## 1A Proof by contradiction

Sometimes it is difficult to show directly that something must be true, but it is much simpler to show that the opposite is impossible. For example, suppose that we have an odd square number $n^2$ and we want to prove that $n$ must also be an odd number. It is not really obvious how to start. We could try taking the square root of $n^2$, but we don't know whether this produces an odd number (remember, this is what we are trying to prove!). However, thinking about what would happen if $n$ was *not* an odd number allows us to do some calculations: If $n$ was not odd it would be even, and the product of two even numbers is also even, so $n^2$ would be even. But we were told that $n^2$ was odd, so this situation is impossible! We can therefore conclude that $n$ must be odd. This way of reasoning is very common in all branches of mathematics, and is known as **proof by contradiction**.

Proof by contradiction is a special case of a more general form of argument, called *reductio ad absurdum*, in which a proposition is disproved by showing that its truth would lead to an impossible conclusion. This type of argument relies on the *law of excluded middle*, which states that either a proposition or its negation must be true.

KEY POINT 1.1

**Proof by contradiction**

You can prove that a statement is true by showing that if the opposite was true, it would contradict some of your assumptions (or something else we already know to be true).

Proof by contradiction was already used by Euclid around 300 BCE. One of the most famous examples was his proof that there are infinitely many prime numbers (see Worked example 2.15). Although it has been a widely used tool in mathematics since then, its validity has been disputed by some, most notably by the 20th century Dutch mathematician and philosopher L.E.J. Brouwer.

One of the most cited examples of proof by contradiction is the proof that $\sqrt{2}$ is an irrational number. Remember that the definition of an irrational number is that it cannot be written in the form $\frac{p}{q}$, where $p$ and $q$ are integers. It is difficult (if not impossible) to express the fact that a number is not of a certain form using an equation. Here proof by contradiction, where we start by assuming that $\sqrt{2}$ is of the form $\frac{p}{q}$, is a really useful tool.

**Worked example 1.1**

Prove that $\sqrt{2}$ cannot be written in the form $\frac{p}{q}$, where $p,q \in \mathbb{Z}$.

| | |
|---|---|
| Try proof by contradiction: Start by writing $\sqrt{2}$ as a fraction and show that this leads to impossible consequences | Suppose that $\sqrt{2} = \frac{p}{q}$ with $p,q \in \mathbb{Z}$, |
| The same fraction can be written in several ways (e.g. $\frac{1}{2} = \frac{3}{6} = \frac{5}{10}$) so we should specify which one we are using | and that the fraction is in its simplest form so that $p$ and $q$ have no common factors. |

→