3 The language of proof

After working through this section, you should be able to:

(a) understand what is asserted by various types of mathematical statements, in particular *implications* and *equivalences*;

(b) produce simple proofs of various types, including *direct proof*, *proof by induction*, *proof by contradiction* and *proof by contraposition*;

(c) read and understand the logic of more complex proofs;

(d) disprove a simple false implication by providing a *counter-example*.

You will have seen many examples of mathematical statements, theorems and proofs during your study of mathematics. In this section we examine these concepts more closely. This should help you to become more adept at reading and understanding mathematics, and should make you more familiar with the structures of various different types of mathematical proof. It should also help you to express your own mathematical thoughts and ideas more clearly.

3.1 Statements and negations

The building blocks of mathematical theorems and proofs are assertions called **statements**, also known as *propositions*. In mathematics, a statement is an assertion that is either true or false, though we may not know which. The following are examples of statements.

1. The equation $2x - 3 = 0$ has solution $x = \frac{3}{2}$.
2. $1 + 1 = 3$.
3. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for each positive integer n.
4. There is a real number x such that $\cos x = x$.
5. Every even integer greater than 2 is the sum of two prime numbers.
6. x is greater than 0.

In the above list, Statement 1 is true, and Statement 2 is false. Statements 3 and 4 are in fact both true, although this is probably not immediately obvious to you in either case. At the time of writing this unit, it is not known whether Statement 5 is true or false.

We shall prove that Statement 3 is true later in this section. You can check that Statement 4 is true by noting that the graphs of $y = \cos x$ and $y = x$ intersect; a rigorous proof can be obtained by using the *Intermediate Value Theorem*, which is given later in the course. Statement 5 is known as *Goldbach's conjecture*; mathematicians have been trying to prove it since 1742.

Statement 6 is a little different from the others, since whether it is true or false depends on the value of the variable x. A statement, such as this one, that is either true or false depending on the value of one or more variables, is called a *variable proposition*. When considering a variable proposition, we must have in mind a suitable set of values from which the possible values of the variable are taken. For example, the set associated with Statement 6 might be $\mathbb{R}$, since for each real number x the assertion is either true or false. A variable proposition with several variables may have several such associated sets.

Often the set or sets associated with a variable are clear from the context and so we do not state them explicitly. In particular, unless it is stated otherwise, it is conventional to assume that if the variable is x or y, then the associated set is $\mathbb{R}$, whereas if the variable is n or m, then the associated set is is $\mathbb{Z}$ or $\mathbb{N}$, depending on the context. We follow this convention in this section.

An example of an assertion that is not a mathematical statement is '$\{1, 2\}$ is greater than 0', which is meaningless and therefore neither true nor false. Other examples are 'π is interesting' and '1000 is a large number', which are not precise enough to be either true or false.

Statements can be combined in various ways to give more complicated statements. For example, the statement

x is greater than 0 and x is an integer

is true if *both* of the statements 'x is greater than 0' and 'x is an integer' are true, and false otherwise. Thus the combined statement is true if $x = 4$, for example, but false if $x = 3.5$. Similarly, the statement

x is greater than 0 or x is an integer

is true if *at least one* of the statements 'x is greater than 0' and 'x is an integer' is true, and false otherwise. Thus this combined statement is true if $x = 4$, $x = 3.5$ or $x = -4$, for example, but false if $x = -3.5$.

The word 'or' is used in its inclusive sense in mathematical statements.

Every statement has a related statement, called its **negation**, which is true when the original statement is false, and false when the original statement is true. The negation of a statement P can usually be written as 'it is not the case that P', but there are often better, more concise ways to express it. Thus, for example, the negation of the statement 'x is greater than 0' can be written as 'it is not the case that x is greater than 0', but is

better expressed as 'x is not greater than 0' or even '$x \leq 0$'. The process of finding the negation of a statement is called *negating* the statement. Here are some more examples.

Example 3.1 Express concisely the negation of each of the following statements.

(a) There is a real number x such that $\cos x = x$.

(b) Both x and y are integers.

Solution

(a) The negation is 'it is not the case that there is an real number x such that $\cos x = x$'; that is, 'there is no real number x such that $\cos x = x$'.

Another way of expressing this negation is 'for all real numbers x, $\cos x \neq x$'.

(b) The negation is 'it is not the case that both x and y are integers'; that is, 'at least one of x and y is not an integer'. ■

Exercise 3.1 Express concisely the negation of each of the following statements.

(a) $x = \frac{3}{5}$ is a solution of the equation $3x + 5 = 0$.

(b) π is less than 5.

(c) There is an integer that is divisible by 3 but not by 6.

(d) Every real number x satisfies the inequality $x^2 \geq 0$.

(e) The integers m and n are both odd.

(f) At least one of the integers m and n is odd.

A **theorem** is simply a mathematical statement that is true. However, we usually reserve the word for a statement that is considered to be of some importance, and whose truth is not immediately obvious, but instead has to be proved. A **lemma** is a 'less important' theorem that is useful when proving other theorems. A **corollary** is a theorem that follows from another theorem by a short additional argument. Theorems are sometimes called *results*.

3.2 Implications and equivalences

Many mathematical statements are of the form 'if something, then something else', for example:

if $x > 2$, then $x^2 > 4$.

