are three natural numbers and that $x\,R\,y$ and $y\,R\,z$. Then $x + y$ is even and $y + z$ is even. To show that $x\,R\,z$ we need to establish that $x + z$ is even. Well,

$$x + z = (x + y) + (y + z) - 2y,$$

and all three terms on the right ($x + y$, $y + z$, and $2y$) are even. Therefore, $x + z$ is even and so $x\,R\,z$.

Example 5.3 Let X be the set of $n \times n$ real matrices. Define a relation $\sim$ on X by:

$$M \sim N \iff \exists r, s \in \mathbb{N} \text{ s.t. } M^r = N^s.$$

Then $\sim$ is an equivalence relation.

Reflexivity and symmetry are easy to see: $M^1 = M^1$ and, if $M^r = N^s$, then $N^s = M^r$. Proving transitivity requires more work. Suppose $M \sim N$ and $N \sim R$. Then there are $r, s, t, u \in \mathbb{N}$ with $M^r = N^s$ and $N^t = R^u$. Then

$$M^{rt} = (M^r)^t = (N^s)^t = (N^t)^s = (R^u)^s = R^{us},$$

so there are integers $w = rt$ and $x = us$ such that $M^w = R^x$ and hence $M \sim R$.

Example 5.4 Let S be a set of people in a given social network, and let F be the relation 'friendship', i.e. aFb if a and b are people in S who are friends in the social network. This relation is symmetric (in real life, it might be that a says they are friends with b but b disagrees. Social networks such as Facebook don't allow this one-sided 'friendship'). Let's say that you are automatically a friend of yourself, so the relation is reflexive.

Is the relation transitive? Well, that depends on the social network. You probably want to say 'No', because (if you're on Facebook) you surely have some friend not all of whose friends you know. So for the example of S and F coming from Facebook, you know the relation F is not transitive; you have a counterexample—and hence it's also not an equivalence relation. But it doesn't have to be that way. If S is all the people in this lecture hall—well, we're all friends (I hope!) and so from the lecture example we do get a transitive relation, and hence (because we checked all three properties) an equivalence relation.

5.3 Equivalence classes

Given an equivalence relation, it is natural to group together objects that are related to each other. The resulting groupings are known as *equivalence classes*. In this section, we formally define equivalence classes and discuss some of their properties.

Definition 5.3 Suppose R is an equivalence relation on a set X and, for $x \in X$, let $[x]_R$ be the set of all $y \in X$ such that $y\,R\,x$. So,

$$[x]_R = \{y \in X \mid y\,R\,x\}.$$

Often, we will want to talk about the set of all equivalence classes of R. This set is written X/R, and referred to as the *quotient set of X by R*. So we have

$$X/R = \left\{[x]_R : x \in X\right\}.$$

Notice that each $[x]_R$ is a *subset* of X. If R is clear from the context—which it usually will be; in general we will only be talking about one equivalence relation at any given time—we may just write $[x]$ for $[x]_R$.

Example 5.5 Consider again R on $\mathbb{N}$ given by $m\,R\,n \iff m+n$ is even. Any even number is related to any other even number; and any odd number to any odd number. So there are two equivalence classes:

$$[1] = [3] = [5] = \cdots = \text{set of odd positive integers},$$

$$[2] = [4] = [6] = \cdots = \text{set of even positive integers},$$

and we have $\mathbb{N}/R = \{[1], [2]\}$.

Example 5.6 Given a function $f : X \to Y$, define a relation R on X by $x\,R\,z \iff f(x) = f(z)$. Then R is an equivalence relation. If f is a surjection, the equivalence classes are the sets

$$\{x \in X : f(x) = y\} = f^{-1}(\{y\}),$$

for $y \in Y$. Note that the place where we use that f is a surjection is that it implies each $f^{-1}(\{y\})$ is non-empty. If f is not a surjection, then the equivalence classes are the sets $f^{-1}(\{y\})$ for all $y \in Y$ such that there is an $x \in X$ with $y = f(x)$, in other words for each $y \in f(X)$.

Activity 5.1 Check this!

The equivalence classes have a number of important properties. These are given in the following result.

Theorem 5.1 Suppose R is an equivalence relation on a set X. Then

(i) For $x, y \in X$, $[x] = [y] \iff x\,R\,y$

(ii) For $x, y \in X$, if x and y are not related by R, then $[x] \cap [y] = \emptyset$.

Proof. (i) This is an if and only if statement, so we have two things to prove: namely that $[x] = [y] \Rightarrow x\,R\,y$ and that $x\,R\,y \Rightarrow [x] = [y]$.

Suppose, then, that $[x] = [y]$. The relation R is reflexive, so we have $x\,R\,x$. This means that $x \in [x]$. But if $[x] = [y]$, then we must have $x \in [y]$. But that means (by definition of $[y]$) that $x\,R\,y$.

Conversely, suppose that $x\,R\,y$. We now want to show that $[x] = [y]$. So let $z \in [x]$. (We will show that $z \in [y]$.) Then $z\,R\,x$. But, because $x\,R\,y$ and R is transitive, it follows that $z\,R\,y$ and hence $z \in [y]$. This shows $[x] \subseteq [y]$. We now need to show that $[y] \subseteq [x]$. Suppose $w \in [y]$. Then $w\,R\,y$ and, since $x\,R\,y$, we also have, since R is symmetric, $y\,R\,x$. So $w\,R\,y$ and $y\,R\,x$. By transitivity of R, $w\,R\,x$ and hence $w \in [x]$. This shows that $[y] \subseteq [x]$. Because $[x] \subseteq [y]$ and $[y] \subseteq [x]$, $[x] = [y]$, as required.

(ii) Suppose x and y are not related. We prove by contradiction that $[x] \cap [y] = \emptyset$. So suppose $[x] \cap [y] \neq \emptyset$. Let z be any member of the intersection $[x] \cap [y]$. (The fact that we're assuming the intersection is non-empty means there is such a z.) Then $z \in [x]$, so $z\,R\,x$ and $z \in [y]$, so $z\,R\,y$. Because R is symmetric, $x\,R\,z$. So: $x\,R\,z$ and $z\,R\,y$ and, therefore, by transitivity, $x\,R\,y$. But this contradicts the fact that x, y are not related by R. So $[x] \cap [y] = \emptyset$. □

Theorem 5.1 shows that either two equivalence classes are equal, or they are *disjoint*. Furthermore, because an equivalence relation is reflexive, any $x \in X$ is in some equivalence class (since it certainly belongs to $[x]$ because $x\,R\,x$). So what we see is that the equivalence classes form a *partition* of X: their union is the whole of X, and no two equivalence classes overlap.

Example 5.7 Consider again the equivalence relation R on $\mathbb{N}$ given by

$$m \, R \, n \iff m + n \text{ is even.}$$

We have seen that there are precisely two equivalence classes: the set of odd positive integers and the set of even positive integers. Note that, as the theory predicted, these form a partition of all of $\mathbb{N}$ (since every natural number is even or odd, but not both).

5.4 Construction of the integers from the natural numbers

This section might seem at first a little tricky. We know what the integers are, so why do we have to *define* or *construct* them, you might well ask. Why not just say that 0 is the solution to the equation $x + 1 = 1$, and then say that for each $n \in \mathbb{N}$ the number $-n$ is the solution to the equation $x + n = 0$? We can just define some new symbols and then do algebra as we're used to, can't we?

There are three ways to answer this question about constructing the integers. One is to point at the same reason why we gave an axiomatic definition of the natural numbers: we want to be clear that everyone is working with the same structure, otherwise we might start disagreeing about what statements are true.

The second, more important, reason is that very often in mathematics we construct a new structure from existing structures, and most of the time the new structure will be one which you did not study in school and you do not know how it behaves: you really need to know how to prove properties of your new structure from the construction. This is your first chance to see how to do that; we will meet it again when we study rational numbers and modular arithmetic, and this idea will show up again and again in your degree programme.

And finally, the third reason is that you are probably fairly convinced that the natural numbers exist, that the axioms we gave won't lead to a contradiction. Is that so obvious for the integers? If you skipped it earlier, now would be a good time to look back at Section 3.10. Someone told you before that the complex numbers $\mathbb{C}$ exist: you can do algebra as you're used to without running into contradictions, but the number system $\mathbb{E}$ we described in Section 3.10 doesn't exist: if you believe it exists then (as we calculated) you also believe $1 = 1 + 1$. Why is there a difference? If you can't answer that, then how do you know that you won't run into a similar contradiction if you try to do algebra as you're used to with the integers $\mathbb{Z}$?

We are going to give a construction which looks complicated at first, but which we can easily prove works. Again, the main motivation for this is that we will give an idea which we can re-use later in your degree course to construct structures which are more complicated and which you don't have intuition for.

The idea behind what follows is this: imagine you have deposits of a and debts of b (which are natural numbers). Denote this by (a, b). Then (informally—we didn't

define 'subtraction' yet!) you have a total of $a - b$, which might be negative.

We can describe, or construct, the integers from the natural numbers, using an equivalence relation. In fact, we consider an equivalence relation on the set $\mathbb{N} \times \mathbb{N}$ of all ordered pairs of natural numbers. Given (a, b) and (c, d) in $X = \mathbb{N} \times \mathbb{N}$, let us say that

$$(a, b)\, R\, (c, d) \iff a + d = b + c.$$

(Informal motivation: we're thinking of $[(a, b)]$ as the (familiar) integer $a - b$. That's why we defined

$$(a, b)\, R\, (c, d) \iff a + d = b + c.$$

This is the 'same' as $a - b = c - d$. **But** we want to make this work, in the set of **natural numbers** and **using addition**, not subtraction, which we haven't defined.)

I've said this is an equivalence relation, but let's check this.

First, R is reflexive because $(a, b)\, R\, (a, b)$ if and only if $a + b = b + a$, which is clearly true (It's ($\mathbb{N}$**2**)).

Next, R is symmetric, for

$$(a, b)\, R\, (c, d) \iff a + d = b + c \iff c + b = d + a \iff (c, d)\, R(a, b).$$

Finally, R is transitive. For suppose that $(a, b)\, R\, (c, d)$ and $(c, d)\, R\, (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Therefore,

$$(a + d) + (c + f) = (b + c) + (d + e).$$

That is (after cancelling c and d from each side),

$$a + f = b + e,$$

which means $(a, b)\, R\, (e, f)$.

OK, so we know R is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. What are the equivalence classes of R? The typical equivalence class $[(a, b)]$ contains all (c, d) for which $a + d = b + c$. For example, $[(2, 1)]$ will be

$$[(2, 1)] = \{(3, 2), (4, 3), (5, 4), \dots\}.$$

Now, for $n \in \mathbb{N}$, let us denote the equivalence class $[(n + 1, 1)]$ by n and let us denote the equivalence class $[(1, n + 1)]$ by $-n$. Also, we denote by 0 the class $[(1, 1)]$.

> **Activity 5.2** Check that all these equivalence classes are distinct. In other words, show that $[(n + 1, 1)]$ is not the same as $[(m + 1, 1)]$ if $m, n \in \mathbb{N}$ are distinct, and also $[(1, n + 1)]$ is not the same as $[(1, m + 1)]$ if $m \neq n$, and $[(n + 1, 1)]$ is not the same as $[(1, 1)]$, and $[(1, n + 1)]$ is not $[(1, 1)]$, and $[(1, n + 1)]$ is not $[(m + 1, 1)]$ for any $m, n \in \mathbb{N}$. (Did I cover all the cases? Check that too!) And finally, check that there is no other equivalence class.

We *define* the integers to be the set $(\mathbb{N} \times \mathbb{N})/R$, in other words (by Activity 5.2) the set

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Let's stop for a moment and (again) try to explain what the point of all this abstract nonsense is. First off, you might be a bit confused: after all, 1 is 1 is a member of $\mathbb{N}$, and now for some reason we are also writing 1 for the equivalence class $[(2,1)]_R$ of this equivalence relation on $\mathbb{N} \times \mathbb{N}$, which we are (by definition) saying is a member of $\mathbb{Z}$. This is naughty—the two things are *not* the same, and we should *not* use the same symbol for both. What we are doing is called an *abuse of notation*, which means we are doing something naughty but we will avoid getting into trouble. How can we do that? Well, (as you will see, once we define addition and so on), the equivalence classes $[(2,1)]$, $[(3,1)]$ and so on (which we are calling 1, 2 and so on) satisfy the axioms for the natural numbers. That means we know there is a dictionary correspondence between $\mathbb{N}$ and these equivalence classes (as we proved); they really behave in exactly the same way.

Second, you might ask: why on earth are we giving this funny and complicated construction for $\mathbb{Z}$? I want to get on with my calculations without worrying about it. This is the right question to ask, and the answer is: give me a moment to prove that all your calculations will work, and then you can forget the construction (or at least not keep thinking about it) and get on with your calculations. That's why we (naughtily) use the same symbol 1 for the element of $\mathbb{N}$ and for the equivalence class $[(2,1)]_R$ in $\mathbb{Z}$: because once we check that this construction does what we want, we are going to forget it and just work with $\mathbb{Z}$ as you're used to—in particular, we want to think of 1 in $\mathbb{N}$ and $[2,1]_R$ in $\mathbb{Z}$ as being basically the same thing. We do *not* want to keep thinking about equivalence classes any more, once we convince ourselves that $\mathbb{Z}$ makes sense.

Let's get back to the construction, and check we can do arithmetic with it. First, let's define an addition operation (between equivalence classes) by

$$[(a,b)] + [(c,d)] = [(a+c, b+d)].$$

So, for example, what does this say about the sum of integers $+3$ and -1. Well, $+3 = [(4,1)]$ and $-1 = [(1,2)]$ and therefore

$$+3 + -1 = [(4,1)] + [(1,2)] = [(5,3)].$$

Now, $(5,3)\ R\ (3,1)$, so $[(5,3)] = [(3,1)]$, which is what we called $+2$. No surprise there, then: $3 + (-1) = 2$ in the usual notation for integer arithmetic. Henceforth, we can simply write $m + (-n)$ as the subtraction $m - n$. In other words, we now *defined* subtraction. We waited this long because subtraction always makes sense in $\mathbb{Z}$; in $\mathbb{N}$ it doesn't: for example $3 - 5$ is not in $\mathbb{N}$.

There is quite a subtle point about this definition of addition of equivalence classes. We know that there are many (infinitely many) pairs (a', b') such that $[(a,b)] = [(a',b')]$. Such an (a',b') is called a *representative* of the equivalence class. (It is always the case, for any equivalence relation, as Theorem 5.1 shows, that $[x]$ and $[x']$ are the same whenever $x'\ R\ x$. So any equivalence class can be represented by potentially many different representatives: any member of the class will do.) So we need to be sure that the definition of addition will give us the same answer if we use different representatives. In other words, suppose that $[(a',b')] = [(a,b)]$ and $[(c',d')] = [(c,d)]$. The definition of addition,

$$[(a,b)] + [(c,d)] = [(a+c, b+d)],$$

will only make sense (or, it will only be 'well-defined') if

$$[(a', b')] + [(c', d')] = [(a, b)] + [(c, d)].$$

Thus, we need to prove that if $[(a', b')] = [(a, b)]$ and $[(c', d')] = [(c, d)]$, then

$$[(a + c, b + d)] = [(a' + c', b' + d')].$$

We can see this easily enough in specific cases. For instance, $[(4, 1)] = [(6, 3)]$ and $[(1, 2)] = [(2, 3)]$. We have

$$[(4, 1)] + [(1, 2)] = [(5, 3)] \quad \text{and } [(6, 3)] + [(2, 3)] = [(8, 6)].$$

Well, $(5, 3)\ R\ (8, 6)$, because $5 + 6 = 3 + 8$, so $[(5, 3)] = [(8, 6)]$. So, in this case, and with these choices of representatives for each equivalence class, we end up with the same class when we apply the addition operation.

5

We can prove, more generally, that the definition works, that it does not depend on the choice of representatives of the classes. Remember, what we need to prove is that if $[(a', b')] = [(a, b)]$ and $[(c', d')] = [(c, d)]$, then

$$[(a + c, b + d)] = [(a' + c', b' + d')].$$

Well, $[(a', b')] = [(a, b)]$ and $[(c', d')] = [(c, d)]$ mean that $(a', b')\ R\ (a, b)$ and $(c', d')\ R\ (c, d)$, so that $a' + b = b' + a$ and $c' + d = d' + c$. We need to show that $[(a + c, b + d)] = [(a' + c', b' + d')]$. This means we need to show that $(a + c, b + d)\ R\ (a' + c', b' + d')$. But

$$\begin{aligned} (a + c, b + d)\ R\ (a' + c', b' + d') &\iff (a + c) + (b' + d') = (b + d) + (a' + c') \\ &\iff (a + b') + (d' + c) = (a' + b) + (c' + d), \end{aligned}$$

which is true, because $a' + b = b' + a$ and $c' + d = d' + c$.

Multiplication, $\times$, is defined on these equivalence classes by

$$[(a, b)] \times [(c, d)] = [(ac + bd, ad + bc)].$$

Again, we should check that this definition 'makes sense', in that whatever representative of the equivalence classes you take, you get the same answer.

Activity 5.3 Check that multiplication as defined above makes sense.

Finally, you should check that this construction 'makes sense' in general, i.e. that addition and multiplication in $(\mathbb{N} \times \mathbb{N})/R$ as we defined them really correspond to what you think addition and multiplication of integers should do. Let's be a little more concrete: we want to check that the following hold.

($\mathbb{Z}1$) Closure under addition and multiplication: for each $a, b \in \mathbb{Z}$ both $a + b$ and ab are in $\mathbb{Z}$.

($\mathbb{Z}2$) Commutative addition and multiplication: for each $a, b \in \mathbb{Z}$ we have $a + b = b + a$ and $ab = ba$.

(ℤ3) Associative addition and multiplication: for each $a, b, c \in \mathbb{Z}$ we have $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.

(ℤ4) The distributive law: for each $a, b, c \in \mathbb{Z}$ we have $(a+b)c = ac+bc$.

(ℤ5) Additive and multiplicative identity: there are two different elements 0 and 1, such that for each $a \in \mathbb{Z}$ we have $a+0 = a$ and $a \times 1 = a$.

(ℤ6) Additive inverses: for each $a \in \mathbb{Z}$ there is an element $-a$ such that $a+(-a) = 0$.

(ℤ7) Multiplicative cancellation: for each $a, b, c \in \mathbb{Z}$, if $c \neq 0$ and $ac = bc$ then $a = b$.

You should *not* try to memorise these properties (I will not ask them in the exam), you should simply check that you agree with the following two statements. First, $\mathbb{Z}$ as we just defined it satisfies all these properties. Second, these are the properties you would normally use to do arithmetic in $\mathbb{Z}$. Unlike the axioms for the natural numbers, these properties do *not* uniquely define the integers—there are other structures which also satisfy them. We could add some more axioms in order to find something which does uniquely define the integers—if you're interested, try to do so. But there isn't really a need—$\mathbb{Z}$ is what you get from $\mathbb{N}$ by adding 0 and, for each $n \in \mathbb{N}$, the number $-n$. That already defines it uniquely (and the funny construction proves that this definition, unlike the number system $\mathbb{E}$, makes sense).

We'll show one of these properties hold, as an example.

Example 5.8 We show that for any integer z we have $z+0 = z$. Recall that, for some (a, b), we will have $z = [(a, b)]$ and that 0 is $[(1, 1)]$. Now, the definition of addition of integers (that is, of the equivalence classes) means that

$$z+0 = [(a, b)] + [(1, 1)] = [(a+1, b+1)].$$

But $(a+1, b+1)\ R\ (a, b)$ because $(a+1)+b = (b+1)+a$, and hence $[(a+1, b+1)] = [(a, b)] = z$. So $z+0 = z$.

Activity 5.4 With integers defined in the formal way as these equivalence classes, prove that for any integer z we have $z \times 0 = 0$.

You probably realise at this point that it is easy to check these properties; writing out all of them would take a lot of space, but it would not be hard. In principle you should check them though! And at this point we are done. These properties we gave are all you will ever need to do arithmetic with $\mathbb{Z}$, and that arithmetic works the way you think it should. At this point, **you can stop thinking about the funny construction, and simply work with the integers $\mathbb{Z}$ as you're used to doing**. (Actually, that's not quite true—we'll use the funny construction in the next section to define an order $<$ on $\mathbb{Z}$.)

What did we gain from doing all this? Well, suppose you do some arithmetic with $\mathbb{Z}$—could it happen that you run into a contradiction, that for example you prove $0 = 1$? Well, maybe—but if you do, then you can rewrite your proof, using this funny construction (meaning you write $[(1, 1)]$ instead of 0, and so on). In that case you end up with a proof that $[(1, 1)] = [(2, 1)]$ (which we saw in Activity 5.2 is a false

statement). What's the difference? Well, the difference is that the second proof doesn't make any use of properties of $\mathbb{Z}$, it only uses the axioms for the natural numbers. To put it another way: let's assume you are happy that $\mathbb{N}$ exists. Then you should now be happy that $\mathbb{Z}$ exists, even if you were a bit unhappy about negative numbers before.

That might seem like a lot of effort to prove something obvious. Again, the point is that we will do this kind of thing over and over again, in order to prove that structures exist where you probably do *not* think it is obvious. We can begin to answer the question about what the difference between $\mathbb{C}$ and $\mathbb{E}$ from Section 3.10 is now. We saw $\mathbb{E}$ doesn't exist. It isn't obvious that $\mathbb{C}$ exists; if you think it is, you're fooling yourself (so you should not have a simple answer to the question of what the difference is).

But we can *prove* the complex numbers exist, by constructing them from the real numbers in a similar way to the construction we just gave of $\mathbb{Z}$ from $\mathbb{N}$. We'll do this in Section 8.5. Again, the point is not to make you think of a complicated construction whenever you want to work with the complex numbers. The point is to convince you that the complex numbers really work—if you could find a problem with the complex numbers, say if you could prove $0 = 1$ by doing some arithmetic with complex numbers, then you can also prove the same thing without using the complex numbers, just working with the real numbers.

5.5 Ordering the integers

For integers $x = [(a, b)]$ and $y = [(c, d)]$, we say $x < y$ if and only if $a + d < b + c$.

We noted in an earlier chapter that any non-empty subset of $\mathbb{N}$ has a least member. But this is not true for subsets of integers.

For a subset S of $\mathbb{Z}$, m is a *lower bound* for S if for all $s \in S$, $m \leq s$; and M is an *upper bound* for S if for all $s \in S$, $s \leq M$. We say that S is *bounded below* if it has a lower bound; and that it is *bounded above* if it has an upper bound. The natural number l is a *least member* of S if $l \in S$ and, for all $s \in S$, $l \leq s$. So a least member will be a lower bound that belongs to S. The natural number g is a *greatest member* of S if $g \in S$ and, for all $s \in S$, $g \geq s$. So a greatest member will be an upper bound that belongs to S.

The following fact is a fundamental property of the integers, known as the *well-ordering principle*. (The well-ordering principle was discussed earlier, when it was presented as an axiom for the natural numbers. This is a generalisation of that principle.)

The Well-ordering Principle: If S is a non-empty set of integers that has a lower bound, then S has a least member.

(The same statement is true with 'lower' replaced by 'upper' and 'least' replaces by 'greatest'.)

Furthermore, if S is bounded below, then there is *precisely one* least member. For, if l, l' are least members then $l, l' \in S$ and so (since for all $s \in S$, $l \leq s$ and $l' \leq s$) we have both $l \leq l'$ and $l' \leq l$, so that $l = l'$.

