Section 1: Methods of proof

Notes and Examples

These notes have subsections on:

What is proof?

The word "proof" is used in many different contexts in everyday life. We often hear that scientists have "proved" a previously unknown fact about the world we live in, or we hear that forensic evidence in a court case has "proved" the guilt or innocence of a defendant.

In reality these situations do not involve proof in the mathematical sense. Scientists and lawyers use evidence that they collect to make deductions. In a court of law the evidence needs only to show "*beyond reasonable doubt*" that a defendant is guilty, but it can never be absolutely without doubt. DNA testing can offer overwhelmingly strong evidence, but even in these cases there is a very small probability that two people could have very similar DNA, or that the sample was contaminated.

Similarly, evidence collected by a scientist from observations may be overwhelmingly in favour of a particular theory, but it is always possible that further observations might contradict the theory. To take a very simple example, suppose you want to test whether or not a coin is biased. Suppose you tossed the coin 1000 times and got heads 1000 times. This seems to be very strong evidence that the coin is biased towards heads. However, it is always possible (though extremely unlikely) that if you tossed the coin another 1000 times you would get tails 1000 times! (If you study Statistics, you will learn, or may have already learned, how hypothesis testing helps us to make a decision about whether evidence is sufficient to support a theory. However, this does not *prove* that a theory is true!)

In real life, strong evidence for a particular claim is normally sufficient. In fact it has to be, since in the situations described above it is impossible to offer a completely watertight proof. However, a mathematician is never satisfied with overwhelming evidence. A mathematician wants to prove that a particular result is *always* true, in *all* possible cases.

To disprove a false conjecture, all you need to do is to find one counter-example for which the conjecture is not true. However, this may involve a lot of looking!

An interesting example: Fermat's Last theorem

Pierre de Fermat, a lawyer and amateur mathematician, was born in 1601. After his death a note was found in the margin of one of his books stating a conjecture that is known as "Fermat's last theorem", and the words "I have discovered a truly marvellous proof of this, but this margin is too narrow to contain it."

The conjecture itself is fairly straightforward to understand. You probably know that the equation

$$a^2 + b^2 = c^2$$

has solutions for which a, b and c are all integers, such as 3, 4, 5 ($3^2 + 4^2 = 5^2$) and 5, 12 , 13 ($5^2 + 12^2 = 13^2$). These are known as Pythagorean triples as they correspond to the length of the sides of a right-angled triangle, for which Pythagoras' theorem applies.

Fermat's conjecture was that there are no integer solutions to the equation

$$a^n + b^n = c^n$$

for any values of n greater than 2.

Various mathematicians have proved that this conjecture is true for particular values of n, such as $n = 3$ and $n = 4$. Computers allow a large number of cases to be checked in a short time, and by 1982 it had been shown that if a counter-example existed (i.e. a set of integers a, b, c and n for which $a^n + b^n = c^n$) then it involved values of a, b, c and n greater than 4,000,000. Since the value of a^n for such numbers is greater than the total number of the elementary particles in the known universe, it seemed unlikely that a counter-example would be found! However, even this overwhelming evidence is not enough for a mathematician!

Fermat's Last Theorem was finally proved in 1994 by Andrew Wiles of Cambridge, who had been obsessed since boyhood by the problem. Since his proof involved around 150 pages and used mathematical techniques which would not have been available to Fermat in the 17th century, it seems unlikely that Wiles' proof is the same as Fermat's "truly marvellous proof". It is now generally believed that Fermat had found a flaw in his own proof, as no further references to it have been found in his work. However, we cannot be sure of this, so although the theorem has been proved, a mystery remains: what was Fermat's "truly marvellous proof", and was it valid?

In this section you will look at three main methods of proof: direct proof; proof by exhaustion, and proof by contradiction. You will also look at disproof by use of a counter example.

Some notes and examples of each type are given below.

Direct proof

The main problem with direct proof is often deciding where to start. In many cases it will be useful to express the problem algebraically, and sometimes simple algebraic manipulation is all that is needed. In geometrical proofs a diagram is likely to be an essential part of the proof. Often you will need to use results that you know, such as Pythagoras' theorem or the quadratic formula. Don't be afraid to try something which you aren't sure whether it will work: even if a particular approach doesn't work, it may give you another idea.

Example 1 shows an example of a direct proof where a simple piece of algebraic manipulation is all that is needed.

Example 1
Prove that every odd integer is the difference of two perfect squares.

Solution
Any odd integer can be expressed in the form $2a + 1$.

$$2a + 1 = a^2 + 2a + 1 - a^2$$
$$= (a + 1)^2 - a^2.$$

Thinking about what you are aiming for helps to give the idea for this step

Example 2 shows direct proofs of two well-known results about divisibility.

Example 2
Prove that:
(i) a number is divisible by 3 if and only if the sum of its digits is divisible by 3
(ii) a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Solution
This conjecture involves numbers with any number of digits.
A number with n digits can be written as

$a_1a_2a_3....a_n$, where $a_1, a_2, a_3, ..., a_n$ are all single digits.