This type of statement is called an **implication**. An implication is made up from two smaller statements, which in the example above are '$x > 2$' and '$x^2 > 4$', and can be expressed by combining these statements using the words 'if' and 'then'. In an implication 'if P, then Q', the statement P is called the **hypothesis** of the implication, and the statement Q is called the **conclusion**. It is important to be clear about exactly what an implication asserts. The above statement asserts only that if you know that $x > 2$, then you can be sure that $x^2 > 4$. It does not assert anything about the truth or falsity of '$x^2 > 4$' when x is not greater than 2. In general, the implication 'if P, then Q' asserts that if P is true, then Q is also true; it does not assert anything about the truth or falsity of Q when P is false.

If the hypothesis P of an implication consists of several smaller statements, combined using 'and'—for example, the implication might be expressed in the form 'if P_1, P_2 and P_3, then Q'—then it is common to consider each of the smaller statements as a separate hypothesis, and to say that the implication has several *hypotheses*. Similarly, an implication can have several conclusions.

If x is a real variable, then the statement

if $x > 2$, then $x^2 > 4$

is true because for every real number x for which '$x > 2$' is true, '$x^2 > 4$' is true also. Strictly speaking, this statement should be expressed as

for all $x \in \mathbb{R}$, if $x > 2$, then $x^2 > 4$.

However, it is conventional to omit the initial 'for all $x \in \mathbb{R}$', and interpret the statement as if it were there. In general, throughout this course, and throughout almost any mathematical text that you will read, a statement of the form 'if P, then Q' in which P and/or Q are variable propositions is similarly interpreted as applying to all values of the variables in the statements P and Q.

An implication does not have to be expressed using the words 'if' and 'then'—there are many other ways to convey the same meaning. The left-hand side of the table below lists some ways of expressing the implication 'if P, then Q'. The right-hand side gives similar examples, but for the particular implication 'if $x > 2$, then $x^2 > 4$'.

Ways of writing 'if P, then Q'	Ways of writing 'if $x > 2$, then $x^2 > 4$'
P implies Q	$x > 2$ implies $x^2 > 4$
$P \Rightarrow Q$	$x > 2 \Rightarrow x^2 > 4$
Q whenever P	$x^2 > 4$ whenever $x > 2$
	(or: $x^2 > 4$, for all $x > 2$)
Q follows from P	$x^2 > 4$ follows from $x > 2$
P is sufficient for Q	$x > 2$ is sufficient for $x^2 > 4$
Q is necessary for P	$x^2 > 4$ is necessary for $x > 2$
P only if Q	$x > 2$ only if $x^2 > 4$

The symbol $\Rightarrow$ is read as 'implies'.

The form 'P only if Q' may seem strange at first; it asserts that the only circumstance in which P can be true is if Q is also true—that is, P implies Q.

Exercise 3.2 Rewrite each of the following statements in the form 'if P, then Q'. In each case, state whether you think the implication is true. You are not asked to justify your answers.

(a) $x^2 - 2x + 1 = 0 \Rightarrow (x-1)^2 = 0$.

(b) Whenever n is odd, so is n^3.

(c) Every integer that is divisible by 3 is also divisible by 6.

(d) $x > 2$ only if $x > 4$.

You will see how to prove or disprove statements like those in parts (b) and (c) formally later in this section. Whether the statement in part (a) is true or false may be established by algebraic manipulation.

The **converse** of the implication 'if P, then Q' is the implication 'if Q, then P'. For example, the converse of the implication

if $x > 2$, then $x^2 > 4$

is

if $x^2 > 4$, then $x > 2$.

In this example, the original implication is true, and its converse is false. It is also possible for an implication and its converse to be both true, or both false. In other words, knowledge of whether an implication is true or false tells you *nothing at all* about whether its converse is true or false. You should remember this important fact whenever you read or write implications.

To see that the converse is false, consider, for example, $x = -3$.

To help you remember facts like this about statements, you may find it helpful to consider non-mathematical examples. For example, consider the implication 'if Rosie is a sheep, then Rosie is less than two metres tall.' This implication is true, but its converse, 'if Rosie is less than two metres tall, then Rosie is a sheep', certainly is not!

Exercise 3.3 Write down the converse of each of the following statements about integers m and n. In each case, state whether you think the statement is true and whether you think the converse is true. You are not asked to justify your answers at this stage.

(a) If m and n are both odd, then $m + n$ is even.

(b) If one of the pair m, n is even and the other is odd, then $m + n$ is odd.

The statement 'if P, then Q, and if Q, then P', which asserts that the implication 'if P, then Q' and its converse are *both* true, is usually expressed more concisely as 'P if and only if Q'. Here are two examples.

'P if Q' means '$Q \Rightarrow P$', and 'P only if Q' means '$P \Rightarrow Q$'.

1. n is odd if and only if n^2 is odd.
2. $x > 2$ if and only if $x^2 > 4$.

Statements like these are called **equivalences**. Equivalence 1 above is true, because both implications are true, whereas equivalence 2 is false, because the implication 'if $x^2 > 4$, then $x > 2$' is false. As with implications, there are many different ways to express equivalences. The table below lists some ways in which this can be done.

Ways of writing 'P if and only if Q'	Ways of writing 'n is odd if and only if n^2 is odd'
$P \Leftrightarrow Q$	n is odd $\Leftrightarrow$ n^2 is odd
P is **equivalent** to Q	n is odd is equivalent to n^2 is odd
P is necessary and sufficient for Q	n is odd is necessary and sufficient for n^2 to be odd

The symbol $\Leftrightarrow$ is usually read as 'if and only if', or sometimes as 'is equivalent to'.

Exercise 3.4 For each of the following equivalences about integers, write down the two implications that it asserts, state whether you think each is true, and hence state whether you think the equivalence is true. You are not asked to justify your answers at this stage.