5.6 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- demonstrate that you know what is meant by a relation
- demonstrate that you know what it means to say a relation is reflexive, symmetric or transitive, or that it is an equivalence relation
- verify whether given relations are reflexive, symmetric or transitive
- demonstrate that you know the definition of equivalence classes and that you know some of their basic properties, in particular that they form a partition of the set on which the relation is defined
- determine the equivalence classes that correspond to an equivalence relation
- demonstrate knowledge of the way in which the integers can be formally constructed from the natural numbers through the use of an equivalence relation
- state the Well-Ordering Principle

5.7 Sample exercises

Exercise 5.1
Define a relation R on $\mathbb{Z}$ by: for $x, y \in \mathbb{Z}$, $x\,R\,y \iff x^2 = y^2$. Prove that R is an equivalence relation, and describe the corresponding equivalence classes.

Exercise 5.2
Define the relation R on the set $\mathbb{N}$ by $x\,R\,y$ if and only if there is some $n \in \mathbb{Z}$ such that $x = 2^n y$. Prove that R is an equivalence relation. □

Exercise 5.3
Let X be the set of $n \times n$ real matrices. Define a relation $\sim$ on X by:

$$M \sim N \iff \exists \text{ an invertible } P \in X \text{ s.t. } N = P^{-1}MP.$$

Prove that $\sim$ is an equivalence relation.

Exercise 5.4
Suppose that $f : X \to Y$ is a surjection. Define the relation R on X by $x\,R\,y \iff f(x) = f(y)$. Prove that R is an equivalence relation. What are the equivalence classes? Let C denote the set of equivalence classes $[x]$ for $x \in X$. Prove that if $[x] = [y]$ then $f(x) = f(y)$. This means that we can define a function $g : C \to Y$ by: $g([x]) = f(x)$. Prove that g is a bijection. □

Exercise 5.5
Prove that the set $\{x \in \mathbb{Z} \mid x \text{ is a multiple of } 4\}$ has no lower bound. □

5.8 Comments on selected activities

Learning activity 5.4 Suppose $z = [(a, b)]$. By definition, we have $0 = [(1, 1)]$. The definition of multiplication is that

$$[(a, b)] \times [(c, d)] = [(ac + bd, ad + bc)].$$

So,

$$z \times 0 = [(a, b)] \times [(1, 1)] = [(a + b, a + b)].$$

Now, $(a + b, a + b)\, R\, (1, 1)$ because $a + b + 1 = 1 + a + b$ and therefore $[(a + b, a + b)] = [(1, 1)] = 0$. So we see that $z \times 0 = 0$.

5.9 Solutions to exercises

Solution to exercise 5.1

R is reflexive because for any x, $x^2 = x^2$. R is symmetric because $x^2 = y^2 \iff y^2 = x^2$. To show R is transitive, suppose $x, y, z \in \mathbb{Z}$ and $x\, R\, y$ and $y\, R\, z$. Then $x^2 = y^2$ and $y^2 = z^2$, so $x^2 = z^2$, which means $x\, R\, z$. Thus R is an equivalence relation. Given any $x \in \mathbb{Z}$, the equivalence class $[x]$ consists precisely of those integers y such that $y^2 = x^2$. So $[x] = \{x, -x\}$.

Solution to exercise 5.2

R is reflexive because for any x, $x = 2^0 x$. R is symmetric because if $x\, R\, y$ then $\exists n \in \mathbb{Z}$ with $x = 2^n y$. This means that $y = 2^{-n} x$ and hence, taking $m = -n$, $\exists m \in \mathbb{Z}$ such that $y = 2^m x$. So $y\, R\, x$. To show R is transitive, suppose $x, y, z \in \mathbb{Z}$ and $x\, R\, y$ and $y\, R\, z$. Then there are $m, n \in \mathbb{Z}$ such that $x = 2^n y$ and $y = 2^m z$, so $x = 2^n y = 2^n (2^m z) = 2^{m+n} z$ which, since $m + n \in \mathbb{Z}$, shows that $x\, R\, z$. Thus R is an equivalence relation.

Solution to exercise 5.3

For any M, $M = I^{-1} M I$ where I is the identity matrix, so $M \sim M$. For matrices $M, N \in X$, if $M \sim N$ then there's an invertible P with $N = P^{-1} M P$ and so $M = P N P^{-1}$, which can be written as $M = (P^{-1})^{-1} M P^{-1}$. So there is an invertible matrix Q (equal to P^{-1}) such that $M = Q^{-1} N Q$ and hence $M \sim N$. This shows the relation is symmetric. Suppose $M \sim N$ and $N \sim R$. Then there are invertible matrices P and Q such that $N = P^{-1} M P$ and $R = Q^{-1} N Q$. We therefore have

$$R = Q^{-1}(P^{-1} M P) Q = (Q^{-1} P^{-1}) M (P Q) = (P Q)^{-1} M (P Q),$$

so there is an invertible matrix $T = PQ$ so that $R = T^{-1} M T$ and hence $M \sim R$, establishing that $\sim$ is transitive. It follows that $\sim$ is an equivalence relation. (We used here the fact that $(PQ)^{-1} = Q^{-1} P^{-1}$. This follows from the fact that $(Q^{-1} P^{-1})(PQ) = Q^{-1}(P^{-1} P) Q = Q^{-1} I Q = Q^{-1} Q = I$.)

Solution to exercise 5.4

$x\, R\, x$ because $f(x) = f(x)$. If $x\, R\, y$ then $f(x) = f(y)$ so $f(y) = f(x)$ and hence $y\, R\, x$. If $x\, R\, y$ and $y\, R\, z$ then $f(x) = f(y)$ and $f(y) = f(z)$, so $f(x) = f(z)$ and $x\, R\, z$. Hence R is an equivalence relation.

For $x \in X$, $[x]$ is the set of all $y \in X$ with $f(y) = f(x)$, so, since f is a surjection, the equivalence classes are exactly the sets C_z for each $z \in Y$, where $C_z = \{x \in X \mid f(x) = z\}$ is the set of elements of X mapped onto z by f.

The fact that $[x] = [y]$ implies $f(x) = f(y)$ follows directly either from this description of equivalence classes, or from the fact that $[x] = [y]$ implies $x\,R\,y$, which implies $f(y) = f(x)$.

Let g be as defined. It is surjective because for each $z \in Y$, there is some $x \in X$ such that $f(x) = z$ (since f is surjective) and hence $g([x]) = f(x) = z$. Also, g is bijective because $g([x]) = g([y])$ implies $f(x) = f(y)$, which means $x\,R\,y$ and hence that $[x] = [y]$. □

Solution to exercise 5.5

We can prove this by contradiction. Suppose that the set $S = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 4\}$ has a lower bound, l. Then, for all $x \in S$, $x \geq l$. Now, one of $l-1, l-2, l-3, l-4$ must be a multiple of 4. So one of these numbers is in S. However, each is less than l, contradicting the fact that l is a lower bound on S.

Chapter 6
Divisibility and prime numbers

☞ Biggs, N. L. *Discrete Mathematics*. Chapter 8.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapters 15–17 and Chapter 23 (except section 23.5)

6.1 Introduction

In this chapter we begin to study elements of number theory. We start with a discussion of divisibility and this leads us to discuss common divisors. Prime numbers are the basic building blocks in the theory of numbers: in particular, each number can be written in essentially only one way as a product of primes.

6.2 Divisibility

For integers x, y we say that x is a *multiple* of y or that y *divides* x, or that x is *divisible* by y if, for some $q \in \mathbb{Z}$, $x = yq$. We use the notation $y \,|\, x$ to signify that y divides x.

If you're being careful, you might remember we defined 'divisible' earlier for natural numbers. This definition *extends* the definition we gave earlier: that is, if x and y happen to be natural numbers, then 'x is divisible by y' is a true statement (by this definition) if and only if it is true by the earlier definition (in Section 2.2.2). So we did *not* change any definition, we are simply explaining what it means for integers which are not in $\mathbb{N}$.

Note that, for every $x \in \mathbb{Z}$, $x \,|\, 0$. But $0 \,|\, x$ only if $x = 0$.

When y does not divide x, we write $y \nmid x$. In this case, as you will know from elementary arithmetic, dividing x by y will leave a remainder.

6.3 Quotients and remainders

The following theorem is very useful. It formalises the fact that one integer may be divided by another, leaving a remainder.

Theorem 6.1 For any positive integers a and b, there are unique non-negative integers q and r such that

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

This can be proved using some standard properties of integers. Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and let

$$Q = \{m \in \mathbb{N}_0 \mid bm \leq a\}.$$

Then Q is non-empty because $0 \in Q$ (since $0b = 0 \leq a$). Also, Q is finite, because if $qb \leq a$, then, given that $b \in \mathbb{N}$, we have $q \leq a$. So Q must have a maximum member. Let's call this q. Let $r = a - bq$. Because $q \in Q$, $bq \leq a$ and hence $r \geq 0$. Now, q is the maximum member of A, so $q + 1 \notin A$, which means that $(q+1)b > a$, so $qb + b > a$ and hence $r = a - bq < b$. So we have established that $a = bq + r$, and that $0 \leq r < b$. To show that q and r are unique, suppose we have $a = bq + r = bq' + r'$ where $0 \leq r, r' < b$. We want to show $q = q'$ and $r = r'$.

Either $q \leq q'$ or $q \geq q'$. Let's suppose that $q \geq q'$ (the argument is similar if $q \leq q'$). Then

$$0 \leq r = a - bq \leq a - bq' = r' < b.$$

So

$$0 \leq (a - bq') - (a - bq) < b,$$

which simplifies to $0 \leq b(q - q') < b$. This implies $0 \leq q - q' < 1$. But $q - q'$ is an integer, and so we must have $q - q' = 0$. So $q = q'$. Then, $r = a - bq = a - bq' = r'$.

The same result holds more generally, without the restriction that $a > 0$, but the proof is simplest when we restrict to the positive case. The general *Division Theorem* is:

Theorem 6.2 (Division Theorem) For any integers a and b with $b > 0$, there are unique integers q and r such that

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

6.4 Representation of integers with respect to a base

Let t be a positive integer. Then any positive integer x can represented uniquely in the form

$$x = x_n t^n + x_{n-1} t^{n-1} + \cdots + x_1 t + x_0$$

for some integer n. The numbers x_i are integers between 0 and $t - 1$ and can be found by repeated division by t: see Biggs, Section 8.3. We write

$$x = (x_n x_{n-1} \ldots x_1 x_0)_t .$$

To justify the 'repeated division by t' procedure, observe that

$$(x_n x_{n-1} \ldots x_1 x_0)_t = x_n t^n + x_{n-1} t^{n-1} + \cdots + x_1 t + x_0$$

is equal to a multiple of t plus x_0, where $0 \leq x_0 \leq r - 1$. By the Division Theorem, since the quotient and remainder are unique, when we divide x by t we necessarily get quotient $x_n t^{n-1} + x_{n-1} t^{n-2} + \cdots + +x_2 t + x_1 = (x_n x_{n-1} \ldots x_2 x_1)_t$ and remainder x_0. By the same logic, dividing $(x_n x_{n-1} \ldots x_2 x_1)_t$ by t we obtain quotient $(x_n x_{n-1} \dot{s} x_3 x_2)_t$ and remainder x_1, and so on.

In practice, actually doing this calculation is painful by hand. It is generally best to use a calculator or computer algebra system such as Maple or MATLAB. The latter

implements a modular division function which will directly return a quotient and remainder. Calculators generally do not have this function, however performing a normal division, subtracting the integer part, and multiplying will return the correct remainder.

Note that (due to imprecision in the calculator) what is returned might be a decimal number which is very close to an integer rather than an actual integer. Thus to divide 2342 by 37, we perform the (usual) division: $2342/37 = 63.297297....$ Subtracting the integer part (which is the quotient, 63) we get 0.297297... and multiplying by 37 we get 10.9999998 from which we can guess the correct remainder is 11. Checking, $63 \times 37 + 11 = 2342$, as we expected.

Example 6.1 The number 60 (written in base 10) can be written in base 3 as $(2020)_3$ because:

$$60 = 2(3^3) + 0(3^2) + 2(3) + 0(1).$$

The representation can be found by repeated division.

$$\begin{aligned} 60 &= 3 \times 20 + \mathbf{0} \\ 20 &= 3 \times 6 + \mathbf{2} \\ 6 &= 3 \times 2 + \mathbf{0} \\ 2 &= 3 \times 0 + \mathbf{2}. \end{aligned}$$

Example 6.2 What's the representation in base 4 of the number $(201)_{10}$?

$$\begin{aligned} 201 &= 4 \times 50 + \mathbf{1} \\ 50 &= 4 \times 12 + \mathbf{2} \\ 12 &= 4 \times 3 + \mathbf{0} \\ 3 &= 4 \times 0 + \mathbf{3}. \end{aligned}$$

So the answer is $(3021)_4$.

Check: $3(4^3) + 2(4) + 1 = 201$.

Finally, if you are converting a number $\left(x_n x_{n-1} \ldots x_1 x_0\right)_t$ from base t to base 10, generally the easiest method is simply to type in to a calculator the formula

$$\left(x_n x_{n-1} \ldots x_1 x_0\right)_t = x_n t^n + x_{n-1} t^{n-1} + \cdots + x_1 t + x_0 \,.$$

This of course works because the calculator will evaluate the number in base 10.

6.5 Greatest common divisor

The greatest common divisor of two integers is defined as follows.

Definition 6.1 (Greatest common divisor) Suppose a, b are two integers, at least one of which is not 0. Then the *greatest common divisor* (gcd) of a and b, denoted by $\gcd(a, b)$, is the unique positive integer d with the following properties:

(i) d divides both a and b (that is, it is a *common divisor* of a and b)

(ii) d is greater than every other common divisor of a and b: that is, if $c \mid a$ and $c \mid b$ then $c \leq d$.

Implicit here is the fact that the gcd is unique. This easily follows from properties (i) and (ii). For, suppose that d and d' are two positive integers satisfying (i) and (ii). Because d' divides a and b and because d satisfies (ii), we have $d' \leq d$. But also, because d divides a and b and because d' satisfies (ii), we have $d \leq d'$. So we must have $d = d'$.

It's not too hard to see that the gcd exists. For any $n \in \mathbb{Z}$, let $D(n) = \{m \in \mathbb{Z} : m \mid n\}$. This is the set of positive divisors of n. Since $1 \mid n$, for every $n \in \mathbb{Z}$ we have $D(n) \neq \emptyset$. Consider now the set $D(a, b) = D(a) \cap D(b)$, which is the set of positive common divisors of a and b. Now, $D(a, b) \neq \emptyset$ since $1 \in D(a, b)$. Suppose $a \neq 0$. (We know that at least one of a, b is nonzero. If $a \neq 0$, a very similar argument will work using b in place of a.)

Take any $m \in D(a, b)$. By definition, we have $a = qm$ for some $q \in \mathbb{Z}$, and it follows that $|a| = |q| \cdot |m|$. Now q cannot be equal to zero, because $a \neq 0$, so because q is a non-negative integer we have $|q| \geq 1$. Since $|m|$ is also a non-negative integer, it follows that $|q| \cdot |m| \geq |m|$, and thus in particular $|a| \geq |m|$. What we just proved is the statement $m \in D(a, b) \Rightarrow m \leq |a|$.

So $D(a, b)$ is bounded above and hence has a (unique) maximal element d. That's the gcd.

Note that some textbooks use (a, b) to denote the gcd, rather than $\gcd(a, b)$. Apart from the fact that this makes for confusion with elements of $\mathbb{N}^2$, these textbooks usually also write $[a, b]$ for the *least common multiple* of a and b (you can guess the definition), and I usually forget quickly which is which—the only advantage of the (a, b) notation is that it saves ink.

> **Example 6.3** $\gcd(12, 20) = 4$ because $4 \mid 12$ and $4 \mid 20$, but there is no common divisor of 12 and 20 that is greater than 4.

> **Activity 6.1** Convince yourself that $\gcd(35, -77) = 7$.

If two numbers a, b have $\gcd(a, b) = 1$, then we say that a and b are *coprime*. In this case, a and b have no common factors other than 1 and -1. For example, 72 and 77 are coprime.

6.6 The Euclidean algorithm

There is a standard method for computing greatest common divisors, known as the *Euclidean algorithm*. The word 'algorithm' simply means a clearly defined method for

solving a certain problem (in this case, for finding the gcd of two integers).

Before presenting this, we state two important properties of greatest common divisors.

- If $a, b \in \mathbb{N}$ and $b \mid a$, then $\gcd(a, b) = b$.
- For non-zero integers a and b, if $a = bq + r$ where q, r are integers, then $\gcd(a, b) = \gcd(b, r)$.

The first fact is clear: for a is, in this case, a common divisor of a and b. And there's no greater positive divisor of a than a itself.

> **Activity 6.2** Prove this second fact by proving that the set of common divisors of a and b is the same as the set of common divisors of b and r (and hence both sets have the same greatest member.)

These observations provide a way to determine gcds. Let's think about a simple example. Suppose we want $\gcd(100, 15)$. (You can see immediately that the answer is 5, but let's try to explain a method that will be useful in rather less easy examples.)

We have $100 = 15 \times 6 + 10$ so, by the second fact above, $\gcd(100, 15) = \gcd(15, 10)$. Next, $15 = 10 \times 1 + 5$, so $\gcd(15, 10) = \gcd(10, 5)$. But $10 = 2 \times 5$, so 5 divides 10 and so, by the first of the two facts above, $\gcd(10, 5) = 5$. It follows, then, that $\gcd(100, 15) = 5$.

The method is known as the *Euclidean Algorithm*. Here's another, more substantial, example.

> **Example 6.4** Let us calculate $\gcd(2247, 581)$. We have
>
> $$\begin{aligned} 2247 &= 581 \times 3 + 504 \\ 581 &= 504 \times 1 + 77 \\ 504 &= 77 \times 6 + 42 \\ 77 &= 42 \times 1 + 35 \\ 42 &= 35 \times 1 + 7 \\ 35 &= 7 \times 5. \end{aligned}$$
>
> It follows that $\gcd(2247, 581) = 7$. The *reason* is that these divisions establish the following equalities:
>
> $$\begin{aligned} \gcd(2247, 581) &= \gcd(581, 504) \\ &= \gcd(504, 77) \\ &= \gcd(77, 42) \\ &= \gcd(42, 35) \\ &= \gcd(35, 7) = 7, \end{aligned}$$
>
> this last equality because $7 \mid 35$.

And finally let's give the algorithm in general. It makes life easier if we assume a and b are positive integers, and that $a > b$. This is OK, because the cases we are ignoring are 'easy'. First, $\gcd(a, b) = \gcd(|a|, |b|)$, so provided we know how to work out gcd for non-negative integers we automatically can deal with any integers. Second, for all natural numbers n we have $\gcd(0, n) = \gcd(n, 0) = \gcd(n, n) = n$ by definition, so if one of a and b is zero, or if they're equal, we know what to do. Finally, if $a < b$ then we can observe that $\gcd(a, b) = \gcd(b, a)$; in other words, if we don't have $a > b$ then we can swap them over and then compute the gcd.

In order to write a nice algorithm, let's write a_1 and a_2 rather than a and b. So we will write an algorithm which takes as input two positive integers a_1 and a_2, which satisfy $a_1 > a_2$, and 'returns' the gcd of a_1 and a_2.

1. Given positive integers $a_1 > a_2$, set $i = 1$ (we'll use i to count loops; this is the first loop).
2. If $a_{i+1} | a_i$ then return $\gcd(a_1, a_2) = a_{i+1}$ and halt.
3. Find integers q_i and a_{i+2} such that $a_i = a_{i+1}q_i + a_{i+2}$ with $1 \leq a_{i+2} < a_{i+1}$.
4. Increase i by one and return to step 2.

Let's first explain these steps, then prove the algorithm works. Step 1 is just setting things up.

Step 2 is where the algorithm should end—in the examples you did, the last line was always that the larger number (a_i) is divisible by the smaller (a_{i+1}), and we saw that in the examples the gcd is the smaller number. Certainly what is true is that if $a_i > a_{i+1} \geq 1$ and $a_{i+1} | a_i$ then $\gcd(a_i, a_{i+1}) = a_{i+1}$, as we observed above. We claim the algorithm, at every loop, preserves two properties. First, we have $a_i > a_{i+1} \geq 1$. Second, we have $\gcd(a_1, a_2) = \gcd(a_i, a_{i+1})$. If you believe these two properties, then it follows that step 2 is doing the right thing.

Step 3 is where all the work happens. We only get here in a given loop if we don't halt at step 1, i.e. if a_{i+1} does not divide a_i. By the division theorem, there are integers q_i and a_{i+2} such that $a_i = a_{i+1}q_i + a_{i+2}$ with $0 \leq a_{i+2} < a_{i+1}$. (If you wanted to find them in practice, you'd check if $a_i - a_{i+1}$ is smaller than a_{i+1}, if not try $a_i - 2a_{i+1}$, then $a_i - 3a_{i+1}$, and so on) Now, if $a_{i+2} = 0$ then we would have $a_i = a_{i+1}q_i$, i.e. $a_{i+1} | a_i$—but then we would have halted (stopped) at step 2; we would not have reached step 3. So we can't have $a_{i+2} = 0$. That means we have $a_{i+1} > a_{i+2} \geq 1$, which is one of the properties we want the algorithm to have for loop $i + 1$. Finally, as we saw above, we have $\gcd(a_i, a_{i+1}) = \gcd(a_{i+1}, a_{i+2})$. Since $\gcd(a_i, a_{i+1}) = \gcd(a_1, a_2)$, that means we have the other property we want for loop $i + 1$.

Finally, step 4 just loops back to step 2 with i increased by one.

At this point, you might ask: what's still to prove? You've shown me this algorithm always does the right thing, so of course it will give me the right answer. What is still to prove is that the algorithm doesn't loop forever without ever halting in step 2. But this is now obvious: if it looped forever, we would have an infinite sequence of decreasing positive integers

$$a_1 > a_2 > a_3 > \dots$$

which is impossible—after at most a_1 loops we have to stop, and the only way to stop is to give the right answer.

If you feel this proof is a bit too informal, try writing it a bit more carefully. The right way to do this is to use induction: prove that for each $i \geq 1$, either we have the properties $a_i > a_{i+1} \geq 1$ and $\gcd(a_1, a_2) = \gcd(a_i, a_{i+1})$, or the algorithm halted before reaching loop i. The base case $i = 1$ is obvious, and what we explained above is the induction step.

6.7 Some consequences of the Euclidean algorithm

A useful consequence of the Euclidean algorithm is that we can use it to express d, the gcd of a and b, as an integer linear combination of a and b, by which we mean the following.

Theorem 6.3 (Bézout's identity) Suppose a and b are integers (at least one of which is not 0) and let $d = \gcd(a, b)$. Then there are $m, n \in \mathbb{Z}$ such that $d = am + bn$.

