M1 Maths

A6-5 Further Methods of Proof

- proof by deduction
- proof by exhaustion
- proof by contradiction
- proof by induction

Deduction Exhaustion Contradiction Induction

At Levels 5 and 6, you will sometimes be asked to prove a result that you already know or that is given. Proving means demonstrating that the result ***must*** be true.

Good communication will sometimes constitute a proof, though proofs are generally a bit more formal than good communication.

As explained in '*What is Maths*' the idea of proof is fundamental to the building of the body of mathematical knowledge.

Note that proof in a court of law is 'proof beyond reasonable doubt'. Mathematical proof is proof beyond any doubt, proof with absolute certainty.

There are four techniques of mathematical proof:

- proof by deduction
- proof by exhaustion
- proof by contradiction
- proof by induction

Proof by deduction is included in Knowledge Modules A5-8 and G5-1, though you may be introduced to the idea of proof earlier. In Australia, proofs by exhaustion, contradiction and induction are more the domain of senior maths – Specialist Maths in particular.

An explanation of each type of proof is given below. Although proof by deduction is included in the Knowledge modules, it is also included here for completeness and treated more fully.

Proof by Deduction

Proof by deduction is basically the same as showing working, though maybe a little more formal. It is writing a sequence of mathematical statements, the first being something that we are told (given information), each subsequent statement following in an obvious way from earlier ones, and the final statement being the result we are required to prove.

The ideas of proof by deduction are introduced informally in the context of geometry in Modules G2-2 (Geometric Figures), G2-3 (Properties of Polygons) and G2-6 (Congruence) and G3-1 (Similarity) and then more formally in the context of Geometry in Module G5-1 (Geometric Proofs) and algebra in Module A5-8 (Algebraic Proofs). Working through these modules should give a good feel for this type of proof.

There are a couple of conventions when writing up a formal proof. The first is to start with the initials 'RTP' followed by a statement of the result which is to be proved. RTP stands for 'Required to Prove'. The second is to write 'QED' after the final line of the proof. QED stands for 'Quod Erat Demonstrandum', which is Latin for 'What was to be shown'. Some jokingly say it stands for 'Quite Easily Done'. It doesn't, but that might be an easier way of remembering the initials.

Here is an example proof by deduction:

RTP: Multiplying any two odd numbers will produce an odd number

Any odd number is 2 times a whole number plus 1.

Let the two odd numbers be $2m + 1$ and $2n + 1$, where m and n are whole numbers

Their product will be $(2m + 1)(2n + 1)$

$$= 4mn + 2m + 2n + 1$$

$$= 2(2mn + m + n) + 1$$

Which is 2 times a whole number plus 1 and therefore an odd number.

QED

You can't prove by examples

One point that should be noted is that there is a common misconception that results like this can be proved by giving a few examples of multiplying odd numbers and showing that the result is always odd. This is maybe a proof beyond reasonable doubt, but it is not a proof beyond **any** doubt. It is always possible that there are a few exceptions to the rule and that the examples chosen happened not to include any of them. No number of examples constitutes a proof. However, it should be noted that even one counter-example is sufficient to disprove a statement.

Suppose we wanted to prove that $n^2 + n + 17$ is prime for all whole number values of n. We could pick some examples as follows:

n	$n^2 + n + 17$	n	$n^2 + n + 17$
0	17	7	73
1	19	8	89
2	23	9	107
3	29	10	127
4	37	11	149
5	47	12	173
6	59	13	199

All these numbers are prime. So it looks like the statement is true.

But $17^2 + 17 + 17 = 323$, which is 19×17 and therefore not prime.

No number of examples can ever prove a statement, but this one counter-example disproves it.

The other three techniques of proof are generally required only for Specialist Maths. They are not included in the knowledge modules, are introduced here for interest only.

Proof by Exhaustion

It was stated above that no number of examples can ever prove a statement. This is not totally true. If there are a finite number of possible examples and the statement is shown to be true for all of them, then that constitutes a valid proof.

This type of proof is called a proof by exhaustion because we have exhausted all the possible cases, not so much because the mathematician is exhausted after trying them all.