(a) The product mn is odd if and only if both m and n are odd.

(b) The product mn is even if and only if both m and n are even.

Although a mathematical statement should normally be interpreted as meaning precisely what it says—no more and no less, there is one common exception to this rule. When giving a definition, we usually write 'if' when we really mean 'if and only if'. For example, we write

a function $f : A \longrightarrow B$ is onto if $f(A) = B$.

3.3 Direct proof

A *proof* of a mathematical statement is a logical argument that establishes that the statement is true. Here is a simple example.

Example 3.2 Prove the following statement:

If n is an odd number between 0 and 10, then n^2 is also odd.

Solution The odd numbers between 0 and 10 are 1, 3, 5, 7, and 9. The squares of these numbers are 1, 9, 25, 49 and 81, respectively, and these are all odd. ■

In the above example, there were only a small number of possibilities to consider, and so it was easy to prove the statement by considering each one in turn. This method of proof is known as *proof by exhaustion*, because we exhaust all possibilities. In contrast, it is not possible to prove the statement 'If n is an odd number, then n^2 is also odd' using proof by exhaustion, because there are infinitely many possibilities to consider. Most mathematical statements that you will come across cannot be proved by exhaustion, because there are too many possibilities to consider—usually infinitely many. Instead we must supply a general proof.

Suppose that we wish to prove that the implication $P \Rightarrow Q$ is true. We have to prove that whenever the statement P is true, the statement Q is also true. Often the best way to do this is to start out by *assuming* that P is true, and proceed as follows. If we know that the statement

$$P \Rightarrow P_1$$

is true for some statement P_1, then we can deduce that P_1 is also true. Similarly, if we know that the statement

$$P_1 \Rightarrow P_2$$

is true for some statement P_2, then we can deduce that P_2 is also true. In this way we can build up a sequence of statements

$$P, P_1, P_2, \ldots,$$

each of which we know to be true under the assumption that P is true. The aim is to build up such a sequence

$$P, P_1, P_2, \ldots, P_n, Q,$$

which leads to Q. If this can be achieved, then we have a proof of the implication $P \Rightarrow Q$. Here is an example.

Example 3.3 Prove that if n is odd, then n^2 is odd.

Solution Let n be an odd integer. Then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

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

This shows that n^2 is an odd integer. ■

We see that n^2 is odd because we have shown that n^2 is equal to 2 times some integer plus 1.

In the above proof, statement P is 'n is odd', and we start by assuming that this is true. Statement P_1 is '$n = 2k + 1$ for some integer k', and so on. We use words like 'then' and 'hence' to indicate that one statement follows from another.

The string of equalities

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

in the proof in Example 3.3 can be regarded either as a sequence of three statements, namely

$$n^2 = (2k+1)^2,$$
$$n^2 = (2k)^2 + 2(2k) + 1,$$
$$n^2 = 2(2k^2 + 2k) + 1,$$

or as a single statement asserting the equality of all four expressions.

Many of the true statements about odd and even integers that appeared in the exercises in the last subsection can be proved using ideas similar to those of the proof in Example 3.3; that is, we write an odd integer as $2 \times$ some integer $+ 1$, and an even integer as $2 \times$ some integer. (Similarly, we can often prove statements about multiples of 3 by writing each such number as $3 \times$ some integer, and so on.) Here is another example.

Example 3.4 Prove that the sum of two odd integers is even.

Solution Let x and y be odd integers. Then

$$x = 2k + 1 \text{ and } y = 2l + 1 \text{ for some integers } k \text{ and } l.$$

It is important to choose different symbols k and l here. We certainly cannot deduce from the first statement that $x = 2k + 1$ and $y = 2k + 1$ for some integer k; that would be the case only if x and y were equal!

Hence

$$x + y = (2k + 1) + (2l + 1) = 2k + 2l + 2 = 2(k + l + 1).$$

This shows that $x + y$ is an even integer. ■

We have seen that a sequence $P, P_1, P_2, \ldots, P_n, Q$ of statements forms a proof of the implication $P \Rightarrow Q$ provided that each statement is shown to be true under the assumption that P is true. In Examples 3.3 and 3.4 each statement in the sequence was deduced from the statement immediately before, but the sequence can also include statements that are deduced from one or more statements further back in the sequence, and statements that we know to be true from our previous mathematical knowledge. This is illustrated by the next example.

A fact that you may already know which will be useful in this example, and also later in this section, is that every integer greater than 1 has a unique expression as a product of primes. For example, $6468 = 2 \times 2 \times 3 \times 7 \times 7 \times 11$, and this is the only way to express 6468 as a product of primes (except of course that we can change the order of the primes in the expression). This fact is known as the *Fundamental Theorem of Arithmetic*.

Recall that a *prime number* is an integer n, greater than 1, whose only positive factors are 1 and n.

It is certainly not obvious that the Fundamental Theorem of Arithmetic is true! However, a proof is outside the scope of this unit.

Example 3.5 Prove that for every integer n, the number $n^3 + 3n^2 + 2n$ is divisible by 6.