Before we prove this, I want to explain how we can actually find these m and n (the theorem just promises they exist; it doesn't tell you how to find them). The short version is: we use the Euclidean algorithm to find $d = \gcd(a, b)$. And then we work backwards through the calculation. Let's give an example: $a = 2247$ and $b = 581$ (we just calculated the gcd of these two numbers in the last section). Now we want to find integers m and n such that

$$2247m + 581n = 7.$$

We can use the calculation we had above, by 'working backwards' through the sequence of equations, as follows:

$$\begin{aligned} 7 &= 42 - 35 \\ &= 42 - (77 - 42) = 42 \times 2 - 77 \\ &= (504 - 77 \times 6) \times 2 - 77 = 504 \times 2 - 77 \times 13 \\ &= 504 \times 2 - (581 - 504) \times 13 = 504 \times 15 - 581 \times 13 \\ &= (2247 - 581 \times 3) \times 15 - 581 \times 13 = 2247 \times 15 - 581 \times 58 \\ &= 2247 \times 15 + 581 \times (-58). \end{aligned}$$

So we see that $m = 15$ and $n = -58$ will work. Not an answer you could easily have guessed! Notice how, in each line of this calculation, we use one of the lines from the calculation that arises from the Euclidean algorithm (and we also simplify as we go along). You will get used to this with practice. There are many examples you could make up for yourself in order to help you practice.

Activity 6.3 In the above procedure to find m and n, figure out exactly which part of the Euclidean algorithm calculation is being used at each stage.

Activity 6.4 Choose two particular positive integers a and b. Use the Euclidean algorithm to find $\gcd(a, b)$ and then use your calculation to find integers m and n

> such that $d = ma + nb$. Do this several times with different choices of numbers until you have mastered it.

By this point, you should have some idea why Bézout's identity is true: you have a procedure for finding the numbers m, n such that $\gcd(a, b) = am + bn$. Let's try to formalise this procedure—that means giving an algorithm that finds the numbers. As before, the interesting case is when $a > b \geq 1$; if we can deal with this case, we can deal with any other case. (Check you see why this is true!)

As with the Euclidean algorithm, to write a nice algorithm, which we'll call the Bézout algorithm, let's write a_1 and a_2 rather than a and b. So we want to find integers m, n such that

$$\gcd(a_1, a_2) = a_1 n + a_2 m\,.$$

We do this as follows.

Run the Euclidean algorithm to find $\gcd(a_1, a_2)$. It generates numbers $a_1 > a_2 > a_3 > \cdots > a_s$ (so it stops in the loop number $s-1$ when we find $a_s | a_{s-1}$, i.e. $a_{s-1} = q_{s-1} a_s$) and in addition numbers $q_1, q_2, \ldots, q_{s-2}$. By definition of the Euclidean algorithm, we have $a_1 = a_2 q_1 + a_3$, or equivalently $a_3 = a_1 - q_1 a_2$. Let's write $n_3 = 1$ and $m_3 = -q_1$. Then we have $a_3 = a_1 n_3 + a_2 m_3$. We just wrote a_3 as an integer linear combination of a_1 and a_2.

Again by definition of the Euclidean algorithm, we have $a_2 = a_3 q_2 + a_4$. We can rearrange and substitute in our expression for a_3 to get

$$a_4 = a_2 - (a_1 n_3 + a_2 m_3) q_2 = a_1 n_4 + a_2 m_4 \quad \text{where} \quad n_4 = -n_3 q_2 \text{ and } m_4 = 1 - m_3 q_2\,.$$

and now we have a_4 as a linear combination of a_1 and a_2. Why is it an integer linear combination? Well, we get n_4 and m_4 by adding, subtracting and multiplying integers (not dividing) and so we know that the results must be integers.

We can keep repeating this until we get to $a_{s-1} = a_1 n_{s-1} + a_2 m_{s-1}$ is an integer linear combination, and then finally

$$\gcd(a_1, a_2) = a_s = a_1 n_{s-1} q_{s-1} + a_2 m_{s-1} q_{s-1}$$

where the last part is by definition a linear combination of a_1 and a_2, and it is an integer linear combination because n_{s-1}, m_{s-1} and q_{s-1} are integers. This time we don't have to check anything about infinite loops—we know the Euclidean algorithm doesn't enter an infinite loop, and the Bézout algorithm runs the same number of steps.

This looks rather like hard work and painful algebra—but bear in mind that in real life, you wouldn't actually do these calculations yourself on paper. You'd program a computer to do them, and the point of an algorithm is that it's easy to make a computer run an algorithm: the method is already precisely specified, just as computers like it.

So now how do we prove Theorem 6.3? Well, like this:

Proof. (of Bézout's identity) We already proved the Euclidean algorithm works correctly. We also explained why the Bézout algorithm works correctly—we proved it. But if we have an algorithm which for input a, b provably finds integers n, m such that $\gcd(a, b) = an + bm$, then in particular those integers have to exist. □

This is a *proof by algorithm*: in order to show that something exists, write down an algorithm to find that thing, and prove it works. Some people may say they don't like algorithms and hence they would rather write this proof as an induction proof (which you can also do). I think it's clearer to write it this way.

The fact that there are $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = am + bn$ (that is, that the gcd of two integers is an integer linear combination of them) is very useful. Here's one nice consequence.

We know that, by definition, if $c \mid a$ and $c \mid b$, then $c \leq d = \gcd(a, b)$. But we can say something stronger, namely that $c \mid d$.

Theorem 6.4 Suppose that $a, b \in \mathbb{Z}$ so that a and b are not both zero, and let $d = \gcd(a, b)$. If $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. There are integers m, n such that $d = ma + nb$. Suppose that $c \mid a$ and $c \mid b$. Then $c \mid ma$ and $c \mid nb$, so $c \mid (ma + nb)$. But this says $c \mid d$, as required. □

Here's another consequence:

Theorem 6.5 For $a, b \in \mathbb{Z}$, with a, b not both zero, let $d = \gcd(a, b)$. Then, for $c \in \mathbb{N}$, there are integers m and n such that $c = am + bn$ **if and only if** $d \mid c$.

Proof. Suppose $c = am + bn$. Now, $d = \gcd(a, b)$ satisfies $d \mid a$ and $d \mid b$, so, also, $d \mid (ma + nb)$ and hence $d \mid c$.

Conversely, suppose $d \mid c$, so that for some integer k, $c = kd$. Now, there are $m, n \in \mathbb{Z}$ with $d = ma + nb$. Then,

$$c = kd = k(ma + nb) = (km)a + (kn)b = Ma + Nb,$$

where $M, N \in \mathbb{Z}$. This shows that c can be written as an integer linear combination of a and b, as required. □

We also have:

Theorem 6.6 Suppose that $a, b \in \mathbb{N}$ are coprime (meaning $\gcd(a, b) = 1$). If $a \mid r$ and $b \mid r$, then $ab \mid r$.

This is not generally true if the numbers a, b are not coprime. Think of a counterexample!

Proof. Because $\gcd(a, b) = 1$, there are integers m, n such that $1 = ma + nb$. So

$$r = r \times 1 = r(ma + nb) = mra + nrb.$$

Because $a \mid r$ and $b \mid r$, there are integers k_1, k_2 such that $r = k_1 a$ and $r = k_2 b$. So

$$r = mra + nrb = m(k_2 b)a + n(k_1 a)b = (mk_2 + nk_1)ab,$$

which shows that $ab \mid r$. □

6.8 Prime numbers

A *prime number* (or a *prime*) is a natural number $p \geq 2$ with the property that the only divisors of p are 1 and p. In a precise sense, which we'll see shortly, primes are the building blocks of the natural numbers.

One important property of primes is that if a prime divides a product of numbers, then it must divide at least one of the numbers in the product. This isn't true for non-primes: for example, $4 \mid 12 = 2 \times 6$, but 4 does not divide either 2 or 6.

Theorem 6.7 Suppose that p is a prime number and that $a, b \in \mathbb{N}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. The proof makes use of the useful fact (seen above) that the gcd of any two numbers can be written as an integer linear combination of the numbers (Theorem 6.3). Suppose, then, that p is prime and that $p \mid ab$. If $p \mid a$, then the conclusion of the theorem holds, so suppose $p \nmid a$ (and we will try to prove $p \mid b$) Then p and a have no common positive divisor other than 1. (The only positive divisors of p are 1 and p because it is prime, and p does not divide a, by assumption.) So $\gcd(p, a) = 1$ and therefore there exist integers m and n with $1 = mp + na$.

Remember that we want to write b as an integer multiple of p (because that's what it means to say p divides b). So let's multiply both sides of this equation by b, in order that we write b equal to something—and then try to see why the something is a multiple of p.

We get $b = b(mp + na) = (bm)p + n(ab)$. So again, our job is to find out why $(bm)p + n(ab)$ is a multiple of p. Well, obviously $(bm)p$ is a multiple of p. What about $n(ab)$? We assumed above that $p \mid ab$, which (by definition) means there is some integer s such that $ab = sp$. Substituting this in, we get

$$b = (bm)p + n(ab) = (bm)p + n(sp) = (bm + ns)p\,,$$

and $bm + ns$ is an integer because each of b, m, n, s is integer. So we wrote b as an integer multiple of p. It follows that $p \mid b$, as required. □

This result can easily be extended: if $a_1, a_2, \ldots, a_n \in \mathbb{N}$ and $p \mid a_1 a_2 \ldots a_n$, then, for some i between 1 and n, $p \mid a_i$.

Activity 6.5 Prove this generalisation of Theorem 6.7.

6.9 Prime factorization: the Fundamental Theorem of Arithmetic

6.9.1 The Fundamental Theorem

The *Fundamental Theorem of Arithmetic* is the name given to the following Theorem. (As its name suggests, this is an important theorem!)

Theorem 6.8 (Fundamental Theorem of Arithmetic) Every integer $n \geq 1$ can be expressed as a product of one or more prime numbers. Furthermore, there is essentially only one such way of expressing n: the only way in which two such expressions for n can differ is in the ordering of the prime factors.

You might ask what is going on with $n = 1$: how do I write 1 as a product of primes? Simple: it's a product of no primes at all: $1 = 2^0 \times 3^0 \times 5^0 \times \ldots$. And we generally don't write all the primes raised to the power zero, because $p^0 = 1$ for each prime p; they don't change the product. This might look like a funny piece of formalism (or like nonsense), but the reason for writing it this way is (a) that it is true, and (b) it will make life easier later not to make an exception for 1.

The expression of an integer as a product of primes is known as its prime decomposition. For example, the prime decomposition of 504 is

$$504 = 2 \times 2 \times 2 \times 3 \times 3 \times 7 = 2^3 \cdot 3^2 \cdot 7\,.$$

Note that, in this last expression, the dot, '$\cdot$' denotes multiplication. It's generally easier to read and write mathematics when we use $\cdot$ rather than $\times$ ($\times$ and $+$ can easily get confused when written hurriedly) so this is common practice. The exception is if we are discussing decimals when $\cdot$ can be confused with the decimal point.

The proof of the Fundamental Theorem is not very difficult, given the results we already have about prime numbers. Establishing that each positive integer can be written as a product of primes is easy. Showing that such a decomposition is essentially unique (that is, unique up to the ordering of the factors) is a little trickier, but can be established using Theorem 6.7.

6.9.2 Proof of the Fundamental Theorem

There are two things to prove:

- Any $n \geq 1$ can be written as a product of primes: $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes and $k_1, k_2, \ldots, k_r \in \mathbb{N}$. ('Existence')
- This is essentially unique: if $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} = q_1^{\ell_1} q_2^{\ell_2} \ldots q_s^{\ell_s}$, are two equal such expressions, then $r = s$, $p_i = q_i$ and $k_i = \ell_i$ for all i. ('Uniqueness').

Fundamental Theorem: 'Existence'

Proof. We use (strong) induction. For $n \geq 1$, let $P(n)$ be the statement:

n can be written as a product of primes

Base case: $n = 1$ is a product of no primes, so $P(1)$ is true.

Assume, inductively, that $k \in \mathbb{N}$ and that $P(s)$ is true for all $s \leq k$. (We're using strong induction.) Consider $k + 1$. This could be a prime number, in which case we're done and $P(k + 1)$ is true. Otherwise $k + 1 = ab$ where $1 < a, b < k + 1$. But then $P(a)$ and $P(b)$ are true (by assumption) so each of a, b is a product of primes. So, therefore, is $k + 1$. □

Fundamental Theorem: 'Uniqueness'

The basic idea here is simple, but the notation makes it a bit obscure, so let's explain it before giving the proof. Suppose we have:

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{\ell_1} q_2^{\ell_2} \dots q_s^{\ell_s} \tag{6.1}$$

where $p_1 < p_2 < \dots < p_r$ and $q_1 < q_2 < \dots < q_s$ are prime numbers, and $k_1, \dots, k_r$ and $\ell_1, \dots, \ell_s$ are natural numbers. By insisting on the order of the primes in each product, we've fixed the orders of the prime factors, so we would like to show that these two factorisations are the same, i.e. we have $r = s$, and for each $1 \leq i \leq r$ we have $p_i = q_i$ and $k_i = \ell_i$.

Suppose for a counterexample that this isn't true. Now, obviously the LHS of (6.1) is divisible by p_1, so the RHS is also divisble by p_1. By applying Theorem 6.7, it follows that p_1 has to divide some q_i, and since q_i is prime it follows $p_1 = q_i$. But now dividing both sides by p_1 we get a smaller counterexample. This tells us we should again use strong induction to prove 'Uniqueness'; then we can simply say that by induction no such counterexample exists, and we're done. Let's write this a little more formally now.

Proof. Base case: Suppose we have

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = 1$$

and $r \geq 1$. Since 1 is not a prime number, we have $p_1 > 1$ and so $p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \geq p_1 > 1$, which is a contradiction.

Assume, inductively, that $n \in \mathbb{N}$ and that $P(s)$ is true for all $s \leq n$. (We're using strong induction.) Consider $n+1$. Suppose we have a counterexample:

$$n+1 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{\ell_1} q_2^{\ell_2} \dots q_s^{\ell_s} \tag{6.2}$$

where $p_1 < p_2 < \dots < p_r$ and $q_1 < q_2 < \dots < q_s$ are prime numbers, and $k_1, \dots, k_r$ and $\ell_1, \dots, \ell_s$ are natural numbers.

Now, we have $n+1 = p_1 \cdot \left(p_1^{k_1 - 1} p_2^{k_2} \dots p_r^{k_r}\right)$, so $n+1$ is divisible by p_1. This means that p_1 divides

$$\underbrace{q_1 \cdot q_1 \cdot \dots \cdot q_1}_{\ell_1} \cdot \underbrace{q_2 \cdot q_2 \cdot \dots \cdot q_2}_{\ell_2} \cdot \dots \cdot \underbrace{q_s \cdot q_s \cdot \dots \cdot q_s}_{\ell_s} .$$

By Activity 6.5, it follows that for some i we have $p_1 | q_i$. Now p_1 is a prime, so it is not 1; and q_i is a prime, so by definition $p_1 = q_i$. So we can write

$$\tfrac{n+1}{p_1} = p_1^{k_1 - 1} p_2^{k_2} \dots p_r^{k_r} = q_1^{\ell_1} q_2^{\ell_2} \dots q_i^{\ell_i - 1} \dots q_s^{\ell_s} .$$

Now these two factorisations of $\frac{n+1}{p_1}$ are different, because the two factorisations of $n+1$ we started with are different. Because $p_1 > 1$ we have $(n+1)/p_1 \leq n$, so this is a contradiction to the strong induction hypothesis. □

We can use the Fundamental Theorem of Arithmetic to prove that there are infinitely many primes. You can find an outline of this proof in Chapter 2.

> **Activity 6.6** Look again at the proof, in Chapter 2, that there are infinitely many primes, and understand where the Fundamental Theorem of Arithmetic is used in the proof.

You should also note that we rather often used 'because 1 is not a prime' in this proof—and indeed, if we considered 1 to be a prime then the theorem would be false: $2 = 1 \times 2 = 1^2 \times 2 = 1^3 \times 2$ would be different factorisations of 2.

6.9.3 Non-examinable: why the Fundamental Theorem of Arithmetic isn't obvious

You quite possibly feel we did something over-complicated to prove the Fundamental Theorem of Arithmetic. The Existence part is clear enough—what we did is the same as the following routine: to factorise n, try dividing by 2, if you can then try dividing $n/2$ by 2, and so on until you can't, then move on to 3, then 5, and so on until you find all the factors (you don't have to keep going forever; at worst n is prime and you will try dividing by all the primes up to n). And surely this is the only way to do it—isn't it obvious? So 'Uniqueness' should be easy, really.

Well, 'Uniqueness' depends on Theorem 6.7 (which is actually not so easy to prove—look back at the proof and the theorems it depends on!); the rest of the proof is really just handling notation. And Theorem 6.7 really looks obvious! But it's not quite as obvious as it looks. Suppose we look at numbers of the form

$$a + b\sqrt{-5}$$

where a and b are integers. These numbers, written $\mathbb{Z}[\sqrt{-5}]$, behave in many ways like the usual integers; if you add or multiply them you still get a number in $\mathbb{Z}[\sqrt{-5}]$, and so on. You can write sensible definitions of 'divisible', 'prime' and so on for $\mathbb{Z}[\sqrt{-5}]$ easily enough, more or less by copying the definitions for $\mathbb{Z}$. But we have

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})\,.$$

Now $1 + \sqrt{-5}$ is not divisible by 2, because $\frac{1+\sqrt{-5}}{2}$ is not in $\mathbb{Z}[\sqrt{-5}]$. And similarly $1 - \sqrt{-5}$ is not divisible by 2. So Theorem 6.7 isn't true in $\mathbb{Z}[\sqrt{-5}]$; and nor is it true that we have unique factorisation (we just gave a counterexample).

What that means is that to prove Theorem 6.7 you certainly need to use *some* property which is true in $\mathbb{Z}$ and not in $\mathbb{Z}[\sqrt{-5}]$. We can do algebra as you're used to in either structure, so it can't be that—what is it?

> **Activity 6.7** What's the difference between $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-5}]$ that makes Theorem 6.7 work?

This actually connects to a rather well-known part of mathematics. You maybe know that Pierre de Fermat claimed in 1637 to have a proof that if $n \geq 3$ is an integer, then $x^n + y^n = z^n$ does not have any solutions where $x, y, z \in \mathbb{N}$. But the proof, if he had one, was lost.

Now, Fermat wasn't just bluffing: he did have a proof for the case $n = 4$ (it was discovered in his papers after his death). It seems unlikely that he really had a proof in general—he certainly did not have the proof which Wiles famously announced in 1994. Perhaps he believed that he had a proof, but there was a mistake?

There was a proof announced (by Lamé) which Fermat might have also found (perhaps!)—but that proof is wrong. The way it is wrong is that it assumes that some numbers which look like the integers (in more or less the same way as $\mathbb{Z}[\sqrt{-5}]$) have unique factorisation. This is an obvious mistake for you now after seeing a counterexample—but it wasn't so obvious when Lamé was working in the 1800s, let alone to Fermat.

6.10 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- state clearly what it means to say that one number divides another
- state the Division Theorem and, given two numbers, find the remainder and quotient when one is divided by the other
- understand what is meant by the representation of an integer with respect to a particular basis and be able to work with this definition
- state the definition of the greatest common divisor of two numbers
- use the Euclidean algorithm to find the gcd of two numbers
- demonstrate that you know that the gcd of two numbers can always be expressed as an integer linear combination of the two numbers; and be able to express the gcd in this way for any two numbers.
- use the Euclidean algorithm to express the gcd of two numbers as an integer linear combination of them
- state what is meant by a prime number
- state the Fundamental Theorem of Arithmetic.

6.11 Sample exercises

Exercise 6.1
Find $d = \gcd(2406, 654)$. Express d in the form $d = 2406m + 654n$ for integers m, n. □

Exercise 6.2
Suppose that $a, b \in \mathbb{N}$, both non-zero, and let $d = \gcd(a, b)$. We know that, by definition, if $c \mid a$ and $c \mid b$, then $c \leq d$. Prove, in fact, that $c \mid d$. □

Exercise 6.3
Suppose $a, b \in \mathbb{N}$ and that $d = \gcd(a, b)$. Prove that, for $c \in \mathbb{N}$, there are integers m and n such that $c = am + bn$ *if and only if* $d \mid c$.

Exercise 6.4
Suppose $a, b \in \mathbb{N}$. Prove that if there are integers m and n such that $am + bn = 1$ then a and b are coprime. □

Exercise 6.5
Prove that for all $n \in \mathbb{N}$, the numbers $9n + 8$ and $6n + 5$ are coprime.

Exercise 6.6
Suppose that $a, b \in \mathbb{N}$ and that $\gcd(a, b) = 1$. Suppose that $a \mid r$ and $b \mid r$. Prove that $ab \mid r$.

Exercise 6.7
The Fibonacci numbers $f_1, f_2, f_3, \ldots$ are defined as follows: $f_1 = f_2 = 1$ and, for $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Prove that for all $n \in \mathbb{N}$, $\gcd(f_n, f_{n+1}) = 1$. □

Exercise 6.8
Suppose that $p_1, p_2, \ldots, p_k$ are primes and that $a, b \in \mathbb{N}$ are given by

$$a = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}, \quad b = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}.$$

Prove that

$$\gcd(a, b) = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k},$$

where, for $i = 1$ to k, r_i is the smaller of the two numbers l_i and m_i. □

Exercise 6.9
Suppose $a, b \in \mathbb{N}$ satisfy $\gcd(a, b) = 1$ and, for some $k \in \mathbb{N}$, $ab = k^2$. Prove that for some integers m, n, $a = m^2$ and $b = n^2$.

6.12 Comments on selected activities

Learning activity 6.1 Certainly, 7 divides both 35 and -77, but there is no larger common divisor. (For, the only larger divisor of 35 is 35 itself, and this does not divide -77.)

Learning activity 6.2 We prove that $D(a, b) = D(b, r)$. The result on gcds will follow since $\gcd(x, y)$ is the maximal element of $D(x, y)$.

Suppose $m \in D(a, b)$. Then $m \mid a$ and $m \mid b$. It follows that $m \mid (a - bq)$; that is, $m \mid r$. So $m \mid b$ and $m \mid r$ and hence $m \in D(b, r)$. Therefore $D(a, b) \subseteq D(b, r)$.

Suppose $m \in D(b, r)$. Then $m \mid b$ and $m \mid r$. It follows that $m \mid (bq + r)$; that is, $m \mid a$. So $m \mid b$ and $m \mid a$ and hence $m \in D(a, b)$. Therefore $D(b, r) \subseteq D(a, b)$.

Learning activity 6.5 To prove this, we can (unsurprisingly) use induction on n. Let $P(n)$ be the statement:

If $a_1, a_2, \ldots, a_n \in \mathbb{N}$ and $p \mid a_1 a_2 \ldots a_n$, then, for some i between 1 and n, $p \mid a_i$.

Then $P(1)$ is clearly true (and $P(2)$ is the theorem just proved). Suppose $P(n)$ is true and let's show $P(n+1)$ follows. So, suppose $a_1, a_2, \ldots, a_{n+1} \in \mathbb{N}$ and $p \,|\, a_1 a_2 \ldots a_n a_{n+1}$. Well, since $p \,|\, A a_{n+1}$, where $A = a_1 a_2 \ldots a_n$, we can apply the $n = 2$ case to see that $p \,|\, A$ or $p \,|\, a_{n+1}$. But, by $P(n)$, if $p \,|\, A = a_1 a_2 \ldots a_n$ then $p \,|\, a_i$ for some i between 1 and n. So we're done: p divides at least one of the a_i for i between 1 and $n+1$.

Learning activity 6.6 Here's the proof, with explicit reference to the Fundamental Theorem.

Suppose there were *not* infinitely many primes, so there's a largest prime, M, say. Let

$$X = (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times M) + 1.$$

Since $X > M$, X is not a prime. By the Fundamental Theorem of Arithmetic, X has a prime divisor p which satisfies $1 < p < X$. This p must be one of the numbers $2, 3, 5, \ldots, M$ (since these are the only primes). However, X is **not** divisible by any of these numbers. So we have a contradiction. We conclude there are infinitely many primes.