RTP: For any one-digit counting number, n, $n^7 - n$ is divisible 7

If $n = 1$, $n^7 - n = 0$, which is divisible by 7
If $n = 2$, $n^7 - n = 126$, which is divisible by 7 (7×18)
If $n = 3$, $n^7 - n = 2184$, which is divisible by 7 (7×312)
If $n = 4$, $n^7 - n = 16\,380$, which is divisible by 7 (7×2340)
If $n = 5$, $n^7 - n = 78\,120$, which is divisible by 7 ($7 \times 11\,160$)
If $n = 6$, $n^7 - n = 279\,930$, which is divisible by 7 ($7 \times 39\,990$)
If $n = 7$, $n^7 - n = 823\,536$, which is divisible by 7 ($7 \times 117\,648$)
If $n = 8$, $n^7 - n = 2\,097\,144$, which is divisible by 7 ($7 \times 299\,592$)
If $n = 9$, $n^7 - n = 4\,782\,960$, which is divisible by 7 ($7 \times 683\,280$)

So, for any one-digit counting number, n, $n^7 - n$ is divisible 7

QED

Proof by Contradiction

Proof by contradiction is sometimes called indirect proof to distinguish it from proof by deduction, which is sometimes called direct proof.

To prove a statement by contradiction, we assume the negation of the statement. (The negation of a statement is another statement that contradicts it.) Then we use deduction to prove that the negation is not true. This cannot happen if the negation is true and so proves it is not true, and this proves that the original statement is true.

RTP: $\sqrt{2}$ is irrational

Assume that $\sqrt{2}$ is rational,

Then $\sqrt{2}$ can be expressed as ${}^{a}/_{b}$ where a and b are integers with no common factor.

Then ${}^{a^2}/_{b^2} = 2$

$\therefore\ a^2 = 2b^2$

$\therefore\ a^2$ has a factor of 2,

$\therefore\ a$ has a factor of 2, so can be written $2k$, where k is an integer

$\therefore\ (2k)^2 = 2b^2$

$\therefore\ 4k^2 = 2b^2$

$\therefore\ 2k^2 = b^2$

$\therefore\ b^2$ has a factor of 2

$\therefore\ b$ has a factor of 2

$\therefore\ a$ and b both have a factor of 2, which contradicts our assumption.

Thus our assumption cannot be true and $\sqrt{2}$ must be irrational.

QED

Proof by Induction

Proof by induction is most often used for proving that something is true for all natural numbers. For instance, we can use induction to prove that the sum of the first n natural numbers is $\frac{1}{2}(n^2 + n)$.

We go about it in two steps.

The first step is to show that the statement is true for $n = 1$. This is generally quite easy: we just substitute 1 for n and show that the resulting statement is true. In this case:

The sum of the first 1 natural number is 1

$\frac{1}{2}(1^2 + 1) = \frac{1}{2} \times 2 = 1$

Therefore the statement is true for $n = 1$.

The second step is to show that, if the statement is true for $n = k$, where k is any counting number, then it will also be true for $n = k+1$. This will then tell us that, if it is true for $n = 1$ (which it is), then it will be true for $n = 2$, and if it is true for $n = 2$, then it will be true for $n = 3$, and so on to infinity.

To do this, we let $n = k$ and assume that the statement is correct, i.e. that the sum, of the first k natural numbers is $\frac{1}{2}(k^2 + k)$.

The sum of the first k+1 natural numbers is the sum of the first k plus the $k+1^{th}$, i.e. $\frac{1}{2}(k^2 + k) + k + 1$.

This can be rearranged

$$\begin{aligned}\tfrac{1}{2}(k^2 + k) + k + 1 &= \tfrac{1}{2}(k^2 + k + 2k + 2)\\ &= \tfrac{1}{2}(k^2 + 2k + 1 + k + 1)\\ &= \tfrac{1}{2}((k + 1)^2 + (k + 1))\end{aligned}$$

∴ the statement is true for $n = k+1$.

∴ the statement is true for all n.

The completed proof might look like this:

> RTP: the sum of the first n natural numbers is $\frac{1}{2}(n^2 + n)$
>
> Let n be 1
>
> The sum of the first 1 natural number is 1
>
> $\frac{1}{2}(1^2 + 1) = \frac{1}{2} \times 2 = 1$
>
> Therefore the statement is true for $n = 1$.
>
> Let n be k and assume that the statement is correct:
>
> Then the sum, of the first k natural numbers is $\frac{1}{2}(k^2 + k)$.
>
> The sum of the first k+1 natural numbers is the sum of the first k plus the $(k+1)^{th}$, i.e. $\frac{1}{2}(k^2 + k) + k + 1$.
>
> This can be rearranged
>
> $$\begin{aligned}\tfrac{1}{2}(k^2 + k) + k + 1 &= \tfrac{1}{2}(k^2 + k + 2k + 2)\\ &= \tfrac{1}{2}(k^2 + 2k + 1 + k + 1)\\ &= \tfrac{1}{2}((k+1)^2 + (k+1))\end{aligned}$$
>
> This is what the statement predicts for $n = k+1$.
>
> ∴ the statement is true for $n = k+1$.
>
> ∴ the statement is true for all n.
>
> QED