Solution Let n be an integer. Now

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

Thus $n^3 + 3n^2 + 2n$ is the product of three consecutive integers. We know that out of any two consecutive integers, one must be divisible by 2, and out of any three consecutive integers, one must be divisible by 3. It follows that the three factors n, $n + 1$ and $n + 2$ include one that is divisible by 2, and one that is divisible by 3 (possibly the same one). Hence both the primes 2 and 3 are factors of $n^3 + 3n^2 + 2n$. Hence (by the Fundamental Theorem of Arithmetic) $n^3 + 3n^2 + 2n$ can be expressed as $2 \times 3 \times r$ for some integer r, and so it is divisible by $6 = 2 \times 3$. ■

In this course you are expected to be able to produce only simple proofs yourself. However, you should also be able to read through more complex proofs like some of those later in the course, and understand why they prove the statements that they claim to prove.

The next exercise gives you practice in the techniques that you have seen in this subsection.

Exercise 3.5 Prove each of the following implications.

(a) If n is an even integer, then n^2 is even.

(b) If m and n are multiples of k, then so is $m + n$.

(c) If one of the pair m, n is odd and the other is even, then $m + n$ is odd.

(d) If n is a positive integer, then $n^2 + n$ is even.

If a proof of an implication is particularly simple, and each statement in the sequence follows directly from the one immediately before, then we sometimes present the proof by writing the sequence of statements in the form

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \cdots \Rightarrow P_n \Rightarrow Q.$$

It is conventional to write this to indicate that each of the statements $P \Rightarrow P_1$, $P_1 \Rightarrow P_2$, $\ldots$, $P_n \Rightarrow Q$ is true.

This is particularly appropriate for proofs that depend mostly on algebraic manipulation. Here is an example.

Example 3.6 Prove that if $x(x-2) = 3$, then $x = -1$ or $x = 3$.

Solution

$$\begin{aligned} x(x-2) = 3 &\Rightarrow x^2 - 2x - 3 = 0 \\ &\Rightarrow (x+1)(x-3) = 0 \\ &\Rightarrow x + 1 = 0 \text{ or } x - 3 = 0 \\ &\Rightarrow x = -1 \text{ or } x = 3. \end{aligned}$$

■

By proving the implication in Example 3.6, we showed that -1 and 3 are the only possibilities for solutions of the equation $x(x-2) = 3$. We did not show that -1 and 3 actually *are* solutions, since for that it is necessary to prove also that if $x = -1$ or $x = 3$, then $x(x-2) = 3$, that is, the *converse* of the given implication. Thus strictly we have not solved the equation! Whenever we solve an equation, an implication and its converse must both be proved; in other words, we need to prove an equivalence. We do this for the equation in Example 3.6 shortly.

See Example 3.7.

First we discuss how to prove equivalences in general. Since an equivalence asserts that two implications are true, the best way to prove it is usually to tackle each implication separately. However, if a simple proof of one of the implications can be found, in which each statement follows from the one before, then it is sometimes possible to 'reverse all the arrows' to obtain a proof of the converse implication. That is, if you have found a proof of the form

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow \cdots \Rightarrow P_n \Rightarrow Q,$$

Recall that the equivalence 'P if and only if Q' asserts that both the implication '$P \Rightarrow Q$' ('P only if Q') and its converse '$Q \Rightarrow P$' ('P if Q') are true.

then you *may* find that also each of the following implications is true:

$$Q \Rightarrow P_n \Rightarrow \cdots \Rightarrow P_3 \Rightarrow P_2 \Rightarrow P_1 \Rightarrow P.$$

In this case you may be able to present the proofs of both implications at once, by writing

$$P \Leftrightarrow P_1 \Leftrightarrow P_2 \Leftrightarrow P_3 \Leftrightarrow \cdots \Leftrightarrow P_n \Leftrightarrow Q.$$

As with implications, this is particularly appropriate for proofs that depend mostly on algebraic manipulation. The next example gives a proof of this type showing that the implication in Example 3.6 and its converse are both true.

Example 3.7 Prove that $x(x-2) = 3$ if and only if $x = -1$ or $x = 3$.

Solution

$$\begin{aligned} x(x-2) = 3 &\Leftrightarrow x^2 - 2x - 3 = 0 \\ &\Leftrightarrow (x+1)(x-3) = 0 \\ &\Leftrightarrow x + 1 = 0 \text{ or } x - 3 = 0 \\ &\Leftrightarrow x = -1 \text{ or } x = 3. \end{aligned}$$

■

Remember that the symbols $\Leftrightarrow$ and $\Rightarrow$ are used to link *statements*, not *expressions*. It is meaningless to write, for example, $x^2 - 2x - 3 \Leftrightarrow (x+1)(x-3)$; the correct symbol here is $=$.

In Example 3.7 we solved the equation $x(x-2)=3$; we showed that its solution set is $\{-1,3\}$. The forward ($\Rightarrow$) part of the proof shows that if x satisfies $x(x-2)=3$, then $x=-1$ or $x=3$; in other words, these are the only possible solutions of the equation. The backward ($\Leftarrow$) part shows that if $x=-1$ or $x=3$ then x satisfies $x(x-2)=3$; in other words, these two values actually are solutions of the equation. The symbol $\Leftrightarrow$ is the one to use when solving equations or inequalities, and you must be sure that its use is valid at each step; in other words, that both implications hold.

If you wanted to prove only that $x=-1$ and $x=3$ are solutions, and not that they are the only solutions, then although you could do so by giving the backward part of the above proof, it would be more natural to simply substitute each of these values in turn into the equation.

In this subsection we have discussed proof in the context of how to prove implications (and equivalences—but an equivalence is just two implications). However, what we have said extends to proofs of other types of statements. A statement Q that is not an implication can be proved by building up a sequence of statements leading to Q in the way that we have seen for an implication, except that there is no assumption P to be made at the start. Instead the first statement in the sequence must be one that we know to be true from our previous mathematical knowledge.