Learning activity 6.7 The answer is that in $\mathbb{Z}$ there is an order $<$ such that any two elements are either the same, or one is bigger than the other, and this order 'plays nicely' with addition and multiplication. There is no such order in $\mathbb{Z}[\sqrt{-5}]$. This means that we can define gcd for two numbers in $\mathbb{Z}$; we can't do so (or at least we don't get a nice result) for two numbers in $\mathbb{Z}[\sqrt{-5}]$. It's a bit more subtle than it looks!

6.13 Solutions to exercises

Solution to exercise 6.1

See Biggs, Section 8.4. The gcd is 6 and we have $6 = 28 \times 2406 + (-103) \times 654$.

Solution to exercise 6.2

We know that there are integers m, n such that $d = ma + nb$. Suppose that $c \,|\, a$ and $c \,|\, b$. Then $c \,|\, ma$ and $c \,|\, nb$, so $c \,|\, (ma + nb)$. But this says $c \,|\, d$, as required. □

Solution to exercise 6.3

Suppose first that $c = am + bn$ for some some integers m and n. Now, $d = \gcd(a, b)$ satisfies $d \,|\, a$ and $d \,|\, b$, so we also have $d \,|\, (ma + nb)$ and hence $d \,|\, c$. Conversely, suppose $d \,|\, c$, so that for some integer k, $c = kd$. Now, the gcd $d = \gcd(a, b)$ can be written as an integer linear combination of a and b, so there are $m, n \in \mathbb{Z}$ with $d = ma + nb$. Then,

$$c = kd = k(ma + nb) = (km)a + (kn)b = Ma + Nb,$$

where $M, N \in \mathbb{Z}$. This shows that c can be written as an integer linear combination of a and b, as required. □

Solution to exercise 6.4

This follows from the previous exercise, but we can prove it directly. Suppose that $d \in \mathbb{N}$, that $d \,|\, a$ and $d \,|\, b$. Then $d \,|\, (am + bn)$, which means $d \,|\, 1$. Therefore, we must have $d = 1$. That is, the only positive common divisor of a and b is 1 and hence $\gcd(a, b) = 1$ and the numbers are coprime.

Solution to exercise 6.5

We have $2(9n+8)-3(6n+5)=1$. So, if $d=\gcd(9n+8,6n+5)$, then $d\,|\,(9n+8)$ and $d\,|\,(6n+5)$, so $d\,|\,2(9n+8)-3(6n+5)$. But this says $d\,|\,1$ and hence $d=1$. □

Solution to exercise 6.6

Before we begin, let's just note that this property does not hold if a and b are not coprime. For example, $6\,|\,12$ and $4\,|\,12$ but $24\not|\,12$. Suppose then that $a\,|\,r$ and $b\,|\,r$. The fact that $\gcd(a,b)=1$ means that there are integers m,n such that $1=ma+nb$. So

$$r=r\times 1=r(ma+nb)=mra+nrb.$$

Now, because $a\,|\,r$ and $b\,|\,r$ there are integers k_1,k_2 such that $r=k_1a$ and $r=k_2b$. So

$$r=mra+nrb=m(k_2b)a+n(k_1a)b=(mk_2+nk_1)ab,$$

which shows that r is an integer multiple of ab and hence $ab\,|\,r$.

Solution to exercise 6.7

We prove this by induction on n. Let $P(n)$ be the statement that $\gcd(f_n,f_{n+1})=1$. When $n=1$, this is true, because $\gcd(f_1,f_2)=\gcd(1,1)=1$. It is true also when $n=2$ because $f_3=2$ and hence $\gcd(f_2,f_3)=\gcd(1,2)=1$. Suppose, inductively, that $k\geq 2$ and $\gcd(f_k,f_{k+1})=1$. We want to show that $\gcd(f_{k+1},f_{k+2})=1$. Now, $f_{k+2}=f_{k+1}+f_k$. Therefore, if $d\,|\,f_{k+1}$ and $d\,|\,f_{k+2}$ then $d\,|\,f_{k+1}$ and $d\,|\,(f_{k+2}-f_{k+1})=f_k$. So any common divisor of f_{k+1} and f_{k+2} is also a common divisor or f_k and f_{k+1}. Also, if $d\,|\,f_k$ and $d\,|\,f_{k+1}$ then we also have $d\,|\,f_{k+1}$ and $d\,|\,(f_k+f_{k+1})=f_{k+2}$, so any common divisor of f_k and f_{k+1} is also a common divisor or f_{k+1} and f_{k+2}. This all shows that the common divisors of the pair $\{f_{k+1},f_{k+2}\}$ are precisely the same as the common divisors of the pair $\{f_{k+1},f_k\}$. Therefore, the greatest common divisors of each pair are equal. That is,

$$\gcd(f_{k+1},f_{k+2})=\gcd(f_{k+1},f_k)=\gcd(f_k,f_{k+1})=1,$$

where we have used the inductive hypothesis for the last equality.

You can also establish this result by thinking about the way in which the Euclidean algorithm would work in finding the gcd of f_k and f_{k+1}. □

Solution to exercise 6.8

Let $d=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$. Then because r_i is the smaller of l_i and m_i, we have $r_i\leq l_i$ and $r_i\leq m_i$. So $p^{r_i}\,|\,p^{l_i}$ and $p^{r_i}\,|\,p^{m_i}$, for each i. Therefore $d\,|\,a$ and $d\,|\,b$. Explicitly, for example,

$$\begin{aligned}a &= p_1^{l_1}p_2^{l_2}\dots p_k^{l_k}\\ &= p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}\times p_1^{l_1-r_1}p_2^{l_2-r_2}\dots p_k^{l_k-r_k}\\ &= d(p_1^{l_1-r_1}p_2^{l_2-r_2}\dots p_k^{l_k-r_k}),\end{aligned}$$

and because l_k-r_k is a non-negative integer for each i, the number in parentheses is an integer. This shows $d\,|\,a$. The fact that $d\,|\,b$ can be similarly shown. So d is a common divisor of a and b.

Suppose D is any common divisor of a and b. Then, by the Fundamental Theorem of Arithmetic, D can be written as a product of primes. Let p be any one of these. Then $p\,|\,a$ and $p\,|\,b$. Now, we know that if $p\,|\,a_1a_2\dots a_n$ then $p\,|\,a_i$ for some i. (This follows from the

results of Section 6.8.) The only primes appearing in the decomposition of a and b are $p_1, p_2, \ldots, p_k$, so we can deduce that for some i, $p \,|\, p_i$ which means $p = p_i$ (given that p and p_i are primes). So the prime decomposition of D is of the form

$$D = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$$

for some non-negative integers s_i. Now, suppose that, for some i, $s_i > l_i$. Then, for some integers M and N,

$$D = p_i^{s_i} M, \;\; a = p_i^{l_i} N,$$

where, because they involve only products of the other primes, neither N or M is divisible by p_i. Now, the fact that $D \,|\, a$ means that there's an integer L with $a = LD$, so

$$p_i^{l_i} N = L p_i^{s_i} M$$

and hence

$$N = L p_i^{s_i - l_i} M.$$

But this shows, since $s_i - l_i \geq 1$ (because $s_i, l_i \in \mathbb{Z}$ and $s_I > l_i$), that $p_i \,|\, N$, contradicting the observation that $p_i \not| N$. So we must have $s_i \leq l_i$ for all i. A similar argument shows that $s_i \leq m_i$ for all i. So $s_i \leq r_i = \min(l_i, m_i)$ and hence $D \leq d$. The result follows. □

Solution to exercise 6.9

We use the Fundamental Theorem of Arithmetic. Let k have prime decomposition $k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Then

$$ab = k^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_r^{2\alpha_r}.$$

It follows that a and b must have prime decompositions involving only the primes $p_1, p_2, \ldots, p_r$, and that each of a, b takes the form $p_1^{s_1} p_2^{s_2} \ldots p_r^{s_r}$ where s_i is a non-negative integer. But we cannot have, for any i, $p_i \,|\, a$ and also $p_i \,|\, b$, for this would mean that $p_i > 1$ is a common divisor of a, b, contradicting $\gcd(a, b) = 1$. So, for each i, $p_i^{2\alpha_i}$ divides precisely one of a and b and p_i does not divide the other of the two numbers. In other words, each of a, b takes the form $p_1^{2\beta_1} p_2^{2\beta_2} \ldots p_r^{2\beta_r}$ where $\beta_i = 0$ or $\beta_i = \alpha_i$. This can be written as $(p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r})^2$, and hence there are integers m, n such that $a = m^2$ and $b = n^2$.

Chapter 7
Congruence and modular arithmetic

☞ Biggs, N. L. *Discrete Mathematics*. Chapter 13, Sections 13.1–13.3.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapters 19–21.

7.1 Introduction

In this chapter, we study *congruence* and we describe *modular arithmetic*. This builds on the ideas and results on divisibility and equivalence relations that we met in earlier chapters.

You go to sleep at 10 o'clock and you sleep for 8 hours. At what time do you wake. Well, this is simple: you wake at 6 o'clock. What you're doing in this calculation is you're doing what's called *arithmetic modulo* 12. The answer is not $10 + 8 = 18$, because the clock re-starts once the hour of 12 is reached. This is a fairly simple idea, when expressed in these terms, and it's the key concept behind *modular arithmetic*, a topic later in this chapter. We are going to take a more abstract approach.

7.2 Congruence modulo m

7.2.1 The congruence relation

Suppose that m is a fixed natural number, and let's define a relation R on the integers by $a\,R\,b$ if and only if $b - a$ is a multiple of m. That is, $a\,R\,b \iff m \mid (b - a)$. Then R is an equivalence relation.

Activity 7.1 Prove that R is an equivalence relation on $\mathbb{Z}$.

This relation is so important that it has a special notation. If $a\,R\,b$, we say that a and b are *congruent modulo* m and we write $a \equiv b \pmod{m}$.

If a and b are not congruent modulo m, then we write $a \not\equiv b \pmod{m}$.

The division theorem tells us that for any integers a and for any $m \in \mathbb{N}$, there are unique integers q and r such that

$$a = qm + r \quad \text{and} \quad 0 \leq r < m.$$

What this implies for congruence is that, for any a, there is precisely one integer r in the range $0, 1, \ldots, m - 1$ such that $a \equiv r \pmod{m}$.

Congruence relations can be manipulated in many ways like equations, as the following Theorem shows.

Theorem 7.1 Suppose that $m \in \mathbb{N}$ and that $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

(i) $a + c \equiv b + d \pmod{m}$

(ii) $a - c \equiv b - d \pmod{m}$

(iii) $ac \equiv bd \pmod{m}$

(iv) $\forall k \in \mathbb{Z},\ ka \equiv kb \pmod{m}$

(v) $\forall n \in \mathbb{N},\ a^n \equiv b^n \pmod{m}$

Proof. I leave (i) and (ii) for you to prove. Here's how to prove (iii): because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we have $m \,|\, (b - a)$ and $m \,|\, (d - c)$. So, for some integers k, l, $b - a = km$ and $d - c = lm$. That is, $b = a + km$ and $d = c + lm$. So

$$bd = (a + km)(c + lm) = ac + (kmc + alm + klm^2) = ac + m(kc + al + klm).$$

Now, $kc + al + klm \in \mathbb{Z}$, so $bd - ac = (kc + al + klm)m$ is a multiple of m; that is, $m \,|\, (bd - ac)$ and $ac \equiv bd \pmod{m}$. Part (iv) follows from (iii) by noting that $k \equiv k \pmod{m}$, and part (v) follows by repeated application of (iii) (or, by (iii) and induction.). □

Activity 7.2 Prove parts (i) and (ii) of Theorem 7.1.

Theorem 7.1 is useful, and it enables us to solve a number of problems. Here are two examples.

Example 7.1 Suppose that the natural number x has digits $x_n x_{n-1} \ldots x_0$ (when written, normally, in 'base 10'). So, for example, if $x = 1246$ then $x_0 = 6, x_1 = 4, x_2 = 2, x_3 = 1$. Then 9 divides x if and only if $x_0 + x_1 + \cdots + x_n$ is a multiple of 9. (So this provides a quick and easy way to check divisibility by 9. For example, 127224 is divisible by 9 because $1 + 2 + 7 + 2 + 2 + 4 = 18$ is.)

How do we prove that this test works? We can use congruence modulo 9. Note that

$$x = x_0 + (10)x_1 + (10)^2 x_2 + \cdots + (10)^n x_n.$$

Now, $10 \equiv 1 \pmod{9}$, so, for each $k \in \mathbb{N}$, $10^n \equiv 1 \pmod{9}$. Hence

$$x = x_0 + (10)x_1 + (10)^2 x_2 + \cdots + (10)^n x_n \equiv x_0 + x_1 + \cdots + x_n \pmod{9}.$$

A number is divisible by 9 if and only if it is congruent to 0 modulo 9, so

$$\begin{aligned} 9 \,|\, x &\iff x \equiv 0 \pmod{9} \\ &\iff x_0 + x_1 + \cdots + x_n \equiv 0 \pmod{9} \\ &\iff 9 \,|\, (x_0 + x_1 + \cdots + x_n). \end{aligned}$$

This is precisely what the test says.

Example 7.2 We can use congruence to show that there are no integers x and y satisfying the equation $7x^2 - 15y^2 = 1$.

We prove this by contradiction. So suppose such x and y did exist. Then, because $15y^2$ is a multiple of 5, we'd have $7x^2 \equiv 1 \pmod 5$. Now, x is congruent to one of the numbers $0, 1, 2, 3, 4$ modulo 5. That is, we have:

$$x \equiv 0 \text{ or } x \equiv 1 \text{ or } x \equiv 2 \text{ or } x \equiv 3 \text{ or } x \equiv 4 \pmod 5.$$

So,

$$x^2 \equiv 0 \text{ or } x^2 \equiv 1 \text{ or } x^2 \equiv 4 \text{ or } x^2 \equiv 9 \text{ or } x^2 \equiv 16 \pmod 5.$$

But $9 \equiv 4 \pmod 5$ and $16 \equiv 1 \pmod 5$, so, in every case, either $x^2 \equiv 0$ or $x^2 \equiv 1$ or $x^2 \equiv 4 \pmod 5$. It follows, then, that in all cases, we have

$$7x^2 \equiv 0 \text{ or } 7x^2 \equiv 7 \equiv 2 \text{ or } 7x^2 \equiv 28 \equiv 3 \pmod 5.$$

So there does not exist an integer x with $7x^2 \equiv 1 \pmod 5$, and hence there are no integer solutions to the original equation.

7.2.2 Congruence classes

What are the equivalence classes of the congruence relation, modulo a particular positive integer m? These are often called the *congruence classes modulo* m. Let's denote these by $[x]_m$. For a particular $x \in \mathbb{Z}$, $[x]_m$ will be all the integers y such that $y \equiv x \pmod m$. We know that each x is congruent to precisely one of the integers in the range $0, 1, 2, \ldots, m-1$, and we know (from the general theory of equivalence relations) that if $x \equiv y \pmod m$ then $[x]_m = [y]_m$. So it follows that for each $x \in \mathbb{Z}$, we'll have

$$[x]_m = [0]_m, \text{ or } [x]_m = [1]_m, \ldots \text{ or } [x]_m = [m-1]_m.$$

So there are precisely m equivalence classes,

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

The theory of equivalence relations tells us that these form a partition of $\mathbb{Z}$: they are disjoint and every integer belongs to one of them. But what are they? Well, $[0]_m$ is the set of all x such that $x \equiv 0 \pmod m$, which means $m \mid x$. So $[0]_m$ is the set of all integers divisible by m. Generally, for $0 \leq r \leq m-1$, $[r]_m$ will be the set of x such that $x \equiv r \pmod m$. It follows that $[r]_m$ is the set of all integers x which have remainder r on division by m.

Example 7.3 Suppose $m = 4$. Then the congruence classes are:

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$

$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$

$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

7.2.3 What did we just learn?

What we've just done is present modular arithmetic in a familiar way: you can do addition, subtraction and multiplication (but not division!) modulo m as you would do then in the integers. The only change is that you're allowed to add or subtract multiples of m from the answer any time you like and say this doesn't change anything (you still have the same answer modulo m).

This is useful if for some reason you think adding or subtracting a multiple of m is not important. For example if you are calculating angles, 360° is the same thing as 0°, so you can do calculations modulo 360, which means you don't have to work with large numbers. Another, maybe better, example: is it obvious whether $7^{100} - 1$ is divisible by 8? Well, of course you can plug this into a calculator — which will refuse to answer because 7^{100} doesn't fit on the display. Or you can calculate modulo 8: '$7^{100} - 1$ is divisible by 8' is by definition the same as '$7^{100} - 1$ is congruent to 0 modulo 8'. We have

$$7^{100} - 1 \equiv (-1)^{100} - 1 \equiv 1 - 1 \equiv 0 (\text{mod } 8)\,,$$

so indeed $7^{100} - 1$ is divisible by 8 — that really simplified the calculation!

What I want to stress is that you do know how to do calculations modulo m — if you want, you can simply do the calculations in the integers, then at the end add or subtract multiples of m, but you can also do this at any step along the way and doing so may well make your life easier.

What we are now going to do is go through this in a more abstract way. We are going to define some new 'algebraic structures', which you never saw before and do not have much intuition for. You most likely will feel uncomfortable working with them. But bear in mind that all we are doing is modular arithmetic, written a bit differently — if you're not sure whether you got the abstract approach right, try writing it all out in the way we did modular arithmetic above and check it works.

There are two reasons we do this. First, once you do get used to the abstract approach below, it's quicker to write and maybe a bit easier to avoid mistakes — and as we'll see in the examples sessions, modular arithmetic is actually hugely important in modern society!

Second, you will encounter a whole lot more algebraic structures next term and in later courses which you never saw at school. A large part of modern mathematics consists of working with algebraic structures which are not the ones you know and love from school, and it's very important that you get used to the idea that you can work with them and you can become comfortable and confident with doing so, rather than trying to avoid it.

What actually is an algebraic structure? It's not really a formally defined thing; it just means a structure where you can do something that looks like algebra (maybe all the BIDMAS stuff from school, maybe you only know how to add, maybe somewhere in the middle). The natural numbers and the integers are algebraic structures. Later we'll meet the rational numbers, the real numbers and the complex numbers (which you may well already have seen; if not it doesn't matter). These are what you know from school, and you know they are contained one inside another; if you know how algebra in the complex numbers work, well, they contain all the rest and you maybe

feel that this is all there is to algebra.

But that's not true — in fact, you already know that, even if you didn't think of it that way. You know how to add and multiply 2×2 matrices too. So you can think of the set of 2×2 matrices, with addition and multiplication, as an algebraic structure. The rules that addition follows are just like the rules for addition in $\mathbb{Z}$; and the distributive law is also true. But multiplication is not commutative! This algebraic structure really behaves differently to the real or the complex numbers. But as you know from MA100, it's also very important. There are lots more examples; we're just about to show you another.

7.3 $\mathbb{Z}_m$ and its arithmetic

When, in an earlier chapter, we looked at how the integers may be *constructed* from the natural numbers through using an equivalence relation, we also saw that we could 'do arithmetic' with the equivalence classes. We can also do this here, and the resulting addition and multiplication operations are known as *modular arithmetic*.

First, let's introduce a new piece of notation. For $m \in \mathbb{N}$, $\mathbb{Z}_m$ is called the set of *integers modulo* m, and is the set of equivalence classes

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

So $\mathbb{Z}_m$ has m members (We saw $\mathbb{Z}_{24}$ before as the 'clock numbers' in Section 3.2). We can define operations $\oplus$ and $\otimes$ on $\mathbb{Z}_m$ as follows:

$$[x]_m \oplus [y]_m = [x+y]_m, \quad [x]_m \otimes [y]_m = [xy]_m.$$

For example, when $m = 4$, $[2]_4 \oplus [3]_4 = [5]_4 = [1]_4$ and $[2]_4 \otimes [3]_4 = [6]_4 = [2]_4$.

In practice, we do not use the $\oplus$ and $\otimes$ symbols and we simply write x instead of $[x]_m$. It's nice, when possible, to use values of x between 0 and $m-1$, so in our calculations if numbers get out of this range we will often add or subtract multiples of m to return; we say 'reduced modulo m'. This makes sense because $[x]_m = [x+sm]_m$ for each integer s. We would say that we are 'in $\mathbb{Z}_m$' if that's not clear from the context. So the above two calculations may be written:

$$\text{in } \mathbb{Z}_4, \quad 2+3=1, \quad \text{and } 2 \times 3 = 2.$$

Note that we try to use only the symbols $0, 1, \ldots, m-1$, so we do *not* write $2+3=5$. Instead we reduce it modulo 4, i.e. replace 5 by the number that it is congruent to modulo 4 and which lies between 0 and 3.

The equations we've just written are entirely equivalent to the statements

$$2+3 \equiv 1 \pmod 4, \quad 2 \times 3 \equiv 2 \pmod 4.$$

Let me again stress that we *usually* try to use only the symbols $0, 1, \ldots, m-1$, and generally we will want to write our final answer using those symbols. But it might well be useful along the way to use other symbols! In $\mathbb{Z}_8$ we have $7 = -1$, so we can

perfectly well write -1 in a calculation rather than 7 if we want. In fact, we did exactly that earlier. In $\mathbb{Z}_8$ we have

$$7^{100} - 1 = (-1)^{100} - 1 = 1 - 1 = 0$$

and that tells us that the integer $7^{100} - 1$ is divisible by 8.

The addition and multiplication operations we've defined on $\mathbb{Z}_m$ obey a number of rules that are familiar from normal addition and multiplication of integers. In fact, $\mathbb{Z}_m$ satisfies the properties ($\mathbb{Z}1$)–($\mathbb{Z}6$) we listed when we constructed the integers. But (as we saw before) the property ($\mathbb{Z}7$) doesn't necessarily hold: in $\mathbb{Z}_{24}$, for example, we have $5 \times 4 = 20 = 11 \times 4$, but 5 and 11 are not equal in $\mathbb{Z}_{24}$. Let's restate those properties for convenience.

Theorem 7.2 Let $m \in \mathbb{N}$. In $\mathbb{Z}_m$, for all a, b, c,

(i) $a + b$ and $a \times b$ are in $\mathbb{Z}_m$.

(ii) $a + b = b + a$

(iii) $a \times b = b \times a$

(iv) $(a + b) + c = a + (b + c)$

(v) $(a \times b) \times c = a \times (b \times c)$

(vi) $a + 0 = a$

(vii) $a \times 1 = a$ if $a \neq 0$

(viii) $a \times (b + c) = (a \times b) + (a \times c)$

(ix) for each $a \in \mathbb{Z}_m$ there is a unique element $-a \in \mathbb{Z}_m$ such that $a + (-a) = 0$.

Let's think a little about rule (ix) in this Theorem. Suppose we're in $\mathbb{Z}_4$ and that $a = 3$. What is $-a$? Well, what we want is an element of $\mathbb{Z}_m$ which when added to 3 gives 0 when we are doing arithmetic in $\mathbb{Z}_4$. Now, $3 + 1 = 0$ in $\mathbb{Z}_4$ because $3 + 1$ is congruent to 0 modulo 4, so $-3 = 1$. (Alternatively, we can note that $-3 = -1(4) + 1$, so -3 has remainder 1 on division by 4, so $-3 \equiv 1 \pmod 4$.)