For example, statement 4 on page 36 is not an implication (nor an equivalence).

3.4 Counter-examples

Proving that an implication is true can be difficult. However, you may suspect that an implication is false, and it can often (but not always!) be easier to deal with this situation. To prove that an implication $P \Rightarrow Q$ is false, you just have to give *one* example of a case where the statement P is true but the statement Q is false. Such an example is called a **counter-example** to the implication. Here are two examples.

Example 3.8 Show that each of the following implications about integers is false, by giving counter-examples.

(a) If n is prime, then 2^n-1 is prime.

(b) If the product mn is a multiple of 4 then both m and n are multiples of 2.

Solution

(a) The number 11 is a counter-example, because 11 is prime but $2^{11}-1=2047$, which is not prime, since $2047=23\times 89$. Hence the implication is false.

See the text below for how you might find this counter-example.

(b) Taking $m=4$ and $n=1$ provides a counter-example, because then $mn=4$, which is a multiple of 4, but n is not a multiple of 2. Hence the implication is false. ■

There is no general method for finding counter-examples. For some statements, such as the statement in part (b) of the above example, a little thought about the statement should suggest a suitable counter-example. For other statements, the quickest method may just be to try out different values for the variable (or variables) until you hit on a counter-example. For example, for the statement in part (a) of the above example, we can repeatedly choose a prime number n, calculate 2^n-1 and check whether it is prime.

Remember that just *one* counter-example is sufficient. For example, you can show that the statement

if $x^2>4$ then $x>2$

is false by considering the value $x=-3$. There is no need to show that every number x less than -2 is a counter-example, even though this is true.

In order to carry out this procedure for Example 3.8(a), we need a method for checking whether a given number m is prime. We could simply check whether m is divisible by each of the integers between 2 and $m-1$, inclusive, but this involves a large amount of calculation even for fairly small integers m.

We can significantly reduce the amount of calculation needed by using the following fact, which holds for any integer $m \geq 2$:

> If m is not divisible by any of the primes less than or equal to $\sqrt{m}$, then m is a prime number.

You will be asked to prove this statement later in this section. Here is an example of its use.

Example 3.9 Show that 127 is a prime number.

Solution $\sqrt{127} = 11.3$, to one decimal place, so the primes less than or equal to $\sqrt{127}$ are $2, 3, 5, 7$ and 11. Dividing 127 by each of these in turn gives a non-integer answer in each case, so 127 is prime. ■

If this procedure is applied to a number that is not prime, then it will yield a prime factor.

Exercise 3.6 Give a counter-example to disprove each of the following implications.

(a) If $m + n$ is even, then both m and n are even.

(b) If $x < 2$ then $(x^2 - 2)^2 < 4$.

(c) If n is a positive integer, then $4^n + 1$ is prime.

As with implications, you may suspect that an equivalence is false. To prove that an equivalence $P \Leftrightarrow Q$ is false, you have to show that at least one of the implications $P \Rightarrow Q$ and $Q \Rightarrow P$ is false, which you can do by providing a counter-example.

3.5 Proof by induction

Mathematical induction is a method of proof that is useful for proving many statements involving integers. Consider, for example, the statement

$$1 + 3 + \cdots + (2n - 1) = n^2 \text{ for all positive integers } n.$$

Let us denote the statement

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

by $P(n)$. It is easy to check that $P(n)$ is true for small values of n; for example

$$1 = 1^2,$$
$$1 + 3 = 4 = 2^2,$$
$$1 + 3 + 5 = 9 = 3^2,$$

so certainly $P(1)$, $P(2)$ and $P(3)$ are all true. But how can we prove that $P(n)$ is true for all positive integers n?

This type of notation, in which a symbol denoting a statement is followed by a symbol denoting a variable, in brackets, is useful for a variable proposition (a statement that is true or false possibly depending on the value of a variable).

The method of induction works like this. Suppose that we wish to prove that a statement $P(n)$, such as the one above, is true for all positive integers n. Now suppose that we have proved that the following two statements are true.

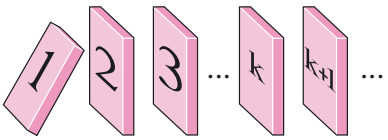
1. $P(1)$
2. If $P(k)$ is true, then so is $P(k + 1)$, for $k = 1, 2, \ldots$.

Let us consider what we can deduce from this. Certainly $P(1)$ is true, because that is statement 1. Also $P(2)$ is true, because by statement 2, if $P(1)$ is true, then so is $P(2)$. Similarly, $P(3)$ is true, since $P(2)$ is. Since this process goes on for ever, we can deduce that $P(n)$ is true for all positive integers n. We thus have the following method.

Principle of Mathematical Induction To prove that a statement $P(n)$ is true for $n = 1, 2, \ldots$.

1. Show that $P(1)$ is true.
2. Show that the implication $P(k) \Rightarrow P(k+1)$ is true for $k = 1, 2, \ldots$.

Mathematical induction is often compared to pushing over a line of dominoes. Imagine a (possibly infinite!) line of dominoes set up in such a way that if any one domino falls then the next domino in line will fall too—this is analogous to step 2 above. Now imagine pushing over the first domino—this is analogous to step 1. The result is that *all* the dominoes fall!



In the next example we apply mathematical induction to prove the statement mentioned at the beginning of this subsection.

This statement also appeared in the list of statements at the beginning of Subsection 3.1.

Example 3.10 Prove that $1 + 3 + \cdots + (2n-1) = n^2$, for $n = 1, 2, \ldots$.