Activity 7.3 In $\mathbb{Z}_9$, what is -4?

It is important to realise that arithmetic in $\mathbb{Z}_m$ does not obey *all* the nice properties that normal arithmetic of integers obeys. In particular, we cannot generally *cancel* multiplication. For example, in $\mathbb{Z}_4$,

$$2 \times 3 = 2 = 2 \times 1,$$

but we cannot 'cancel the 2' (that is, divide both sides by 2) to deduce that $3 = 1$, because $3 \neq 1$ in $\mathbb{Z}_4$. (The reason we cannot 'cancel' the 2 is that 2 has no inverse in $\mathbb{Z}_4$. Existence of inverses is the topic of the next section.)

7.4 Invertible elements in $\mathbb{Z}_m$

A member x of $\mathbb{Z}_m$ is *invertible* if there is some $y \in \mathbb{Z}_m$ such that (in $\mathbb{Z}_m$) $xy = yx = 1$. If such a y exists, it is called the *inverse* of x and is denoted by x^{-1}.

> **Example 7.4** In $\mathbb{Z}_{10}$, 3 has inverse 7 because, in $\mathbb{Z}_{10}$, $3 \times 7 = 1$ (because $3 \times 7 = 21 \equiv 1 \pmod{10}$).

> **Example 7.5** In $\mathbb{Z}_{10}$, 5 has no inverse. There is no x such that $5x = 1$. For, modulo 10, for any $x \in \mathbb{Z}$, $5x \equiv 0$ or 5. (This is just the familiar fact that any multiple of 5 has last digit 0 or 5.)

If $x \in \mathbb{Z}_m$ is invertible, then it is possible to *cancel* x from both sides of an equation in $\mathbb{Z}_m$. That is, we have

$$xa = xb \Rightarrow a = b \quad (\text{in } \mathbb{Z}_m).$$

This is not, as we have seen, generally true, but it works when x has an inverse because in this case

$$xa = xb \Rightarrow x^{-1}(xa) = x^{-1}(xb) \Rightarrow (x^{-1}x)a = (x^{-1}x)b \Rightarrow 1a = 1b \Rightarrow a = b.$$

7

Which $x \in \mathbb{Z}_m$ are invertible? The answer is given by the following theorem.

Theorem 7.3 Suppose $m \in \mathbb{N}$. Then an element x of $\mathbb{Z}_m$ is invertible if and only if x and m are coprime (that is, $\gcd(x, m) = 1$).

Proof. Suppose x is invertible, so that there is y with $xy = 1$ in $\mathbb{Z}_m$. This means that $xy \equiv 1 \pmod{m}$, so, for some $k \in \mathbb{Z}$, $xy = 1 + km$. Let $d = \gcd(x, m)$. Then $d \mid x$ and $d \mid m$, so $d \mid (xy - km)$. That is, $d \mid 1$, from which it follows that $d = 1$ and x and m are coprime.

Conversely, suppose $\gcd(x, m) = 1$. Then (by the fact that the gcd can be written as an integer linear combination), there are integers y, z such that $1 = yx + zm$. But this means $yx \equiv 1 \pmod{m}$, so, in $\mathbb{Z}_m$, $yx = 1$ and x has inverse y. □

As a result of this theorem, we see that if p is a prime, then every non-zero element x of $\mathbb{Z}_p$ is invertible. This is because $\gcd(x, p) = 1$.

7.5 Solving equations in $\mathbb{Z}_m$

7.5.1 Single linear equations

Suppose we want to solve, in $\mathbb{Z}_m$, the equation $ax = b$. That is, we want to find x between 0 and $m - 1$ such that $ax \equiv b \pmod{m}$. This may have no solutions. Indeed, suppose we take $b = 1$. Then the equation we're confronted with is $ax = 1$, which has a solution if and only if a is invertible (by definition of inverse). So if a has no inverse in $\mathbb{Z}_m$, then such a linear equation will not always have a solution. If, however, a is

invertible, then we can see that the equation $ax = b$ in $\mathbb{Z}_m$ has solution $x = a^{-1}b$, because $a(a^{-1}b) = (aa^{-1})b = 1b = b$.

How do you find a solution? Trial and error is not efficient if the numbers involved are large. But we can use the Euclidean algorithm. For suppose we want to solve $ax = b$ in $\mathbb{Z}_m$, where $\gcd(a, m) = 1$. Then, by using the Euclidean algorithm, we have seen how we can find integers k, l such that $1 = ak + ml$. So, $b = abk + mlb$. Since mlb is a multiple of m, by definition $abk \equiv b \pmod{m}$. So bk is a solution, and so $bk + sm$ will also be a solution for any integer s, because $bk \equiv bk + sm \pmod{m}$ by definition. It's usually nicest to find a solution between 0 and $m - 1$ inclusive, so we choose s to obtain this. It's easy to do this for explicit numbers.

Example 7.6 Suppose we want to solve the equation $83x = 2$ in $\mathbb{Z}_{321}$. We can check that 83 and 321 are coprime by the Euclidean algorithm (working in $\mathbb{Z}$), as follows: We have

$$\begin{aligned} 321 &= 83 \times 3 + 72 \\ 83 &= 72 \times 1 + 11 \\ 72 &= 11 \times 6 + 6 \\ 11 &= 6 \times 1 + 5 \\ 6 &= 5 \times 1 + 1 \\ 5 &= 1 \times 5. \end{aligned}$$

It follows that $\gcd(321, 83) = 1$. Now, working backwards, we can express 1 as an integer linear combination of 83 and 321:

$$\begin{aligned} 1 &= 6 - 5 \\ &= 6 - (11 - 6) = 6 \times 2 - 11 \\ &= (72 - 11 \times 6) \times 2 - 11 = 72 \times 2 - 11 \times 13 \\ &= 72 \times 2 - (83 - 72) \times 13 = 72 \times 15 - 83 \times 13 \\ &= (321 - 83) \times 3) \times 15 - 83 \times 13 = 321 \times 15 - 83 \times 58. \end{aligned}$$

This tells us that

$$83 \times (-58) \equiv 1 \pmod{321}.$$

So,

$$83 \times (-116) \equiv 2 \pmod{321}.$$

Now, we want to find x in the range 0 to 321 such that $-116 \equiv x \pmod{321}$. The answer is $x = 205$. So, finally, then, we see that, in $\mathbb{Z}_{321}$, the equation $83x = 2$ has solution $x = 205$.

Activity 7.4 This calculation also reveals that 83 is invertible in $\mathbb{Z}_{321}$. Why? And what is the inverse of 83 in $\mathbb{Z}_{321}$?

More generally, we can ask: when does $ax = b$ have a solution in $\mathbb{Z}_m$?

The answer is: when $d = \gcd(a, m)$ divides b.

So a special case is when $d = 1$.

That is, we have the following theorem.

Theorem 7.4 In $\mathbb{Z}_m$, $ax = b$ has a solution if and only if $d \mid b$, where $d = \gcd(a, m)$.

Proof. First part, $\Longrightarrow$: Suppose $ax_0 = b$ in $\mathbb{Z}_m$. Then $ax_0 - b = km$ for some $k \in \mathbb{Z}$. So, $b = ax_0 - km$. Since $d = \gcd(a, m)$, $d \mid a$ and $d \mid m$, so $d \mid (ax_0 - km)$. That is, $d \mid b$.

Second part, $\Longleftarrow$: Suppose $d \mid b$, so $b = db_1$ for some $b_1 \in \mathbb{Z}$. There are x_1, y_1 such that $d = x_1a + y_1m$. Then, $b = db_1 = (x_1b_1)a + (y_1b_1)m$.
So, in $\mathbb{Z}_m$, $a(x_1b_1) = b$. That is, x_1b_1 (reduced modulo m) is a solution. □

This theorem suggests a general method for solving $ax = b$ in $\mathbb{Z}_m$:

- Find $d = \gcd(a, m)$.
- If $d \nmid b$, there's no solution.
- If $d \mid b$, write $b = db_1$. Use Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $d = xa + ym$. Then a solution is xb_1, reduced modulo m.

7.5.2 Systems of linear equations

We can also consider simultaneous linear equations in $\mathbb{Z}_m$. It should be realised that there might be no solutions, or more than one solution.

Example 7.7 Let's solve the following two equations simultaneously in $\mathbb{Z}_6$:

$$2x + 3y = 1, \quad 4x + 3y = 5.$$

Subtracting the first equation from the second gives $2x = 4$. You might be tempted to cancel the 2 and deduce that x must be 2. But wait! You can't cancel unless 2 and 6 are coprime, and they are not (since their gcd is 2). Instead, you can check for each of the elements of $\mathbb{Z}_6$ whether $2x = 4$. Of course, $x = 2$ is a solution, but so also is $x = 5$ because, in $\mathbb{Z}_6$, $2(5) = 10 = 4$. You can also check by calculating the other values of $2x$ that $x = 2, 5$ are the only solutions. Now, from the first equation, $3y = 1 - 2x$. When $x = 2$ or 5, $2x = 4$, so this is $3y = 1 - 4 = -3 = 3$. So we now have $3y = 3$. Again, we cannot cancel the 3. Instead we check, for each $y \in \mathbb{Z}_6$, whether it is a solution, and we find that $1, 3$ and 5 are all solutions. What this argument shows is that the *possible* solutions are

$$(x, y) = (2, 1), (2, 3), (2, 5), (5, 1), (5, 3), (5, 5).$$

In fact, it can easily be checked (by substituting these pairs of values into the original equations) that these are indeed solutions. So this system has 6 different solutions.

Activity 7.5 Check, by substituting into the original equations, that each of these six possible solution pairs (x, y) is indeed a solution.

Example 7.8 Consider the following system of simultaneous equations in $\mathbb{Z}_7$:

$$3x + y = 1, \quad 5x + 4y = 1.$$

If we multiply the first equation by 4, we obtain $12x + 4y = 4$, which is the same (in $\mathbb{Z}_7$) as $5x + 4y = 4$. But the second equation says $5x + 4y = 1$. Since 1 and 2 are not equal in $\mathbb{Z}_7$, these equations are inconsistent, so there are no solutions to this system.

There is a general theory of how to solve systems of linear equations in modular arithmetic, using something called the Chinese remainder theorem. However, for this course we will not need it. If you are asked to solve a system of linear equations modulo m in this course, there are two possibilities.

First, m is some small number. In this case you can do something like the procedure in Example 7.7: do a bit of algebra to rule out some possibilities, and then just check all the possibilities left over to see which ones work.

Second, m is a prime number. In this case, just use the theory you learned in MA100.

You are quite possibly very unhappy about the last sentence — I'll explain it in the next chapter!

7.6 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- state the definition of the equivalence relation congruence modulo m
- prove that congruence modulo m is an equivalence relation
- demonstrate an understanding of the links between congruence modulo m and remainder on division by m
- state and prove standard properties of congruence
- apply congruence to show, for example, that equations have no solutions
- demonstrate an understanding of what the congruence classes are
- demonstrate an understanding of what $\mathbb{Z}_m$ means and how its addition and multiplication are defined
- find the negatives of elements of $\mathbb{Z}_m$
- state the definition of an invertible element of $\mathbb{Z}_m$
- demonstrate that you know an element x in $\mathbb{Z}_m$ is invertible if and only if x and m are coprime
- find the inverse of an invertible element
- solve linear equations and simple systems of linear equations in $\mathbb{Z}_m$

7.7 Sample exercises

Exercise 7.1
Show that $n \equiv 7 \pmod{12} \Rightarrow n \equiv 3 \pmod{4}$. Is the converse true? □

Exercise 7.2
Show that for all $n \in \mathbb{Z}$, $n^2 \equiv 0$ or $1 \pmod{3}$. Hence show that if 3 divides $x^2 + y^2$ then $3 \mid x$ and $3 \mid y$. Use this to prove that there are no integers x, y, z such that $x^2 + y^2 = 3z^2$, other than $x = y = z = 0$.

Exercise 7.3
Show that, for all $n \in \mathbb{N}$, $3^{3n+1} \equiv 3 \times 5^n \pmod{11}$ and that $2^{4n+3} \equiv 8 \times 5^n \pmod{11}$. Hence show that for all $n \in \mathbb{N}$, $11 \mid (3^{3n+1} + 2^{4n+3})$. □

Exercise 7.4
By working modulo 7, prove that $2^{n+2} + 3^{2n+1}$ is divisible by 7. (This result was proved in a different way, using induction, in the exercises at the end of Chapter 3)

Exercise 7.5
Prove that 290 is an invertible element of $\mathbb{Z}_{357}$ and find its inverse. □

Exercise 7.6
Solve the equation $10x = 3$ in $\mathbb{Z}_{37}$. □

7

7.8 Comments on selected activities

Learning activity 7.1 We have $m \mid 0 = a - a$, so the relation is reflexive. Symmetry follows from $m \mid (b - a) \iff m \mid (a - b)$. Suppose that $a \, R \, b$ and $b \, R \, c$. Then $m \mid (b - a)$ and $m \mid (c - b)$, so $m \mid ((b - a) + (c - b)) = (c - a)$ and hence $a \, R \, c$. Thus, R is transitive.

Learning activity 7.2 We have $m \mid (b - a)$ and $m \mid (d - c)$. So $m \mid ((b - a) + (d - c))$, which is the same as $m \mid ((b + d) - (a + c))$, so $a + c \equiv b + d \pmod{m}$. We also have $m \mid ((b - a) - (d - c))$, which is the same as $m \mid ((b - d) - (a - c))$ so $a - c \equiv b - d \pmod{m}$.

Learning activity 7.3 Because $4 + 5 = 9 \equiv 0 \pmod{9}$, we have $-4 = 5$ in $\mathbb{Z}_9$.

Learning activity 7.4 The calculation shows that $83 \times (-58) \equiv 1 \pmod{321}$. We also know that $-58 \equiv 263 \pmod{321}$ because $58 + 263 = 312 \equiv 0 \pmod{321}$. So we'll have $83 \times 263 \equiv 1 \pmod{321}$. This shows that 83 is invertible in $\mathbb{Z}_{321}$ and that its inverse is 263.

7.9 Solutions to exercises

Solution to exercise 7.1
If $n \equiv 7 \pmod{12}$ then, for some integer k, $m = 7 + 12k$ and so $m = 3 + 4 + 12k = 3 + 4(1 + 3k)$. This means that $n \equiv 3 \pmod{4}$, because $1 + 3k$ is an

integer. The converse is false, because, for example, $3 \equiv 3 \pmod 4$, but $3 \not\equiv 7 \pmod{12}$

Solution to exercise 7.2

We have, modulo 3, $n \equiv 0$ or $n \equiv 1$ or $n \equiv 2$. So, respectively, $n^2 \equiv 0^2 = 0$ or $n^2 \equiv 1^2 = 1$ or $n^2 \equiv 2^2 = 4 \equiv 1$. So in all cases n^2 is congruent to 0 or 1. Suppose $3 \,|\, (x^2 + y^2)$. Then, modulo 3, $x^2 + y^2 \equiv 0$. But each of x^2 and y^2 is congruent to 0 or 1. If either or both are congruent to 1, then we'd have $x^2 + y^2 \equiv 1$ or $x^2 + y^2 \equiv 2$. So we can see that we must have $x^2 \equiv 0$ and $y^2 \equiv 0$. This means $x \equiv 0$ and $y \equiv 0$, which is the same as $3 \,|\, x$ and $3 \,|\, y$.

Now suppose that, for integers x, y, z, $x^2 + y^2 = 3z^2$, where not all of x, y, z are zero. If d is a common factor of x, y and z, then we can write $x = dx_1$, $y = dy_1$ and $z = dz_1$, where $x_1, y_1, z_1 \in \mathbb{Z}$. We can then see that $d^2x_1^2 + d_2y_1^2 = 3d^2z_1^2$, so that $x_1^2 + y_1^2 = 3z_1^2$. What this shows is that if there are any integer solutions, then there is one in which x, y, z have no common divisors (for any common divisors can be cancelled). So assume we're dealing with such a solution. Now, $x^2 + y^2 = 3z^2$ implies $3 \,|\, (x^2 + y^2)$ (noting that neither side of the equation is 0 because not all of x, y, z are). What we've shown earlier in this exercise establishes that $3 \,|\, x$ and $3 \,|\, y$. So $x = 3x_1$ and $y = 3y_1$ for some $x_1, y_1 \in \mathbb{Z}$. Then the equation $x^2 + y^2 = 3z^2$ becomes $9x_1^2 + 9y_1^2 = 3z^2$ and so $z^2 = 3x_1^2 + 3y_1^2$. This implies $3 \,|\, z^2$. But this means $3 \,|\, z$. (You can see this either by the Fundamental Theorem of Arithmetic, or by the fact that if $z \not\equiv 0$ modulo 3 then $z^2 \not\equiv 0$, as we see from the calculations at the start of this solution.) So what we see, then, is that x, y, z are all divisible by 3. But we assumed that they constituted a solution with no common factor and we've reached a contradiction. So there are no solutions other than $x = y = z = 0$.

Solution to exercise 7.3

Modulo 11, we have $3^3 = 27 \equiv 5$ and so $3^{3n} \equiv (3^3)^n \equiv 5^n$ and hence $3^{3n+1} = 3(3^n) \equiv 3 \times 5^n$. Also, $2^4 = 16 \equiv 5$ and so $2^{4n+3} = 8 \times (2^4)^n \equiv 8 \times 5^n$. It follows that

$$3^{3n+1} + 2^{4n+3} \equiv 3 \times 5^n + 8 \times 5^n = 11(5^n) \equiv 0 \pmod{11},$$

which means that $11 \,|\, (3^{3n+1} + 2^{4n+3})$. □

Solution to exercise 7.4

Modulo 7, $3^2 = 9 \equiv 2$, so $3^{2n+1} = 3(3^{2n}) \equiv 3(2^n)$ and $2^{n+2} = 4(2^n)$, so

$$2^{n+2} + 3^{2n+1} \equiv 4(2^n) + 3(2^n) = 7(2^n) \equiv 0,$$

and hence $7 \,|\, (2^{n+2} + 3^{2n+1})$. □

Solution to exercise 7.5

By the Euclidean algorithm, we have

$$\begin{aligned} 357 &= 290 + 67 \\ 290 &= 4 \times 67 + 22 \\ 67 &= 3 \times 22 + 1, \end{aligned}$$

so 290 and 357 are coprime, from which it follows that 290 is invertible. Now, from the calculations just given,

$$\begin{aligned} 1 &= 67 - 3 \times 22 \\ &= 67 - 3(290 - 4 \times 67) = 13 \times 67 - 3 \times 290 \\ &= 13(357 - 290) - 3 \times 290 = 13 \times 357 - 16 \times 290. \end{aligned}$$

The fact that $13 \times 357 - 16 \times 290 = 1$ means that, modulo 357, $-16 \times 290 \equiv 1$. So, in $\mathbb{Z}_{357}$, $(290)^{-1} = -16 = 341$.

Solution to exercise 7.6

Because 37 is prime, we certainly know that 10 and 37 are coprime, so the equation has a solution. The quickest way to find it is simply to note that the equation is equivalent to the congruence, modulo 37, that $10x \equiv 40$, and the 10 can then be cancelled because 10 and 37 are coprime. But suppose we didn't spot that. The Euclidean algorithm tells us that:

$$\begin{aligned} 37 &= 3 \times 10 + 7 \\ 10 &= 1 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \\ 3 &= 3 \times 1, \end{aligned}$$

and so

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2(10 - 7) = 3 \times 7 - 2 \times 10 \\ &= 3(37 - 3 \times 10) - 2 \times 10 \\ &= 3 \times 37 - 11 \times 10. \end{aligned}$$

So we see that $-11 \times 10 \equiv 1 \pmod{37}$ and hence $-33 \times 10 \equiv 3 \pmod{37}$. Now, $-33 \equiv 4 \pmod{37}$, so the solution is $x = 4$. This is easily checked: $10(4) = 40 = 3$ in $\mathbb{Z}_{37}$. □

Chapter 8
Rational, real and complex numbers

☞ Biggs, N. L. *Discrete Mathematics*. Chapter 9.

☞ Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapters 13 and 14.

The treatment in Biggs is probably better for the purposes of this course.

Neither of these books covers complex numbers. You do not have to know very much about complex numbers for this course, but because this topic is not in these books, I have included quite a bit of material on complex numbers in this chapter.

You can find useful reading on complex numbers in a number of books, including the following (which you might already have, given that it is the MA100 text).

☞ Anthony, M. and M. Harvey. *Linear Algebra: Concepts and Methods*. Cambridge University Press 2012. Chapter 13.

8.1 Introduction

In this chapter, we explore rational numbers, real numbers and complex numbers. In this course, we started with natural numbers and then we showed how to construct the set of all integers from these. This construction used an equivalence relation, together with a suitable way of adding and multiplying the equivalence classes. In a similar way, the rational numbers can be constructed from the integers by means of an equivalence relation. In this course, we do not take a very formal approach to the definition or construction of the real numbers (which can, in fact, be quite complicated). But we study properties of real numbers, and in particular we shall be interested in whether real numbers are rational or not. We also consider the 'cardinality' of infinite sets.

As we stressed before, the point of these formal constructions is *not* to make you think about a complicated construction which gets in the way of 'calculation as usual'. Once you proved that a construction does what it's supposed to do, you don't have to think any more; you can calculate as usual. But by now we are getting to mathematical structures which don't obviously make sense—look back to Section 3.10, and again: why does $\mathbb{C}$ exist but $\mathbb{E}$ doesn't? You don't have—yet—any very good reason to believe that calculations using $\mathbb{C}$ make any more sense than using $\mathbb{E}$; maybe all this complex number stuff is nonsense, simply the calculations which show it doesn't work are a bit harder to find than the one which shows $\mathbb{E}$ is nonsense? By the end of this chapter, you should be convinced that it is not nonsense.

8.2 Rational numbers

As when we constructed $\mathbb{Z}$ from $\mathbb{N}$, we are now going to construct the rational numbers $\mathbb{Q}$ from $\mathbb{Z}$. As before, the reason we want to do this—rather than just assume $\mathbb{Q}$ exists and calculations with it make sense—is that, as we saw in Section 3.10, we might be assuming something which is nonsense; it might be that if we try to do algebra with fractions as we're used to, we end up doing a calculation which shows $1 = 1 + 1$ (as with $\mathbb{E}$).

Think about this for a moment—you might say you can make sense of $\frac{-1}{5}$ in terms of reality: it means I owe you a fifth of an apple; if there are five people who each owe you a fifth of an apple, then you are owed one apple, and this all sounds good. But what does it mean to multiply by $\frac{-1}{5}$? Why is $\frac{-1}{5} \cdot \frac{-1}{5}$ equal to $\frac{1}{25}$? You can probably come up with some sentence involving apples, but I'm not sure it will be very convincing—try it!

When we constructed $\mathbb{Z}$ from $\mathbb{N}$, we wrote down a rather funny equivalence relation, and used that to prove that if $\mathbb{Z}$ is in some way nonsense, then so is $\mathbb{N}$—to put it another way, if you're convinced calculations with $\mathbb{N}$ work, then you are also convinced that calculations with $\mathbb{Z}$ work. We're going to do the same thing again, but this time the equivalence relation is one you saw long ago in primary school.