Solution Let $P(n)$ be the statement $1 + 3 + \cdots + (2n-1) = n^2$.

Then $P(1)$ is true, because $1 = 1^2$.

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

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

We wish to deduce that $P(k+1)$ is true; that is,

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

The final term on the left-hand side here is $2(k+1) - 1 = 2k + 1$.

Now

$$\begin{aligned} 1 + 3 + \cdots + (2k+1) &= (1 + 3 + \cdots + (2k-1)) + (2k+1) \\ &= k^2 + (2k+1) \quad \text{(by } P(k)\text{)} \\ &= (k+1)^2. \end{aligned}$$

Hence

$$P(k) \Rightarrow P(k+1), \text{ for } k = 1, 2, \ldots.$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$. ■

Exercise 3.7 Prove each of the following statements by mathematical induction.

(a) $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$, for $n = 1, 2, \ldots$.

(b) $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$, for $n = 1, 2, \ldots$.

In the next example, we need to be careful to carry out appropriate algebraic manipulation so that we can use $P(k)$ to prove $P(k+1)$.

Example 3.11 Prove that $2^{3n+1} + 5$ is a multiple of 7, for $n = 1, 2, \ldots$.

Solution Let $P(n)$ be the statement

$2^{3n+1} + 5$ is a multiple of 7.

Then $P(1)$ is true, because $2^{3\times 1+1} + 5 = 2^4 + 5 = 21 = 3 \times 7$.

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

$2^{3k+1} + 5$ is a multiple of 7.

We wish to deduce that $P(k+1)$ is true; that is,

$2^{3(k+1)+1} + 5 = 2^{3k+4} + 5$ is a multiple of 7.

Now

$$\begin{aligned} 2^{3k+4} + 5 &= 2^3 2^{3k+1} + 5 \\ &= 8 \times 2^{3k+1} + 5 \\ &= 7 \times 2^{3k+1} + 2^{3k+1} + 5. \end{aligned}$$

The first manipulation is intended to create the sub-expression 2^{3k+1} in the expression, so we can use $P(k)$.

The first term here is a multiple of 7, and $2^{3k+1} + 5$ is a multiple of 7, by $P(k)$. Therefore $2^{3k+4} + 5$ is a multiple of 7. Hence

$P(k) \Rightarrow P(k+1)$, for $k = 1, 2, \ldots$.

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \ldots$. ■

Mathematical induction can be adapted to deal with situations that differ a little from the standard one. For example, if a statement $P(n)$ is not true for $n = 1$ but we wish to prove that it is true for $n = 2, 3, \ldots$, then we can do this by following the usual method, except that in step 1 we prove that $P(2)$, rather than $P(1)$, is true. (Also, in step 2 we have to show that $P(k) \Rightarrow P(k+1)$ for $k = 2, 3 \ldots$, rather than for $k = 1, 2, \ldots$.) In the next example we prove that a statement is true for $n = 7, 8, \ldots$.

This is analogous to pushing over the second domino in the line: the result is that all the dominoes except the first fall!

Example 3.12 Prove that $3^n < n!$ for all $n \geq 7$.

Solution Let $P(n)$ be the statement $3^n < n!$.

Then $P(7)$ is true, because $3^7 = 2187 < 5040 = 7!$.

$P(n)$ is false for $n = 1, 2, \ldots, 6$.

Now let $k \geq 7$, and assume that $P(k)$ is true; that is,

$3^k < k!$.

We wish to deduce that $P(k+1)$ is true; that is,

$3^{k+1} < (k+1)!$.

Now

$$\begin{aligned} 3^{k+1} &= 3 \times 3^k \\ &< 3 \times k! \quad (\text{by } P(k)) \\ &< (k+1)k! \quad (\text{because } k \geq 7, \text{ and hence } k+1 \geq 8 > 3) \\ &= (k+1)!\,. \end{aligned}$$

Hence $P(k) \Rightarrow P(k+1)$, for $k = 7, 8, \ldots$.

Hence, by mathematical induction, $P(n)$ is true, for $n = 7, 8, \ldots$. ■

Exercise 3.8 Prove each of the following statements by mathematical induction.

(a) $4^{2n-3} + 1$ is a multiple of 5, for $n = 2, 3, \ldots$.

(b) $5^n < n!$ for all $n \geq 12$.

3.6 Proof by contradiction

Sometimes a useful approach to proving a statement is to ask yourself, 'Well, what if the statement were false?'. Consider the following example.

Example 3.13 Prove that there is no positive real number a such that

$$a + \frac{1}{a} < 2.$$

Solution Suppose that there *is* a positive real number a such that

$$a + \frac{1}{a} < 2.$$

Then, since a is positive, we have

$$a\left(a + \frac{1}{a}\right) < 2a,$$

which, on multiplying out and rearranging, gives

$$a^2 - 2a + 1 < 0; \quad \text{that is,} \quad (a-1)^2 < 0.$$

But this is impossible, since the square of every real number is greater than or equal to zero. Hence we can conclude that there is no such real number a. ■

The above proof is an example of **proof by contradiction**. The idea is that if we wish to prove that a statement Q is true, then we begin by *assuming* that Q is *false*. We then attempt to deduce, using the method of a sequence of statements that you saw in Subsection 3.3, a statement that is definitely false, which in this context is called a *contradiction*. If this can be achieved, then since everything about our argument is valid except possibly the assumption that Q is false, and yet we have deduced a contradiction, we can conclude that the assumption is in fact false – in other words, Q is true.