8.2.1 An important equivalence relation

Rational numbers are simply the fractions you already studied in primary school. You'll certainly be aware that there are many ways of representing a given rational number. For instance, $\frac{2}{5}$ represents the same number as $\frac{4}{10}$. We can capture these sorts of equivalences more formally by using an equivalence relation on pairs of integers (m, n), where $n \neq 0$. So let $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ be the set of all pairs (m, n) where $m, n \in \mathbb{Z}$ and $n \neq 0$, and define a relation R on X by:

$$(m, n)\ R\ (m', n') \iff mn' = m'n.$$

You should quickly check that this relation R does what you think it should do: if (by your school-style calculation) the fractions $\frac{m}{n}$ and $\frac{m'}{n'}$ are the same, then indeed we have $(m, n)R(m', n')$. However so far in this course we did not define 'division' nor 'fraction'—that's exactly what we want to do now. The relation R only uses the properties of $\mathbb{Z}$ which we are already happy with.

Let's pause for a moment to prove that R is indeed an equivalence relation.

R **is Reflexive:** $(m, n)R(m, n)$ because $mn = nm$.

R **is Symmetric:** $(m, n)R(p, q) \Rightarrow mq = np \Rightarrow pn = qm \Rightarrow (p, q)R(m, n)$.

R **is Transitive:** Suppose $(m, n)R(p, q)$ and $(p, q)R(s, t)$. Then $mq = np$ and $pt = qs$. So, $(mq)(pt) = (np)(qs)$ and, after cancelling qp, this gives $mt = ns$, so $(m, n)R(s, t)$. But, wait a minute: can we cancel pq? Sure, if it's nonzero. If it *is* zero then that means $p = 0$ (since we know that $q \neq 0$). But then $mq = 0$, so $m = 0$; and $qs = 0$, so $s = 0$. So, in this case also we get $mt = ns$ (both sides are zero) and so $(m, n)R(s, t)$.

8.2.2 Rational numbers as equivalence classes

We represent the equivalence class $[(m,n)]$ by $\dfrac{m}{n}$. For example, we then have the (familiar) fact that $\frac{2}{5} = \frac{4}{10}$ which follows from the fact that $[(2,5)] = [(4,10)]$, something that is true because $(2,5)\ R\ (4,10)$ ($2 \times 10 = 4 \times 5$). What we've done here is construct the set of rational numbers without reference to division. In an abstract approach, this is the logically sound thing to do. Once we have constructed the rational numbers, we can then make sense of the division of integers: the division of m by n is the rational number m/n.

What, for instance, is the equivalence class $[(1,2)]$? Well, $(m,n)R(1,2)$ means $m \times 2 = n \times 1$, or $n = 2m$. So it consists of

$$(1,2), (-1,-2), (2,4), (-2,-4), (3,6), (-3,-6) \ldots .$$

Denoting the equivalence class $[(m,n)]$ by $\dfrac{m}{n}$, we therefore have

$$\frac{1}{2} = \{(1,2), (-1,-2), (2,4), (-2,-4), (3,6), (-3,-6), \ldots\}.$$

Recall that if $x' \in [x]$ then $[x'] = [x]$. So we can say

$$\frac{1}{2} = \frac{-1}{-2} = \frac{2}{4} = \frac{-2}{-4} = \frac{3}{6} = \frac{-3}{-6} = \cdots .$$

We can think of the integers as particular rational numbers by identifying the integer n with the rational number $\dfrac{n}{1}$ (that is, with the equivalence class $[(n,1)]$). So $\mathbb{Z} \subseteq \mathbb{Q}$.

8.2.3 Doing arithmetic

How do we 'do arithmetic' with rational numbers. Well, you've been doing this for years, but how would we define addition and multiplication of rational numbers in an abstract setting? Just as we defined operations on equivalence classes in earlier chapters (in the construction of $\mathbb{Z}$ from $\mathbb{N}$ and in the construction of $\mathbb{Z}_m$), we can define addition and multiplication as an operation on the equivalence classes of R. Here's how: let $\oplus$ and $\otimes$ be defined on the set of rational numbers as follows:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \otimes \frac{c}{d} = \frac{ac}{bd}.$$

In practice, we just use normal addition and multiplication symbols (and we often omit the multiplication symbol), so we have

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Well, no surprises there, but remember that what we are doing here is *defining* additional and multiplication of rational numbers (and remember also that these rational numbers are, formally, equivalence classes). Now, if you think hard about it, one issue that is raised is whether these definitions depend on the choice of

representatives from each equivalence class (just as when we constructed $\mathbb{Z}$ from $\mathbb{N}$, we had to check this). They should not, but we ought to check that. What I mean is that we really should have

$$\frac{2}{5}+\frac{2}{6}=\frac{4}{10}+\frac{1}{3},$$

for example, because

$$\frac{2}{5}=\frac{4}{10} \text{ and } \frac{2}{6}=\frac{1}{3}.$$

Well, let's see. Consider the addition definition. Suppose that

$$\frac{a}{b}=\frac{a'}{b'} \text{ and } \frac{c}{d}=\frac{c'}{d'}.$$

What we need to check is that

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}.$$

Now, the fact that $\frac{a}{b}=\frac{a'}{b'}$ means precisely that $[(a,b)]=[(a',b')]$, which means that $ab'=a'b$. Similarly, we have $cd'=c'd$. Now,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \text{ and } \frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}$$

and we need to prove that

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}.$$

This means we need to prove that

$$(ad+bc,bd)\ R\ (a'd'+b'c',b'd').$$

Now,

$$\begin{aligned}(ad+bc,bd)\ R\ (a'd'+b'c',b'd') &\iff (ad+bc)b'd'=(a'd'+b'c')bd\\ &\iff adb'd'+bcb'd'=a'd'bd+b'c'bd\\ &\iff (ab')dd'+(cd')bb'=(a'b)dd'+(c'd)bb'.\end{aligned}$$

Now, the first terms on each side are equal to each other because $ab'=a'b$ and the second terms are equal to each other because $cd'=c'd$, so we do indeed have 'consistency' (that is, the definition of addition is independent of the choice of representatives chosen for the equivalence classes).

> **Activity 8.1** Show that the definition of multiplication of rational numbers is 'consistent': that is, that it does not depend on the choice of representatives chosen for the equivalence classes. Explicitly, show that if
>
> $$\frac{a}{b}=\frac{a'}{b'} \text{ and } \frac{c}{d}=\frac{c'}{d'},$$
>
> then
>
> $$\frac{a}{b}\times\frac{c}{d}=\frac{a'}{b'}\times\frac{c'}{d'}.$$

By the way, the rational numbers are described as such because they are (or, more formally, can be represented by) *ratios* of integers.

The rational numbers (as you can easily check, and as you already knew long ago) satisfy the following axioms:

(𝔽1) Closure under addition and multiplication: for each $a, b \in \mathbb{F}$ both $a + b$ and ab are in $\mathbb{F}$.

(𝔽2) Commutative addition and multiplication: for each $a, b \in \mathbb{F}$ we have $a + b = b + a$ and $ab = ba$.

(𝔽3) Associative addition and multiplication: for each $a, b, c \in \mathbb{F}$ we have $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(𝔽4) The distributive law: for each $a, b, c \in \mathbb{F}$ we have $(a + b)c = ac + bc$.

(𝔽5) Additive and multiplicative identity: there are two different elements 0 and 1, such that for each $a \in \mathbb{F}$ we have $a + 0 = a$ and $a \times 1 = a$.

(𝔽6) Additive and multiplicative inverses: for each $a \in \mathbb{F}$ there is an element $-a$ such that $a + (-a) = 0$, and if $a \neq 0$ there is an element a^{-1} such that $a(a^{-1}) = 1$.

There is a name for structures $\mathbb{F}$ which satisfy all of these axioms: they form a *field*. So the rational numbers are a field. You don't need to memorise the list (and it won't be on the exam), because what it says is simply that in any field you can do algebra as you are used to, with addition, subtraction, multiplication and division, and nothing will 'go wrong'; you will never somehow get an answer which isn't in the field (as you would if you tried to work out $3 - 5$ in $\mathbb{N}$, or $3/5$ in $\mathbb{Z}$), nor will the answer do something unexpected (like depending on the order you do things, as would be the case with multiplying 2×2 matrices: there multiplication isn't commutative).

You probably feel intuitively that a field should be something like the rational numbers (or the real or complex numbers, which we'll formally meet shortly). Another, rather different, example of a field is $\mathbb{Z}_p$ for any prime number p. We saw in the last chapter that all the axioms of a field, except (𝔽6), holds for $\mathbb{Z}_m$ whatever m is; and we saw that the additive inverses part of (𝔽6) holds whatever m is. And we saw that if m is prime, then so does the multiplicative inverses part of (𝔽6) — that's all we need to check. So $\mathbb{Z}_2 3$ is a field—but $1 + 1 + \cdots + 1$ could be equal to 0 in $\mathbb{Z}_{23}$ (it is, if there are 23 '1's, for example) whereas this never occurs in $\mathbb{Q}$.

Why should you care about fields? Well, think about solving systems of linear equations in $\mathbb{R}$ using Gaussian elimination (or, as you learned to do in MA100, by writing it in terms of matrices and doing row reduction). What do you do there? You add and subtract real numbers; you multiply and divide (which is the same as multiplying by the multiplicative inverse). And you get an answer. Well, you can do all that in any field, in exactly the same way, because that's what the field axioms say you can do.

So if you want to solve a system of linear equations in $\mathbb{Z}_{23}$, then you can do it just as you would in $\mathbb{R}$, as you learned in MA100, except do your calculations in $\mathbb{Z}_{23}$. Let's try to solve this one, in $\mathbb{Z}_{23}$, by Gaussian elimination:

$$3x + 6y = 4 \quad \text{and} \quad 7x + y = 1$$

Well, we can take 6 times the second equation from the first:

$$3x - 42x = 4 - 6\,, \quad \text{i.e. } 7x = 21$$

And we can multiply this by 7^{-1} to get $x = 3$. Plugging that into $3x + 6y = 4$ we get $9 + 6y = 4$, so $6y = 18$, so $y = 3$. And we're done.

There are lots more examples of fields, some of which you will meet later in your programme — and what you've just seen is that all that linear algebra you're learning in MA100 doesn't just apply to the real and complex numbers, it applies to all fields. You've been learning much more than you thought you were! And this is a large part of the reason for this axiomatic approach to algebra: it lets you clearly see where you can use methods you already know to handle completely new structures.

8.3 Rational numbers and real numbers

So far, you probably never really saw a need for numbers which are not rational. You can add, subtract, multiply and divide rational numbers (apart from dividing by zero, which you saw in Section 3.10 is something you can't do without running into trouble) and you always get a rational number—why do we need more?

Theorem 8.1 The real number $\sqrt{2}$ is irrational. That is, there are no positive integers m, n with $\left(\frac{m}{n}\right)^2 = 2$.

8

Proof. Suppose, for a contradiction, that there were such m, n.

If m, n are divisible by some $d > 1$, we may divide both m and n to obtain m', n' such that the rational number m'/n' equals m/n. So we may assume that m, n have no common divisors greater than 1; that is, $\gcd(m, n) = 1$.

Now, the equation $(m/n)^2 = 2$ means $m^2 = 2n^2$. So we see that m^2 is even. We know (from Chapter 2) that this means m must be even. So there is some m_1 such that $m = 2m_1$. Then, $m^2 = 2n^2$ becomes $4m_1^2 = 2n^2$, and so $n^2 = 2m_1^2$. Well, this means n^2 is even and hence n must be even. So m and n are both divisible by 2. But we assumed that $\gcd(m, n) = 1$, and this is contradicted by the fact that m and n have 2 as a common divisor. So our assumption that $(m/n)^2 = 2$ must have been wrong and we can deduce no such integers m and n exist. □

Isn't this theorem a thing of beauty?

> **Activity 8.2** Make sure you understand that this is a proof by contradiction, and that you understand what the contradiction is.

What this theorem tells us is that, at least if we want to solve equations like $x^2 = 2$, then the rational numbers are not enough; we need more. Of course, we could just invent new symbols and define them to satisfy the equations we want. But (as is the case for $\mathbb{E}$ from Section 3.10) this is a dangerous thing to do—we might be assuming something exists which doesn't in fact exist; whose existence leads to a contradiction. We'd better rather construct the reals.

8.3.1 Non-examinable: what are the real numbers exactly?

There is a simple way to define the real numbers, which you already saw in school. We just say that these are all the things you can get by writing down a decimal number: 123.4124581... for example. Except that we say 0.9999 and 1.000 are to be considered the same (and similarly for any other decimal which after some point consists only of nines). How do we formalise that?

Well, it's easy enough; we can write a decimal as consisting of (for example) an integer n together with a string of digits after the decimal: $(123, 4, 1, 2, 4, 5, 8, 1, ...)$. This is a member of the set $\mathbb{N} \times \{0, 1, \ldots, 9\} \times \{0, 1, \ldots, 9\} \times \ldots$. (There's nothing wrong with an infinite product of sets.) And we can easily write down an equivalence relation which says that $(n, a_1, a_2, \ldots, a_k, 9, 9, 9, \ldots)$ is equivalent to $(n, a_1, a_2, \ldots, a_k + 1, 0, 0, 0, \ldots)$ (whenever a_k is not 9)—we just did it. The real numbers are then the equivalence classes of this relation.

It is a pain to define addition and multiplication. It is *not* hard, it is just annoying. You simply write out the details of how you would in practice add or multiply two numbers by hand (as you learnt to do in primary school). It's not hard, but it is painful, to check that it doesn't matter which representative of an equivalence class you take. And you can check that the structure you end up with is a field—it satisfies (𝔽1)–(𝔽6).

But there is something a bit worrying about this definition: it depends on the fact that we do arithmetic in base 10. Maybe the Martians (who have six fingers, at least in the B-movies I watch) will have a different set of real numbers? That would be terrible—they would certainly attack us if they found out. And in any case, it's not even obvious this definition fixes the problem—is there a decimal whose square is equal to 2?

In fact, these concerns turn out not to be real problems. It doesn't make a difference what base you use, and there is such a decimal. But nevertheless, mathematicians tend to prefer one of two different constructions. These two constructions are really different; depending on what you want one or the other might look 'better', and some mathematicians will get very angry if you don't like their favourite construction. However—and we will *not* prove it!—it doesn't really make a difference which construction you use; you still get a set which behaves the way you think the real numbers should. As before, the point of the construction isn't that you should keep thinking about it when you do calculations, it is to justify that your calculations won't give you a logical contradiction as we saw with 𝔼 from Section 3.10.

The first way is called the 'Dedekind cut' construction.

The idea is the following: if I pick a point on the number line, intuitively it separates the number line into the smaller points and the points at least as large. I can't really make formal sense of that idea—it's recursive: I'm talking about the number line in order to define the number line. But I can also talk about separating the fractions into two sets, and I know how to work with those. Formalising this, I can say a set S of rational numbers is a Dedekind cut if for every rational number x, either x is in S and there is an element s of S which is larger than x, or alternatively x is larger than all elements of S. And then I can say a real number is the same thing as a Dedekind cut. I can easily define addition: it's not hard to check that if S and S' are Dedekind cuts,

then the set $\{s + s' : s \in S, s' \in S'\}$ is a Dedekind cut. More or less the same idea works for multiplication (but you have to be rather careful with negative numbers!). If q is a rational number, then $\{x \in \mathbb{Q} : x < q\}$ is a Dedekind cut which we can easily check behaves like the rational number q (in the same way that the rational number $\frac{2}{1}$ behaves like the integer 2). Now, this definition at least solves the $\sqrt{2}$ problem: $\{q \in \mathbb{Q} : q < 0 \text{ or } q^2 < 2\}$ is a Dedekind cut, and its square is 2. This is a nice clean definition, but it only works because we have a definition of 'order' $<$ on $\mathbb{Q}$.

The second route is the 'Cauchy sequence' construction. This is rather more complicated.

The idea is the following: if I want to specify a real number, I'll give a sequence of rational numbers which get closer and closer to the number I want (the formal term is 'Cauchy sequence'; it'll be defined next term), such as longer and longer parts of the decimal expansion of $\sqrt{2}$; I might give the sequence

$$(1, 1.4, 1.41, 1.414, ...) .$$

It's easy to add such sequences—I just add the terms:

$$(a_1, a_2, a_3, ...) + (b_1, b_2, b_3, ...) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, ...) .$$

Multiplication works similarly (this time negative numbers aren't a problem). So far this looks rather like the 'decimals' construction. But of course I might have many possible sequences of rational numbers which get closer and closer to say 0 (or any other real number), so I should write down an equivalence relation which says two such sequences are equivalent. And then the real numbers are the equivalence classes of this relation.

By the end of next term, you should be able to make formal sense of this second construction—in fact, it would be a good check of your understanding to come back and try to fill in the details. This construction has the advantage that it doesn't use the idea of 'order'; you can use the same idea in lots of different situations. But it requires a lot more work to set up.

8.3.2 Real numbers: a 'sketchy' introduction

For the purposes of this course, you can just think of the real numbers $\mathbb{R}$ as being given; they are all the points on the number line, or equivalently they are all the decimal numbers (bearing in mind that $0.4999... = 0.5000...$). Let's think for a bit about these decimals, and (again a little bit informally) let's write down some properties they have.

First, let's note that if $a_i \in \mathbb{N} \cup \{0\}$ and $a_i \leq 9$ for $1 \leq i \leq n$, then the (finite) decimal expansion

$$a_0.a_1a_2 \ldots a_n$$

represents the rational number

$$a_0 + \frac{a_1}{10} + \frac{a_2}{(10)^2} + \cdots + \frac{a_n}{(10)^n}.$$

For example, what we mean by 1.2546 is the number

$$1 + \frac{2}{10} + \frac{5}{100} + \frac{4}{1000} + \frac{6}{10000}.$$

Every positive real number can be represented by an infinite decimal expansion

$$a_0.a_1a_2a_3 \ldots a_i \ldots,$$

where $a_i \in \mathbb{N} \cup \{0\}$ and $a_i \leq 9$ for $i \geq 1$. We allow for a_i to be 0, so, in particular, it is possible that $a_i = 0$ for all $i \geq N$ where N is some fixed number: such an expansion is known as a *terminating* expansion. Given such an infinite decimal expansion, we say that it represents a real number a if, for all $n \in \mathbb{N} \cup \{0\}$,

$$a_0.a_1a_2 \ldots a_n \leq a \leq a_0.a_1a_2 \ldots a_n + 1/(10)^n.$$

This formalism allows us to see that the infinite decimal expansion $0.99999\ldots$, all of whose digits after the decimal point are 9, is in fact the same as the number $1.0000000\ldots$.

For example, two infinite decimal expansions are

$$3.1415926535\ldots$$

and

$$0.1833333333333\ldots.$$

(You'll probably recognise the first as being the number π.) Suppose, in this second decimal expansion, that every digit is 3 after the first three (that is, $a_i = 3$ for $i \geq 3$). Then we write this as $0.18\overline{3}$ (or, in some texts, $0.18\dot{3}$). We can extend this notation to cases in which there is a repeating pattern of digits. For example, suppose we have

$$0.1123123123123\ldots,$$

where the '123' repeats infinitely. Then we denote this by $0.1\overline{123}$.

8.3.3 Rationality and repeating patterns

You probably have heard stories of strange, obsessive mathematicians working out the expansion of π to millions and millions of decimal places. (This has been the subject of a novel, a play, a film, and a song!) This is relevant because the digits of π have no repeating pattern, which you might think quite remarkable. In fact, it turns out that a real number will have an infinitely repeating pattern in its decimal expansion (which includes the case in which the pattern is 0, so that it includes terminating expansions) *if and only if* the number is rational.

Let's look at part of this statement: if a number is rational, then its decimal expansion will have a repeating pattern (which might be 0). Let's look at an example.

Example 8.1 We find the decimal expansion of $4/7$ by 'long-division'.

$$
\begin{array}{r|l}
 & 0.5714285\cdots \\
\hline
7 & 4.0000000 \\
 & \underline{3.5} \\
 & 50 \\
 & \underline{.49} \\
 & 10 \\
 & \underline{7} \\
 & 30 \\
 & \underline{28} \\
 & 20 \\
 & \underline{14} \\
 & 60 \\
 & \underline{56} \\
 & 40 \\
 & \underline{35} \\
 & 50
\end{array}
$$

So,

$$4/7 = 0.\overline{571428}.$$

Notice: we must have the same remainder re-appear at some point, and then the calculation repeats. Here's the calculation again, with the repeating remainder highlighted in bold.

$$
\begin{array}{r|l}
 & 0.5714285\cdots \\
\hline
7 & 4.0000000 \\
 & \underline{3.5} \\
 & \mathbf{50} \\
 & \underline{.49} \\
 & 10 \\
 & \underline{7} \\
 & 30 \\
 & \underline{28} \\
 & 20 \\
 & \underline{14} \\
 & 60 \\
 & \underline{56} \\
 & 40 \\
 & \underline{35} \\
 & \mathbf{50}
\end{array}
$$

Next, we think about the second part of the statement: that if the decimal expansion repeats, then the number is rational.

Clearly, if the decimal expansion is terminating, then the number is rational. But what about the infinite, repeating, case? We've given two examples above. Let's consider these in more detail.

Example 8.2 Consider $a = 0.18\overline{3}$. Let $x = 0.00\overline{3}$. Then $10x = 0.0\overline{3}$ and so $10x - x = 0.0\overline{3} - 0.00\overline{3} = 0.03$. So, $9x = 0.03$ and hence $x = (3/100)/9 = 1/300$, so

$$0.18\overline{3} = 0.18 + 0.00\overline{3} = \frac{18}{100} + \frac{1}{300} = \frac{55}{300} = \frac{11}{60},$$

and this is the rational representation of a.

Example 8.3 Consider the number $0.1\overline{123}$. If $x = 0.0\overline{123}$, then $1000x = 12.3\overline{123}$ and $1000x - x = 12.3$. So $999x = 12.3$ and hence $x = 123/9990$. So,

$$0.1\overline{123} = \frac{1}{10} + x = \frac{1}{10} + \frac{123}{9990} = \frac{1122}{9990}.$$

In general, if the repeating block is of length k, then an argument just like the previous two, in which we multiply by 10^k, will enable us to express the number as a rational number.

8.3.4 Irrational numbers

A real number is *irrational* if it is not a rational number. So, given what we said above, an irrational number has no infinitely repeating pattern in its decimal expansion.

What's clear from above is that any real number can be approximated well by rational numbers: for the rational number $a_0.a_1a_2\ldots a_n$ is within $1/(10)^n$ of the real number with infinite decimal expansion $a_0.a_1a_2\ldots$.

We can, in some cases, prove that particular numbers are irrational. We already saw that $\sqrt{2}$ is irrational, and in general for any natural number n, either $\sqrt{n}$ is irrational or it is an integer (i.e. it is never a rational number which is not an integer).

Activity 8.3 Prove that if n is any natural number then either $\sqrt{n}$ is an integer or it is irrational.

Many other important numbers in mathematics turn out to be irrational. I've already mentioned π, and there is also e (the base of the natural logarithm). It's not easy to prove either of these numbers is irrational—in fact, it's quite hard to find examples of irrational numbers.

8.3.5 'Density' of the rational numbers

As we've seen, some important numbers in mathematics are not rational. An intuitive question that arises is 'how many real numbers are rational' and this is a difficult question to answer. There are infinitely many real numbers and infinitely many rationals, and infinitely may real numbers are not rational. More on this in the next section!

For the moment, let's make one important observation: not only are there infinitely many rational numbers, but there are no 'gaps' in the rational numbers. If you accept the view of real numbers as (possibly) infinite decimal expansions, then this is quite clear: you can get a very good approximation to any real number by terminating its decimal expansion after a large number of digits. (And we know that a terminating decimal expansion is a rational number.) The following theorem makes sense of the statement that there are no 'rational-free' zones in the real numbers. Precisely, between any two rational numbers, no matter how close together they are, there is always another rational number.

Theorem 8.2 Suppose $q, q' \in \mathbb{Q}$ with $q < q'$. Then there is $r \in \mathbb{Q}$ with $q < r < q'$.

Proof. Consider $r = (1/2)(q + q')$. Details are left to you! □

Activity 8.4 Complete this proof.

8.4 Countability of rationals and uncountability of real numbers

We know that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, and that each inclusion is strict (there are integers that are not natural numbers, rational numbers that are not integers, and real numbers that are not rational). All of these sets are infinite. But there is a sense in which the sets $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$ have the same 'size' and $\mathbb{R}$ is 'larger'. Clearly we have to define what this means in precise terms, because right now all we know is that there are more real numbers than rationals, for instance, but there are infinitely many of each type of number.

The following definition helps us.

Definition 8.1 (Countable sets) A set is *countable* if there is a bijection between the set and $\mathbb{N}$.

Note that in some textbooks this definition is called 'countably infinite'. These textbooks define 'countable' differently, asking only for an injective map from the set to $\mathbb{N}$. This really is different — there is an injective map from any finite set to $\mathbb{N}$ (more or less by definition). But any infinite set which has an injection to $\mathbb{N}$ is countable (by our definition; this needs a proof which I am skipping), so the difference is really only whether we call finite sets 'countable' or not. We are saying that 'countable' in particular means the set has to be infinite.

For instance, $\mathbb{Z}$ is countable: we can define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(1) = 0,\ f(2) = 1,\ f(3) = -1,\ f(4) = 2,\ f(5) = -2,\ f(6) = 3,\ f(7) = -3, \ldots.$$

(In general, $f(n) = (-1)^n \lfloor n/2 \rfloor$, where $\lfloor n/2 \rfloor$ means the largest integer that is no more than $n/2$.) It is straightforward to show that f is a bijection. Hence $\mathbb{Z}$ is countable. So, in this sense, the sets $\mathbb{Z}$ and $\mathbb{N}$ have the same 'cardinality' (even though $\mathbb{Z}$ is strictly larger than $\mathbb{N}$). Working with infinite sets is not the same as

working with finite sets: two finite sets, one of which was a strict subset of the other, could not have the same cardinality!

What does 'countable' mean? The formal definition is given above. But one way of thinking about it is that if S is countable, then the members of S can be *listed*:

$$s_1, s_2, s_3, \ldots, .$$

For, suppose S is countable. Then there is a bijection $f : \mathbb{N} \to S$. Let $s_i = f(i)$ for $i \in \mathbb{N}$. Then, because f is a bijection, the list $s_1, s_2, s_3, \ldots$ will include every element of S, each precisely once.

What is more surprising is that $\mathbb{Q}$ is also countable.

8.4.1 Countability of the rationals

Theorem 8.3 The set $\mathbb{Q}$ of rational numbers is countable.

How can we prove $\mathbb{Q}$ is countable?

By constructing a bijection $\mathbb{N} \to \mathbb{Q}$. We won't do so by means of a formula, but instead by thinking of a way in which all the rational numbers could be listed.

Arrange all the ordered pairs of natural numbers as follows:

$$\begin{array}{cccccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) & \cdots \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}$$

Traverse this array as indicated in the following diagrams, where traversed elements are emboldened and underlined as they are traversed.

$$\begin{array}{cccccccc}
\underline{(\mathbf{1},\mathbf{1})} & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) & \cdots \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}$$

$$\begin{array}{cccccccc}
\underline{(\mathbf{1},\mathbf{1})} & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}$$

$$
\begin{array}{ccccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & (1,3) & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
\underline{(\mathbf{3},\mathbf{1})} & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
\underline{(\mathbf{3},\mathbf{1})} & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
\underline{(\mathbf{4},\mathbf{1})} & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{cccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
\underline{(\mathbf{3},\mathbf{1})} & \underline{(\mathbf{3},\mathbf{2})} & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
\underline{(\mathbf{4},\mathbf{1})} & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}
$$

$$
\begin{array}{cccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & (1,4) & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & \underline{(\mathbf{2},\mathbf{3})} & (2,4) & (2,5) & (2,6) & \cdots \\
\underline{(\mathbf{3},\mathbf{1})} & \underline{(\mathbf{3},\mathbf{2})} & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
\underline{(\mathbf{4},\mathbf{1})} & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}
$$

$$
\begin{array}{cccccc}
\underline{(\mathbf{1},\mathbf{1})} & \underline{(\mathbf{1},\mathbf{2})} & \underline{(\mathbf{1},\mathbf{3})} & \underline{(\mathbf{1},\mathbf{4})} & (1,5) & (1,6) & \cdots \\
\underline{(\mathbf{2},\mathbf{1})} & \underline{(\mathbf{2},\mathbf{2})} & \underline{(\mathbf{2},\mathbf{3})} & (2,4) & (2,5) & (2,6) & \cdots \\
\underline{(\mathbf{3},\mathbf{1})} & \underline{(\mathbf{3},\mathbf{2})} & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
\underline{(\mathbf{4},\mathbf{1})} & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) & \cdots \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) & \cdots \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots
\end{array}
$$

We get a listing of all the ordered pairs of natural numbers:

$$(1,1),(2,1),(1,2),(1,3),(2,2),(3,1),(4,1),(3,2),(2,3),\ldots$$

From this we can get a listing of all positive rational numbers m/n: simply write down the corresponding rationals and ignore any (m,n) such that the rational m/n has already earlier appeared in the list:

$$(1,1),(2,1),(1,2),(1,3),(2,2),(3,1),(4,1),(3,2),(2,3),\ldots$$

gives

$$\frac{1}{1}',\frac{2}{1}',\frac{1}{2}',\frac{1}{3}',\frac{2}{2}',\frac{3}{1}',\frac{4}{1}',\frac{3}{2}',\frac{2}{3}',\frac{1}{4}',\frac{1}{5}',\frac{2}{4}',\frac{3}{3}',\frac{4}{2}',\frac{5}{1}',\frac{6}{1}',\cdots$$

which becomes

$$\frac{1}{1}',\frac{2}{1}',\frac{1}{2}',\frac{1}{3}',\quad\frac{3}{1}',\frac{4}{1}',\frac{3}{2}',\frac{2}{3}',\frac{1}{4}',\frac{1}{5}',\qquad\frac{5}{1}',\frac{6}{1}',\cdots$$

We can then include the negative rational numbers and 0 by starting with 0 and replacing m/n by m/n and $-m/n$:

$$0,\frac{1}{1}',-\frac{1}{1}',\frac{2}{1}',-\frac{2}{1}',\frac{1}{2}',-\frac{1}{2}',\frac{1}{3}',-\frac{1}{3}',\frac{3}{1}',-\frac{3}{1}',\frac{4}{1}',-\frac{4}{1}',\frac{3}{2}',-\frac{3}{2}',\frac{2}{3}',-\frac{2}{3}',$$
$$\frac{1}{4}',-\frac{1}{4}',\frac{1}{5}',-\frac{1}{5}',\frac{5}{1}',-\frac{5}{1}',\frac{6}{1}',-\frac{6}{1}',\cdots$$

It's clear that this listing describes a bijection from $\mathbb{N}$ to $\mathbb{Q}$. So this proves $\mathbb{Q}$ is countable.

We can go one step further in this direction. A number x is rational if and only if there is some equation $ax + b = 0$, with $a, b \in \mathbb{Z}$ not both zero, to which it is a solution. (Check that you agree this is obviously true!) This is a linear equation; what about polynomials?

Definition 8.2 A number x is *algebraic* if it is a solution to an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where n is a natural number and $a_0, a_1, \ldots, a_n$ are integers, not all zero.

The set of algebraic numbers is 'obviously much bigger' than the rationals; for example it contains $\sqrt{2}$. It turns out that e and π are not algebraic—but this is not easy to prove!

But in fact the algebraic numbers are also countable!

> **Activity 8.5** Find out how to modify the proof that the rational numbers are countable in order to show that the algebraic numbers are countable.

So, informally speaking, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and the algebraic numbers, all have the same 'size'. What about $\mathbb{R}$? Well, here it gets very interesting: the set of real numbers is *not* countable. (It is said to be *uncountable*.)

8

8.4.2 Uncountability of the real numbers

Theorem 8.4 The set $\mathbb{R}$ is not countable. (That is, $\mathbb{R}$ is uncountable.)

This theorem is really rather surprising: right now you know two examples of numbers which are real but not algebraic (namely π and e, although we didn't prove it). Of course you can generate more examples from this: 2π is also not algebraic (why?). Is $\pi + e$ algebraic? Probably not, but this is an open problem. But (it is easy to prove) in this way you'll only find a countable set of numbers which are not algebraic. What it means to say that $\mathbb{R}$ is not countable is that it is really much, much larger than the rationals, or the algebraic numbers. Even though you only have two explicit examples of real numbers which are not algebraic, once you know the algebraic numbers are countable but the real numbers are not, you know that 'most' real numbers are not algebraic!

The proof uses the famous 'Cantor diagonal' argument.

Suppose that $f : \mathbb{N} \to \mathbb{R}$ and that

$$f(n) = x_{n0}.x_{n1}x_{n2}x_{n3}\ldots.$$

We show there's a number in $\mathbb{R}$ which isn't the image under f of any element of $\mathbb{N}$ (and hence f is not a surjection). Consider

$$y = 0.y_1y_2y_3\ldots$$

where

$$y_i = \begin{cases} 1 & \text{if } x_{ii} \neq 1 \\ 2 & \text{if } x_{ii} = 1. \end{cases}$$

For all $n \in \mathbb{N}$, $y \neq f(n)$ since y_n is different from x_{nn}.

Since f was arbitrary, this shows that there can be no function $f : \mathbb{N} \to \mathbb{R}$ that is surjective. Hence $\mathbb{R}$ is not countable.

8.5 Complex numbers

8.5.1 Introduction

Consider the two quadratic polynomials,

$$p(x) = x^2 - 3x + 2 \qquad \text{and} \qquad q(x) = x^2 + x + 1$$

If you sketch the graph of $p(x)$ you will find that the graph intersects the x-axis at the two real solutions (or roots) of the equation $p(x) = 0$, and that the polynomial factors into the two linear factors,

$$p(x) = x^2 - 3x + 2 = (x - 1)(x - 2)$$

Sketching the graph of $q(x)$, you will find that it does not intersect the x-axis. The equation $q(x) = 0$ has no solution in the real numbers, and it cannot be factorised (or factored) over the reals. Such a polynomial is said to be *irreducible* over the reals. In order to solve this equation, we need to define the complex numbers.

8.5.2 Complex numbers: a formal approach

To start with, let's formally construct the complex numbers from the real numbers. This is where we can finally answer the question from Section 3.10 of what the difference between $\mathbb{C}$ (which makes sense) and $\mathbb{E}$ (which doesn't exist) is. The formal construction this time is rather similar to the usual way you think about the complex numbers (in contrast to the formal construction of $\mathbb{Z}$ we gave, which probably still looks a bit funny).

We define the set $\mathbb{C}$ of complex numbers to be the set of all ordered pairs (x, y) of real numbers, with addition and multiplication operations defined as follows:

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \times (c, d) = (ac - bd, ad + bc).$$

You should check that these definitions really work, that is, that (for example) the multiplication is commutative, and that the distributive law holds. More generally, you should check that $\mathbb{C}$ satisfies (F1)–(F6), i.e. it is a field: we can do all the algebra we're used to. (What $\mathbb{C}$ *doesn't* have is an order: there isn't any way of defining an order $<$ on $\mathbb{C}$ which plays nicely with addition and multiplication in the way that the order plays nicely in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.)

You can also check that the complex numbers of the form $(x, 0)$ behave like the real numbers, in other words that $(x, 0) + (y, 0) = (x + y, 0)$, and $(x, 0) \times (y, 0) = (xy, 0)$,

which is what you expect for adding and multiplying real numbers. Finally, let's remember why we began this: we wanted to be able to solve the equation $x^2 + 1 = 0$. Well, that means we want a complex number (a, b) such that $(a, b) \times (a, b) + (1, 0) = (0, 0)$. And we can find such a number: $(0, 1) \times (0, 1) = (-1, 0)$, so we are done.

This is where the construction story stops, for us. We have constructed a field $\mathbb{C}$ which contains the number line and in which we can solve $x^2 + 1 = 0$. Let's look back to Section 3.10 briefly. There, we asked whether one can have a number system $\mathbb{E}$ which satisfies (some of) the properties of a field and in which we can solve $x \times 0 = 1$. And we discovered that the answer is No. We proved that the answer is No, by doing a calculation using the properties of this supposed-to-exist $\mathbb{E}$, until we came to a logical contradiction: we calculated that $1 = 1 + 1$, but we also proved that $1 \neq 1 + 1$. And then came the question: why are the complex numbers different? Why is it OK to ask for a solution to $x^2 + 1 = 0$ but not to $x \times 0 = 1$? More concretely: we know that $\mathbb{E}$ doesn't make sense—it doesn't exist—but how do we know that if we do some calculation with the complex numbers using the normal rules of algebra—i.e. using the axioms of a field, ($\mathbb{F}$1)–($\mathbb{F}$6)—we will not wind up calculating something like that $1 = 1 + 1$?

Well, suppose we came upon such a horrible calculation which shows $1 = 1 + 1$ (i.e. which finds a logical contradiction assuming the complex numbers exist). Now, this calculation relies on the fact that $\mathbb{C}$ satisfies ($\mathbb{F}$1)–($\mathbb{F}$6). And we *proved* that $\mathbb{C}$ satisfies these, on the assumption that $\mathbb{R}$ satisfies them. (Well, actually, we didn't really do this proof; I simply told you to check it. But I assume you have done that by now.)

So we can rewrite our horrible calculation in terms of pairs of real numbers: and now we have a logical contradiction which follows from our assumption that $\mathbb{R}$ exists. But we constructed (OK, OK, we did not do that, but at least I promise we could do it..!) the real numbers $\mathbb{R}$ from $\mathbb{Q}$—and that means we can rewrite our horrible calculation in terms of the rationals $\mathbb{Q}$. Now we have a logical contradiction which follows from our assumption that $\mathbb{Q}$ exists.

But we constructed $\mathbb{Q}$ from $\mathbb{Z}$—and following that construction back we have a logical contradiction which follows from our assumption that $\mathbb{Z}$ exists. And finally we constructed $\mathbb{Z}$ from $\mathbb{N}$, so we can follow that construction back too—rewriting all the integers as equivalence classes of pairs of natural numbers—until finally our hypothetical horrible calculation in $\mathbb{C}$ has been translated into a logical contradiction in the natural numbers, using only the axioms of the natural numbers. And we said we believe the natural numbers really do exist, that there are no logical contradictions there.

Let's be clear—you would not want to ever actually rewrite a calculation like this. A complex number is a pair of real numbers, a real number is a set of rational numbers (a Dedekind cut), a rational number is an equivalence class of pairs of integers, and an integer is an equivalence class of pairs of natural numbers. So a complex number is

a pair of (sets of (equivalence classes of pairs of (equivalence classes of pairs of natural numbers)))

which is a pretty unpleasant thing to think about. But you don't actually have to rewrite a calculation. We *proved* each step works, and it follows logically that *if* there

is a logical contradiction which you can find by doing algebra with the complex numbers using axioms (ℍF1)–(ℍF6), *then* there is a logical contradiction which you can find in the natural numbers using the axioms of the natural numbers.[1]

Putting this more simply: if someone tells you they think the complex numbers don't make sense, you can now tell them that they logically also have to believe that counting apples doesn't work either.

Now, it is usual to say that the real numbers are contained in the complex numbers: $(a, 0)$ 'is' the real number a.

You should notice that (if you are trying to be very formal) the last statement isn't quite true. $(a, 0)$ is obviously not the same as the real number a. However, because the numbers $(a, 0)$ behave exactly like the real numbers, we will commit an abuse of notation and say that they are the same. So we will write $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, even though formally this is not really true. If you ask me what I really mean by $\mathbb{N} \subset \mathbb{C}$, I'll tell you that I want to refer to the set of complex numbers of the form $(a, 0)$ where a is a positive integer. And that set, together with addition and multiplication as defined on the complex numbers (and I should define an order $<$, which I can do in the obvious way) indeed satisfies the axioms for the natural numbers. So it might not formally be the set $\mathbb{N}$ which I started with, but it's essentially the same; there is a dictionary correspondence between them (as we proved in Section 3.9). The same is true for all the other inclusions.

At this point we are going to stop trying to be formally careful. We've *proved* that given $\mathbb{N}$ it makes sense to talk about $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, and we've seen why it makes sense to say that (for example) $\mathbb{Q}$ is contained in $\mathbb{C}$. For the rest of your degree course, you don't have to remember the details of these constructions: you know they work, and that's enough. **However**, you should not forget the ideas, in particular the idea of constructing new structures using equivalence relations and old structures. You'll see those ideas repeatedly, and next time they'll be used to construct something you are not so familiar with and have to work to understand.

8.5.3 Complex numbers: a more usual approach

Rather than the ordered pairs approach outlined above, it is more common to define the complex numbers as follows. We begin by defining the *imaginary* number i which has the property that $i^2 = -1$. The term 'imaginary' is historical, and not an indication that this is a figment of someone's imagination—but historically the reason for the name is that (before all these constructions were invented) some mathematicians didn't believe the complex numbers make sense: 'imaginary' is a term of Descartes, and he meant it as an attack on the idea.

This symbol i is simply a nicer way of writing the pair $(0, 1)$ of real numbers; it's easier to write on the board in calculations (in the same way that it's easier to write $\frac{a}{b}$ for the rational rather than the equivalence class $[(a, b)]_R$ of the relation R we defined in Section 8.2.1). We can then say what we mean by the complex numbers.

[1] I'm cheating here—we also used sets, and we didn't justify that these sets make sense. But at least according to the ZFC axioms, they do—in any case, we get back from a contradiction in the complex numbers to a contradiction in something fundamental: natural numbers and sets.

Definition 8.3 A complex number is a number of the form $z = a + ib$, where a and b are real numbers, and $i^2 = -1$. The set of all such numbers is

$$\mathbb{C} = \{a + ib \ : \ a, b \in \mathbb{R}\} .$$

If $z = a + ib$ is a complex number, then the real number a is known as the real part of z, denoted $\mathsf{Re}(z)$, and the real number b is the imaginary part of z, denoted $\mathsf{Im}(z)$. Note that $\mathsf{Im}(z)$ is a *real* number.

If $b = 0$, then z is a real number, so $\mathbb{R} \subseteq \mathbb{C}$. If $a = 0$, then z is said to be *purely imaginary*.

The quadratic polynomial $q(z) = x^2 + x + 1$ can be factorised over the complex numbers, because the equation $q(z) = 0$ has two complex solutions. Solving in the usual way, we have

$$x = \frac{-1 \pm \sqrt{-3}}{2}.$$

We write, $\sqrt{-3} = \sqrt{(-1)3} = \sqrt{-1}\,\sqrt{3} = i\sqrt{3}$, so that the solutions are

$$w = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad \text{and} \qquad \overline{w} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Notice the form of these two solutions. They are what is called a *conjugate pair*. We have the following definition.

Definition 8.4 If $z = a + ib$ is a complex number, then the *complex conjugate* of z is the complex number $\overline{z} = a - ib$.

We can see by the application of the quadratic formula, that the roots of an irreducible quadratic polynomial with real coefficients will always be a conjugate pair of complex numbers.

Addition, multiplication, division

Addition and *multiplication* of complex numbers are defined as for polynomials in i using $i^2 = -1$.

> **Example 8.4** If $z = (1 + i)$ and $w = (4 - 2i)$ then
>
> $$z + w = (1 + i) + (4 - 2i) = (1 + 4) + i(1 - 2) = 5 - i$$
>
> and
>
> $$zw = (1 + i)(4 - 2i) = 4 + 4i - 2i - 2i^2 = 6 + 2i$$

You should check that this is really exactly the same as the definitions we gave when we formally constructed the complex numbers: the only difference is the way we're writing complex numbers.

If $z \in \mathbb{C}$, then $z\overline{z}$ is a real number:

$$z\overline{z} = (a + ib)(a - ib) = a^2 + b^2.$$

Activity 8.6 Carry out the multiplication to verify this: let $z = a + ib$ and calculate $z\overline{z}$.

Division of complex numbers is then defined by $\dfrac{z}{w} = \dfrac{z\overline{w}}{w\overline{w}}$ since $w\overline{w}$ is real.

Example 8.5

$$\frac{1+i}{4-2i} = \frac{(1+i)(4+2i)}{(4-2i)(4+2i)} = \frac{2+6i}{16+4} = \frac{1}{10} + \frac{3}{10}i$$

Properties of the complex conjugate

A complex number is real if and only if $z = \overline{z}$. Indeed, if $z = a + ib$, then $z = \overline{z}$ if and only if $b = 0$.

The complex conjugate of a complex number satisfies the following properties:

- $z + \overline{z} = 2\,\mathrm{Re}(z)$ is real
- $z - \overline{z} = 2i\,\mathrm{Im}(z)$ is purely imaginary
- $\overline{\overline{z}} = z$
- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{zw} = \overline{z}\,\overline{w}$
- $\overline{\left(\dfrac{z}{w}\right)} = \dfrac{\overline{z}}{\overline{w}}$

Activity 8.7 Let $z = a + ib$, $w = c + id$ and verify all of the above properties.

8.5.4 Roots of polynomials

Are we really done with construction? We invented the symbol i because we wanted to have a solution to $x^2 + 1 = 0$. But I also want a solution to $x^6 + 10x^2 + 17 = 0$. Do I need a new symbol for that? It turns out the answer is No.

The *Fundamental Theorem of Algebra* asserts that a polynomial of degree n with complex coefficients has n complex roots (not necessarily distinct), and can therefore be factorised into n linear factors. Explicitly, any equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0$$

where $a_i \in \mathbb{C}$ has n solutions $z \in \mathbb{C}$. Contrast this with the difficulty of solving polynomial equations in $\mathbb{R}$. So, the introduction of i enables us to solve **all** polynomial equations: there's no need to introduce anything else. A fancy way of saying this is: 'The field of complex numbers is algebraically closed.'

If the coefficients of the polynomial are restricted to real numbers, the polynomial can be factorised into a product of linear and irreducible quadratic factors over $\mathbb{R}$ and

into a product of *linear* factors over $\mathbb{C}$. The proof of the *Fundamental Theorem of Algebra* is beyond the scope of this course (and this time not because it's long and boring, but because it is genuinely quite hard). However, we note the following useful result.

Theorem 8.5 Complex roots of polynomials with real coefficients appear in conjugate pairs.

Proof. Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{R}$, be a polynomial of degree n. We shall show that if z is a root of $P(x)$, then so is $\overline{z}$.