Here is a classic proof by contradiction, which was given by Euclid in about 300 BC.

This was a favourite proof of the Cambridge mathematician G. H. Hardy (1877–1947), who described proof by contradiction as 'one of a mathematician's finest weapons'.

Example 3.14 Prove that there are infinitely many prime numbers.

Solution Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.

Consider the integer

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

This integer is greater than each of the primes $p_1, p_2, \ldots, p_n$, so it is not prime. Therefore it has a prime factor, p, say. Now p cannot be any of the primes $p_1, p_2, \ldots, p_n$, since dividing any one of these into N leaves the remainder 1. Thus, p is a prime other than $p_1, p_2, \ldots, p_n$. This is a contradiction, so our supposition must be false. It follows that there are infinitely many primes. ■

We are using the Fundamental Theorem of Arithmetic to deduce that N has a prime factor.

Exercise 3.9 Use proof by contradiction to prove each of the following statements.

(a) There are no real numbers a and b with $ab > \frac{1}{2}(a^2 + b^2)$.

(b) There are no integers m and n with $5m + 15n = 357$.

To prove an implication $P \Rightarrow Q$ using proof by contradiction, you should begin by assuming that P is true in the usual way. Then you should assume, hoping for a contradiction, that Q is false. If under these assumptions you can deduce a contradiction, then you can conclude that if P is true, then Q must also be true, which is the required implication. Here is an example.

Example 3.15 Prove that if $n = a \times b$ where $n > 0$, then at least one of a and b is less than or equal to $\sqrt{n}$.

Solution Suppose that $n = a \times b$ where $n > 0$. Suppose also that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$n = ab > (\sqrt{n})(\sqrt{n}) = n;$$

that is, $n > n$. This contradiction shows that the supposition that $a > \sqrt{n}$ and $b > \sqrt{n}$ must be false; that is, at least one of a and b is less than or equal to $\sqrt{n}$. ■

Exercise 3.10 Use proof by contradiction to prove that if $n = a + 2b$, where a and b are positive real numbers, then $a \geq \frac{1}{2}n$ or $b \geq \frac{1}{4}n$.

3.7 Proof by contraposition

Given any implication, we can form another implication, called its **contrapositive**, which is equivalent to the original implication. The contrapositive of the implication 'if P, then Q' is 'if not Q, then not P', where 'not P' and 'not Q' denote the negations of the statements P and Q, respectively. For example, the contrapositive of the implication

if x is an integer, then x^2 is an integer

is the implication

if x^2 is not an integer, then x is not an integer.

Here is another example: the contrapositive of the implication

if Rosie is a sheep, then Rosie is less than two metres tall

is

if Rosie is not less than two metres tall, then Rosie is not a sheep

or, more simply,

if Rosie's height is two metres or more, then Rosie is not a sheep.

You can think of an implication and its contrapositive as asserting the same thing, but in different ways. You should take a few moments to convince yourself of this in the case of the implication and its contrapositive given above. Try this also with the non-mathematical example in the margin!

Since an implication and its contrapositive are equivalent, if you have proved one, then you have proved the other. Sometimes the easiest way to prove an implication is to prove its contrapositive instead. This is called *proof by contraposition*. Here is an example. The proof makes use of the fact that

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1), \tag{3.1}$$

for any real number x and any positive integer n. This can be verified by multiplying out the right-hand side. (Try it!)

Example 3.16 Prove the following implication about positive integers n:

if $2^n - 1$ is prime, then n is prime.

Solution We shall prove the contrapositive of the implication, which is

if n is not prime, then $2^n - 1$ is not prime.

Suppose that n is a positive integer that is not prime. If $n = 1$, then $2^n - 1 = 2 - 1 = 1$, which is not prime. Otherwise $n = ab$, where $1 < a, b < n$. Hence

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1), \end{aligned}$$

In this proof we consider two cases separately: the cases $n = 1$ and $n > 1$. Splitting into cases is sometimes an effective way to proceed in a proof.

where the last line follows from equation (3.1). Now $2^a - 1 > 1$, since $a > 1$, and similarly $(2^a)^{b-1} + \cdots + 2^a + 1 > 1$, since both a and b are greater than 1. Hence $2^n - 1$ is not prime. We have thus proved the required contrapositive implication in both the cases $n = 1$ and $n > 1$. Hence the original implication is also true. ■

We put $x = 2^a$ and $n = b$ in equation (3.1).

Exercise 3.11 Use proof by contraposition to prove each of the following statements about integers m and n.

(a) If n^3 is even, then n is even.

(b) If mn is odd, then both m and n are odd.

(c) If an integer $n > 1$ is not divisible by any of the primes less than or equal to $\sqrt{n}$, then n is a prime number.

Hint: Use the result of Example 3.15, on page 48.

We used this result in Subsection 3.4.

3.8 Universal and existential statements

Many mathematical statements include the phrase 'for all', or another form of words with the same meaning. Here are a few examples.

$x^2 \geq 0$ *for all* real numbers x.
Every multiple of 6 is divisible by 3.
$1 + 3 + 5 + \cdots + (2n - 1) = n^2$ *for each* positive integer n.
Any rational number is a real number.

Statements of this type are known as *universal* statements, and the phrase 'for all', and its equivalents, are referred to as the *universal quantifier*.

The universal quantifier is sometimes denoted by the symbol $\forall$; for example, the first universal statement above might be abbreviated as

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

which is read as 'for all x in $\mathbb{R}$, x squared is greater than or equal to zero'.