Let z be a complex number such that $P(z) = 0$, then

$$a_0 + a_1z + +a_2z^2 \cdots + a_nz^n = 0$$

Conjugating both sides of this equation,

$$\overline{a_0 + a_1z + a_2z^2 + \cdots + a_nz^n} = \overline{0} = 0$$

Since 0 is a real number, it is equal to its complex conjugate. We now use the properties of the complex conjugate: that the complex conjugate of the sum is the sum of the conjugates, and the same is true for the product of complex numbers. We have

$$\overline{a_0} + \overline{a_1z} + \overline{a_2z^2} + \cdots + \overline{a_nz^n} = 0,$$

and

$$\overline{a}_0 + \overline{a}_1\overline{z} + \overline{a}_2\overline{z}^2 + \cdots + \overline{a}_n\overline{z}^n = 0.$$

Since the coefficients a_i are real numbers, this becomes

$$a_0 + a_1\overline{z} + a_2\overline{z}^2 + \cdots + a_n\overline{z}^n = 0.$$

That is, $P(\overline{z}) = 0$, so the number $\overline{z}$ is also a root of $P(x)$. □

Example 8.6 Let us consider the polynomial

$$x^3 - 2x^2 - 2x - 3 = (x - 3)(x^2 + x + 1).$$

If $w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, then

$$x^3 - 2x^2 - 2x - 3 = (x - 3)(x - w)(x - \overline{w})$$

Activity 8.8 Multiply out the last two factors above to check that their product is the irreducible quadratic $x^2 + x + 1$.

8.5.5 The complex plane

The following theorem shows that a complex number is uniquely determined by its real and imaginary parts.

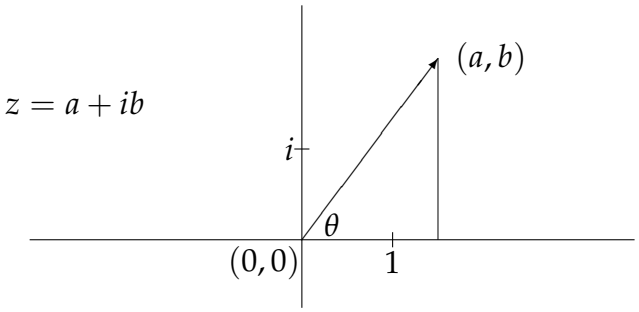
Theorem 8.6 Two complex numbers are equal if and only if their real and imaginary parts are equal.

There are two ways to prove this. We can do it directly, using the fact that the complex numbers are a field:

Proof. Two complex numbers with the same real parts and the same imaginary parts are clearly the same complex number, so we only need to prove this statement in one direction. Let $z = a + ib$ and $w = c + id$. If $z = w$, we will show that their real and imaginary parts are equal. We have $a + ib = c + id$, therefore $a - c = i(d - b)$. Squaring both sides, we obtain $(a - c)^2 = i^2(d - b)^2 = -(d - b)^2$. But $a - c$ and $(d - b)$ are real numbers, so their squares are non-negative. The only way this equality can hold is for $a - c = d - b = 0$. That is, $a = c$ and $b = d$. □

The other, much shorter (by now!) way to prove this is simply to observe that the complex numbers are the same as pairs of real numbers (with addition and multiplication as we defined them when we formally constructed the complex numbers) and pairs of real numbers are by definition equal if and only if both parts—which are precisely the real and imaginary parts—are equal.

As a result of this theorem, we can think of the complex numbers geometrically, as points in a plane. For, we can associate the vector $(a,\ b)^T$ uniquely to each complex number $z = a + ib$, and all the properties of a two-dimensional real vector space apply. A complex number $z = a + ib$ is represented as a point (a, b) in the complex plane; we draw two axes, a horizontal axis to represent the real parts of complex numbers, and a vertical axis to represent the imaginary parts of complex numbers. Points on the horizontal axis represent real numbers, and points on the vertical axis represent purely imaginary numbers.



Complex plane or Argand diagram

Activity 8.9 Plot $z = 2 + 2i$ and $w = 1 - i\sqrt{3}$ in the complex plane.

8.5.6 Polar form of z

If the complex number $z = a + ib$ is plotted as a point (a, b) in the complex plane, then we can determine the polar coordinates of this point. We have

$$a = r\cos\theta, \quad b = r\sin\theta$$

where $r = \sqrt{a^2 + b^2}$ is the length of the line joining the origin to the point (a, b) and θ is the angle measured anticlockwise from the real (horizontal) axis to the line joining the origin to the point (a, b). Then we can write $z = a + ib = r\cos\theta + i\,r\sin\theta$.

Definition 8.5 The *polar form* of the complex number z is

$$z = r(\cos\theta + i\sin\theta).$$

The length $r = \sqrt{a^2 + b^2}$ is called the *modulus* of z, denoted $|z|$, and the angle θ is called the *argument* of z.

Note the following properties:

- z and $\bar{z}$ are reflections in the real axis. If θ is the argument of z, then $-\theta$ is the argument of $\bar{z}$.
- $|z|^2 = z\bar{z}$.
- θ and $\theta + 2n\pi$ give the same complex number.

We define the *principal argument* of z to be the argument in the range, $-\pi < \theta \leq \pi$.

> **Activity 8.10** Express $z = 2 + 2i$, $w = 1 - i\sqrt{3}$ in polar form.
> Describe the following sets of z: (a) $|z| = 3$, (b) argument of z is $\frac{\pi}{4}$.

Multiplication and division using polar coordinates gives

$$\begin{aligned} zw &= r(\cos\theta + i\sin\theta)\cdot\rho(\cos\phi + i\sin\phi) \\ &= r\rho(\cos(\theta+\phi) + i\sin(\theta+\phi)) \end{aligned}$$

$$\frac{z}{w} = \frac{r}{\rho}\big(\cos(\theta-\phi) + i\sin(\theta-\phi)\big)$$

> **Activity 8.11** Show these by performing the multiplication and the division as defined earlier, and by using the facts that $\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$ and $\sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi$.

DeMoivre's Theorem

We can consider explictly a special case of the multiplication result above, in which $w = z$. If we apply the multiplication to $z^2 = zz$, we have

$$\begin{aligned} z^2 &= zz \\ &= (r(\cos\theta + i\sin\theta))(r(\cos\theta + i\sin\theta)) \\ &= r^2(\cos^2\theta + i^2\sin^2\theta + 2i\sin\theta\cos\theta) \\ &= r^2(\cos^2\theta - \sin^2\theta + 2i\sin\theta\cos\theta) \\ &= r^2(\cos 2\theta + i\sin 2\theta). \end{aligned}$$

Here we have used the double angle formulae for $\cos 2\theta$ and $\sin 2\theta$.

Applying the product rule n times, where n is a positive integer, we obtain *DeMoivre's Formula*

Theorem 8.7

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Proof.

$$\begin{aligned} z^n &= \underbrace{z\cdots z}_{n \text{ times}} = \big(r(\cos\theta + i\sin\theta)\big)^n \\ &= r^n\Big(\cos(\underbrace{\theta+\cdots+\theta}_{n \text{ times}}) + i\sin(\underbrace{\theta+\cdots+\theta}_{n \text{ times}})\Big) \end{aligned}$$

□

8.5.7 Exponential form of z

Functions of complex numbers can be defined by the power series (Taylor expansions) of the functions:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots \qquad z \in \mathbb{C}$$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots \qquad \cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \cdots$$

If we use the expansion for e^z to expand $e^{i\theta}$, and then factor out the real and imaginary parts, we find:

$$\begin{aligned} e^{i\theta} &= 1 + (i\theta) + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \cdots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \cdots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots\right) + i\left(\theta - \frac{\theta^3}{3} + \frac{\theta^5}{5!} - \cdots\right) \end{aligned}$$

From which we conclude:

Euler's Formula: $\boxed{e^{i\theta} = \cos\theta + i\sin\theta}$

If you're being careful, you might notice something a bit strange here—what exactly do I mean by these funny infinite sums? and why am I allowed to rearrange the terms in them? Sure, I know addition is commutative, but that will only let me change places of *finitely* many terms in the sum (which I don't quite understand anyway), and I still have infinitely many more thing which I need to change places. The answer to *that* objection is: we'll explain properly some of it next term, and some next year in MA203 Real Analysis. For now, take it on faith that it does actually make sense.

Definition 8.6 The *exponential form* of a complex number $z = a + ib$ is

$$z = re^{i\theta}$$

where $r = |z|$ is the modulus of z and θ is the argument of z.

In particular, the following equality is of note because it combines the numbers e, π and i in a single expression: $e^{i\pi} = -1$.

If $z = re^{i\theta}$, then its complex conjugate is given by $\overline{z} = re^{-i\theta}$. This is because, if $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$, then

$$\overline{z} = r(\cos\theta - i\sin\theta) = r(\cos(-\theta) + i\sin(-\theta)) = re^{-i\theta}.$$

We can use either the exponential form, $z = re^{i\theta}$, or the standard form, $z = a + ib$, according to the application or computation we are doing. For example, addition is simplest in the form $z = a + ib$, but multiplication and division are simpler in exponential form. To change a complex number between $re^{i\theta}$ and $a + ib$, use Euler's formula and the complex plane (polar form).

Example 8.7

$$e^{i\frac{2\pi}{3}} = \cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3} = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}.$$

$$e^{2+i\sqrt{3}} = e^2e^{i\sqrt{3}} = e^2\cos\sqrt{3} + ie^2\sin\sqrt{3}.$$

8

Activity 8.12 Write each of the following complex numbers in the form $a + ib$:

$$e^{i\frac{\pi}{2}} \qquad e^{i\frac{3\pi}{2}} \qquad e^{i\frac{3\pi}{4}} \qquad e^{i\frac{11\pi}{3}} \qquad e^{1+i} \qquad e^{-1}$$

Example 8.8 Let $z = 2 + 2i = 2\sqrt{2}\,e^{i\frac{\pi}{4}}$ and $w = 1 - i\sqrt{3} = 2e^{-i\frac{\pi}{3}}$, then

$$w^6 = (1 - i\sqrt{3})^6 = (2e^{-i\frac{\pi}{3}})^6 = 2^6e^{-i2\pi} = 64$$

$$zw = (2\sqrt{2}e^{i\frac{\pi}{4}})(2e^{-i\frac{\pi}{3}}) = 4\sqrt{2}e^{-i\frac{\pi}{12}}$$

and

$$\frac{z}{w} = \sqrt{2}e^{i\frac{7\pi}{12}}.$$

Notice that in the above example we are using certain properties of the complex exponential function, that if $z, w \in \mathbb{C}$,

$$e^{z+w} = e^ze^w \qquad \text{and} \qquad (e^z)^n = e^{nz} \quad \text{for } n \in \mathbb{Z}.$$

This last property is easily generalised to include the negative integers.

Example 8.9 Solve the equation $z^6 = -1$ to find the 6th roots of -1.

Write $z^6 = (re^{i\theta})^6 = r^6 e^{i6\theta}$, $\quad -1 = e^{i\pi} = e^{i(\pi+2n\pi)}$

Equating these two expressions, and using the fact that r is a real positive number, we have

$$r = 1 \qquad 6\theta = \pi + 2n\pi, \quad \theta = \frac{\pi}{6} + \frac{2n\pi}{6}$$

This will give the six complex roots by taking $n = 0, 1, 2, 3, 4, 5$.

Activity 8.13 Show this. Write down the six roots of -1 and show that any one raised to the power 6 is equal to -1. Show that $n = 6$ gives the same root as $n = 0$.

Use this to factor the polynomial $x^6 + 1$ into linear factors over the complex numbers and into irreducible quadratics over the real numbers.

8.6 Learning outcomes

At the end of this chapter and the relevant reading, you should be able to:

- demonstrate that you understand how the rational numbers can be formally constructed by means of an equivalence relation and that addition and multiplication of rational numbers can be defined as operations on the equivalence classes
- indicate that you know that a real number is rational if and only if it has an infinitely repeating pattern in its decimal expansion
- find the decimal expansion of a rational number
- determine, in the form m/n, a rational number from its decimal expansion
- prove that certain numbers are rational or irrational
- demonstrate that you understand that there are rational numbers arbitrarily close to any real number
- state what it means to say that a set is countable or uncountable
- demonstrate that you know that the rationals are countable and the reals uncountable
- show that you know what is meant by complex numbers, and demonstrate that you can add, subtract, multiply and divide complex numbers
- state the definition of the complex conjugate of a complex number
- show that you know that every polynomial of degree n has n complex roots and that these occur in conjugate pairs
- indicate complex numbers on the complex plane

- determine the polar and exponential form of complex numbers
- state and use DeMoivre's theorem and Euler's formula

8.7 Sample exercises

Exercise 8.1
Prove that $\sqrt{5}$ is irrational.

Exercise 8.2
Express the complex number $\dfrac{1+2i}{4-5i}$ in the form $a+bi$.

Exercise 8.3
Solve the equation $x^2 - 2ix + 3 = 0$.

Exercise 8.4
Write each of the following complex numbers in the form $a+ib$:

$$e^{i\frac{\pi}{2}} \qquad e^{i\frac{3\pi}{2}} \qquad e^{i\frac{3\pi}{4}} \qquad e^{i\frac{11\pi}{3}} \qquad e^{1+i} \qquad e^{-1}.$$

Exercise 8.5
Express $1+\sqrt{3}i$ in exponential form. Hence find $(1+\sqrt{3}i)^{30}$.

8

8.8 Comments on selected activities

Learning activity 8.1 Suppose that

$$\frac{a}{b} = \frac{a'}{b'} \text{ and } \frac{c}{d} = \frac{c'}{d'}.$$

What we need to check is that

$$\frac{a}{b} \times \frac{c}{d} = \frac{a'}{b'} \times \frac{c'}{d'}.$$

Now, the fact that $\dfrac{a}{b} = \dfrac{a'}{b'}$ means precisely that $[(a,b)] = [(a',b')]$, which means that $ab' = a'b$. Similarly, we have $cd' = c'd$. Now,

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}, \text{ and } \frac{a'}{b'} \times \frac{c'}{d'} = \frac{a'c'}{b'd'}$$

and so we need to prove that

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

This means we need to prove that

$$[(ac,bd)]\, R\, [(a'c',b'd')].$$

Now,

$$\begin{aligned}[(ac, bd)]\, R\, [(a'c', b'd')] &\iff acb'd' = a'c'bd \\ &\iff (ab')(cd') = (a'b)(c'd),\end{aligned}$$

which is true because $ab' = a'b$ and $cd' = c'd$.

Learning activity 8.3 The obvious thing to do is to try mimicking the proof that $\sqrt{2}$ is irrational. So let's try. Suppose for a contradiction that there are integers a and b such that $\left(\frac{a}{b}\right)^2 = n$. As before, we can assume $\gcd(a, b) = 1$. We get

$$a^2 = nb^2$$

and it follows that a^2 is divisible by n. But it *doesn't* follow that a is divisible by n, in general (It is true, by Theorem 6.7, if n is prime; but for example $6^2 = 36$ is divisible by 18, but 6 is certainly not divisible by 18). In order to get further, it helps to think about the prime factorisation of n.

Learning activity 8.5 This isn't easy. Maybe the best way to do the problem is to make it more abstract, and split it up into a bunch of building-blocks. Here is one way.

Fact 1: Suppose S and T are countable sets. Then the product $S \times T$ is countable.

We saw how to prove this for the example $S = T = \mathbb{N}$. To do general S and T, imagine writing out the same table, but instead of writing (for instance) $(1, 2)$ write (s_1, t_2) where s_1 is the first element of S and t_2 is the second element of T (in both cases, according to the bijections which show S and T are countable).

Fact 2: Suppose S_i is a countable set for each $i \in \mathbb{N}$. Then the union $S_1 \cup S_2 \cup \ldots$ is countable.

This is basically the same idea. Write out the same table, but replace for instance $(5, 7)$ with the 5th element of S_7; in general, replace (a, b) with the ath element of S_b.

Now we can do the proof. We need one more fact: an equation $a_n x^n + \cdots + a_1 x + a_0 = 0$, where not all the a_i are zero, has at most n different solutions. Think about why this is!

There are countably many equations $a_1 x + a_0 = 0$ (because $\mathbb{Z}^2$ is countable, by Fact 1). Each has (at most) one solution (a rational number x). So (by counting through such equations and skipping over rational numbers we counted earlier) we see (again) that the rational numbers are countable.

There are countably many equations $a_2 x^2 + a_1 x + a_0 = 0$ (because $\mathbb{Z}^3$ is countable, by Fact 1). Each has at most two solutions. So (by counting through such equations, and for each equation its at most two solutions, and skipping over solutions we counted earlier) we see that there are countably many numbers which are solutions to some equation $a_2 x^2 + a_1 x + a_0 = 0$ where the a_i are integers, not all zero.

And we can repeat this argument: for each n there are countably many numbers which are solutions to some equation $a_n x^n + \cdots + a_1 x + a_0 = 0$ where the a_i are integers and not all zero.

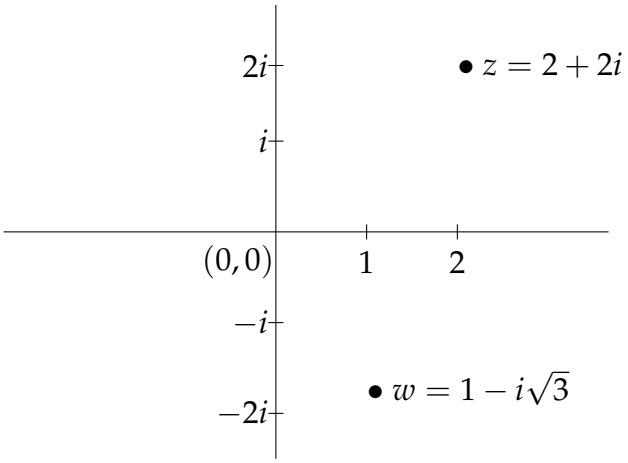
And finally, by Fact 2, the union of all these sets of solutions is also countable—and that union is by definition all the algebraic numbers.

Learning activity 8.8 We have

$$(x-w)(x-\overline{w}) = x^2 - (w+\overline{w})x + w\overline{w}.$$

Now, $w+\overline{w} = 2\,\mathrm{Re}(w) = 2(-\frac{1}{2})$ and $w\overline{w} = \frac{1}{4}+\frac{3}{4}$ so the product of the last two factors is x^2+x+1.

Learning activity 8.9



Learning activity 8.10 Draw the line from the origin to the point z in the diagram above. Do the same for w. For z, $|z| = 2\sqrt{2}$ and $\theta = \frac{\pi}{4}$, so $z = 2\sqrt{2}\big(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})\big)$. The modulus of w is $|w| = 2$ and the argument is $-\frac{\pi}{3}$, so that

$$w = 2\big(\cos(-\frac{\pi}{3}) + i\sin(-\frac{\pi}{3})\big) = 2\big(\cos(\frac{\pi}{3}) - i\sin(\frac{\pi}{3})\big).$$

The set (a) $|z| = 3$, is the circle of radius 3 centered at the origin. The set (b), argument of z is $\frac{\pi}{4}$, is the half line from the origin through the point (1,1).

Learning activity 8.13 The roots are:

$$z_1 = 1\cdot e^{i\frac{\pi}{6}}, \qquad z_2 = 1\cdot e^{i\frac{3\pi}{6}}, \qquad z_3 = 1\cdot e^{i\frac{5\pi}{6}},$$

$$z_4 = 1\cdot e^{i\frac{7\pi}{6}}, \qquad z_5 = 1\cdot e^{i\frac{9\pi}{6}}, \qquad z_6 = 1\cdot e^{i\frac{11\pi}{6}}.$$

These roots are in conjugate pairs, and $e^{i\frac{13\pi}{6}} = e^{i\frac{\pi}{6}}$:

$$z_4 = \overline{z}_3 = e^{-i\frac{5\pi}{6}}, \qquad z_5 = \overline{z}_2 = e^{-i\frac{\pi}{2}}, \qquad z_6 = \overline{z}_1 = e^{-i\frac{\pi}{6}}.$$

The polynomial factors as

$$x^6+1 = (x-z_1)(x-\overline{z}_1)(x-z_2)(x-\overline{z}_2)(x-z_3)(x-\overline{z}_3),$$

Using the $a+ib$ form of each complex number, for example, $z_1 = \frac{\sqrt{3}}{2} + i\frac{1}{2}$, you can carry out the multiplication of the linear terms pairwise (conjugate pairs) to obtain x^6+1 as a product of irreducible quadratics with real coefficients:

$$x^6+1 = (x^2-\sqrt{3}\,x+1)(x^2+\sqrt{3}\,x+1)(x^2+1).$$

8.9 Solutions to exercises

Solution to exercise 8.1

Suppose we have $\sqrt{5} = m/n$ where $m, n \in \mathbb{Z}$. Since $\sqrt{5} > 0$, we may assume that $m, n > 0$. (Otherwise, both are negative, and we can multiply each by -1.) We can also suppose that m, n have greatest common divisor 1. (For, we can cancel any common factors.) Then $(m/n)^2 = 5$ means that $m^2 = 5n^2$. So $5 \,|\, m^2$. Now m can, by the Fundamental Theorem of Arithmetic, be written as a product of primes $m = p_1 p_2 \dots p_k$. Then $m^2 = p_1^2 p_2^2 \dots p_k^2$. If no p_i is 5, then 5 does not appear as a factor in m^2 and so 5 does not divide m^2. So some p_i is equal to 5. So $5 \,|\, m$. Now, this means that $m = 5r$ for some $r \in \mathbb{N}$ and hence $m^2 = (5r)^2 = 25r^2$ and so $25r^2 = 5n^2$. Then, $n^2 = 5r^2$, so $5 \,|\, n^2$. Arguing as before, $5 \,|\, n$. So 5 is a common factor if m and n, which contradicts $\gcd(m, n) = 1$. Hence $\sqrt{5}$ is not rational.

Solution to exercise 8.2

We have

$$\begin{aligned}
\frac{1+2i}{4-5i} &= \frac{1+2i}{4-5i}\frac{4+5i}{4+5i} \\
&= \frac{(1+2i)(4+5i)}{(4-5i)(4+5i)} \\
&= \frac{4+8i+5i+10i^2}{16-25i^2} \\
&= \frac{-6+13i}{41} \\
&= -\frac{6}{41} + \frac{13}{41}i.
\end{aligned}$$

You can *check* that this is the correct answer by calculating the product

$$\left(-\frac{6}{41} + \frac{13}{41}i\right)(4-5i)$$

and observing that the answer is $1+2i$. □

Solution to exercise 8.3

To solve the equation $x^2 - 2ix + 3 = 0$, we could use the formula for the solutions of a quadratic equation. Or we could note that the equation is equivalent to $(x-i)^2 = -4$, so the solutions are given by $x - i = 2i$ and $x - i = -2i$, so they are $x = 3i$ and $x = -i$.

Solution to exercise 8.4

We have

$$e^{i\pi/2} = i, \qquad e^{i3\pi/2} = -i, \qquad e^{i3\pi/4} = -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}},$$

$$e^{i(11\pi/3)} = e^{-i(\pi/3)} = \frac{1}{2} - i\frac{\sqrt{3}}{2}, \qquad e^{1+i} = e^1 e^i = e\cos(1) + i\,e\sin(1),$$

$$e^{-1} = e^{-1} + 0i \text{ is real, so already in the form } a + ib.$$

Solution to exercise 8.5
To express $z = 1 + \sqrt{3}i$ in exponential form, we first note that

$$1 + \sqrt{3}i = 2\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$$

and this is $r(\cos\theta + i\sin\theta)$ when $r = 2, \theta = \pi/3$. So $z = 2e^{\pi i/3}$. Then,

$$(1 + \sqrt{3}i)^{30} = z^{30} = \left(2e^{\pi i/3}\right)^{30} = 2^{30}e^{30\pi i/3} = 2^{30}e^{10\pi i} = 2^{30}.$$