Statements that begin with a phrase like 'There are no . . . ' or 'There does not exist . . .' are universal statements, because they can be rephrased in terms of 'For all'. For example, the statement

there is no integer n such that $n^2 = 3$

can be rephrased as

for all integers n, $n^2 \neq 3$.

Other mathematical statements may include the phrase 'there exists', or another form of words with the same meaning. Here are a few examples.

There exists a real number that is not a rational number.
There is a real number x such that $\cos x = x$.
Some multiples of 3 are not divisible by 6.
The equation $x^3 + x^2 + 5 = 0$ has *at least one* real solution.

In mathematics, the word *some* is used to mean 'at least one', rather than 'several'.

Statements of this type are known as *existential* statements, and the phrase 'there exists' and its equivalents are referred to as the *existential quantifier*.

The existential quantifier is sometimes denoted by the symbol $\exists$; for example, the second existential statement above might be abbreviated as

$\exists x \in \mathbb{R}$ such that $\cos x = x$,

which is read as 'there exists x in $\mathbb{R}$ such that $\cos x$ equals x'.

In natural language, the word 'any' may mean either 'every' or 'at least one', as in 'any fool could do that' and 'did you prove any theorems?'. In mathematics, the meaning depends on the context in a similar way. We try to avoid using 'any' where it might cause confusion.

We saw earlier in this section that it is often necessary to negate statements, for example when we wish to use proof by contradiction or proof by contraposition.

The negation of universal and existential statements needs to be treated with particular care. The negation of a universal statement is an existential statement, and vice versa. This is illustrated by the examples in the table below. You saw further examples in Example 3.1(a), and Exercises 3.1(c) and (d).

Statement	Negation
Every integer is a real number.	There exists an integer that is not a real number.
There is an even prime number.	Every prime number is odd.
The equation $x^2 + 4 = 0$ has a real solution.	The equation $x^2 + 4 = 0$ has no real solutions.

You may have found some of the ideas in this section difficult to get used to—this is to be expected, since reading and understanding mathematics, and writing mathematics clearly and accurately, can both be difficult at first. Your skills will improve as you gain experience. To accelerate this improvement, you should, when reading mathematics, try to make sure that you gain a clear understanding of exactly what each statement asserts. When writing mathematics, you should try to be as clear and accurate as you can. Include enough detail to make the argument clear, but omit any statements that are not necessary to reach the required conclusion. A good check is to read over your work and ask yourself whether you would be able to follow what you have written in six months' time, when you have forgotten the thoughts and rough work that led to it. Use the solutions to the examples and exercises in the course as models for good mathematical writing.

You may find it helpful to re-visit parts of Section 3 later in your study of the course.

Further exercises

Exercise 3.12 Which of the following statements have the same meaning?

(a) If n is even, then n^2 is a multiple of 4.

(b) n is even only if n^2 is a multiple of 4.

(c) n^2 is a multiple of 4 whenever n is even.

(d) $x > 0 \Rightarrow x^2 + 4x > 0$.

(e) $x > 0$ is necessary for $x^2 + 4x > 0$.

(f) $x > 0$ is sufficient for $x^2 + 4x > 0$.

Exercise 3.13 Determine whether the numbers 221 and 223 are prime.

Exercise 3.14 Prove, or give a counter-example to disprove, each of the following statements.

(a) If n is a positive integer, then $n^3 - n$ is even.

(b) If $m + n$ is a multiple of k, then m and n are multiples of k.

(c) If θ is a real number, then $\sin 2\theta = 2 \sin \theta$.

(d) The following function is one-one:

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto 3x^2 - 6x + 1.$$

(e) The function g is the inverse of the function f, where f and g are given by

$$f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{0\} \qquad g : \mathbb{R} - \{0\} \longrightarrow \mathbb{R} - \{1\}$$
$$x \longmapsto \frac{1}{x-1} \quad \text{and} \quad x \longmapsto 1 + \frac{1}{x}.$$

Exercise 3.15

(a) Write down the converse of the following statement.

If m and n are both even integers, then $m - n$ is an even integer.

(b) Determine whether the original statement and the converse are true, and give a proof or counter-example, as appropriate.

Exercise 3.16 Prove each of the following statements by mathematical induction.

(a) $\dfrac{1}{1\times 2} + \dfrac{1}{2\times 3} + \cdots + \dfrac{1}{(n-1)n} = \dfrac{n-1}{n}$ for $n = 2, 3, \ldots$.

(b) The integer $3^{2n} - 1$ is divisible by 8 for $n = 1, 2, \ldots$.

Exercise 3.17 Prove by contradiction that $(a+b)^2 \geq 4ab$ for all real numbers a and b.

Exercise 3.18

(a) Write down the contrapositive of the following statement, for positive integers n.

If n^2 is divisible by 3, then n is divisible by 3.

(b) Prove that the contrapositive is true, and hence that the original statement is true.

Exercise 3.19 Determine which of the following statements are true, and give a proof or counter-example as appropriate.

(a) For all $x, y \in \mathbb{R}$, $x < y \Rightarrow x^2 < y^2$.

(b) For all $x \in \mathbb{R}$, $x^2 - x = 2$.

(c) There exists $x \in \mathbb{R}$ such that $x^2 - x = 2$.

(d) There exists $x \in \mathbb{R}$ such that $x^2 - x = -1$.

(e) There are no real numbers x, y for which x/y and y/x are both integers.

(f) For all positive integers n,

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

(g) For all positive integers $n \geq 2$,

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{n}\right) = \frac{1}{2n}.$$