This number can be expressed as

$$10^{n-1}a_1 + 10^{n-2}a_2 + 10^{n-3}a_3 + ... + 10a_{n-1} + a_n$$
$$= (10^{n-1} - 1)a_1 + a_1 + (10^{n-2} - 1)a_2 + a_2 + ... + 9a_{n-1} + a_{n-1} + a_n$$
$$= (10^{n-1} - 1)a_1 + (10^{n-2} - 1)a_2 + ... + 9a_{n-1} + (a_1 + a_2 + ... + a_n)$$

All the numbers of the form $10^n - 1$ are numbers in which every digit is 9, so all these numbers are divisible by both 3 and 9.

Therefore:
(i) the number $a_1a_2a_3....a_n$ is divisible by 3 if and only if $a_1 + a_2 + a_3 + ... + a_n$ is divisible by 3

(ii) the number $a_1a_2a_3....a_n$ is divisible by 9 if and only if $a_1 + a_2 + a_3 + ... + a_n$ is divisible by 9

Edexcel A level Maths Proof 1 Notes and Examples

Proof by contradiction

In this method, you assume that the converse (i.e. the opposite) of the conjecture is true, and then show that this leads to a contradiction. The two examples which follow are well-known examples of the method of proof by contradiction, and you should be familiar with both of them.

Example 3
Prove that $\sqrt{2}$ is irrational.

Solution
Assume that $\sqrt{2}$ is rational, so it can be expressed in the form $\frac{m}{n}$ where m and n are integers and have no common factor.

$$\sqrt{2} = \frac{m}{n}$$
$$2 = \frac{m^2}{n^2}$$
$$m^2 = 2n^2$$

So m^2 must be even and so m must be even, and therefore m can be written as $2p$ where p is an integer.

$$(2p)^2 = 2n^2$$
$$4p^2 = 2n^2$$
$$2p^2 = n^2$$

So n^2 must be even and so n must be even.
Since m and n are both even, they have a common factor of 2, contradicting the original statement.

Example 4
Prove that there are infinitely many prime numbers.

Solution
Assume that there are only finitely many prime numbers. This means that all of them can be listed as follows: $p_1, p_2 ..., p_n$, where n is a finite number.

Now think about the number defined by $q = p_1p_2... p_n + 1$. If you divide q by any of the prime numbers $p_1, p_2 ..., p_n$, there is a remainder of 1.

So none of the prime numbers in the list are factors of q. Therefore either q is a prime number which is not on the list, or it has prime factors which are not on the list. This contradicts the assumption that **all** primes are in the list $p_1, p_2 ..., p_n$.

Therefore there are infinitely many prime numbers.

Edexcel A level Maths Proof 1 Notes and Examples

Proof by exhaustion

It is important to realise that proof by exhaustion may not necessarily involve testing every single case individually. In some cases it is possible to test a number of possible subsets of cases, as shown in the example below.

Example 5
Prove that no square number ends in an 8.

Solution
Obviously it is not possible to test every square number! However, the final digit of any square number is determined only by the final number of its square root, so you can reduce the problem to considering 1-digit numbers.

$0^2 = 0$ so the square of any number ending in 0 ends in 0.
$1^2 = 1$ so the square of any number ending in 1 ends in 1.
$2^2 = 4$ so the square of any number ending in 2 ends in 4.
$3^2 = 9$ so the square of any number ending in 3 ends in 9.
$4^2 = 16$ so the square of any number ending in 4 ends in 6.
$5^2 = 25$ so the square of any number ending in 5 ends in 5.
$6^2 = 36$ so the square of any number ending in 6 ends in 6.
$7^2 = 49$ so the square of any number ending in 7 ends in 9.
$8^2 = 64$ so the square of any number ending in 8 ends in 4.
$9^2 = 81$ so the square of any number ending in 9 ends in 1.

Therefore no square number ends in an 8.

Disproof using a counter-example

This is often very simple. You may be able to find a counter-example very quickly, and this is enough to disprove a conjecture. However, if you are unable to spot a counter-example, this does not mean that one does not exist. Using computers to check Fermat's Last Theorem up to very large numbers, as mentioned earlier, was an attempt to disprove the theorem rather that to prove it. However, there have been examples of conjectures for which counter-examples have been found after many years. In the 18th century Euler proposed a conjecture along similar lines to Fermat's Last Theorem: that the equation

$$a_1^n + a_2^n + a_3^n + \ldots + a_{n-1}^n = a_n^n$$

has no integer solutions for any $n > 2$. In this conjecture, notice that the number of unknowns is equal to the degree of the equation. So this conjecture states that there are no integer solutions to the equations $a^3 + b^3 = c^3$, $a^4 + b^4 + c^4 = d^4$, $a^5 + b^5 + c^5 + d^5 = e^5$ etc. But in 1966, about 200 years after the conjecture was proposed, a counter example was found for the case $n = 5$:
$27^5 + 84^5 + 110^5 + 133^5 = 144^5$.

Example 6
It is suggested that for every prime number p, $2p + 1$ is also prime. Prove that this is false.

Solution
For $p = 2$, $2p + 1 = 5$ which is prime.
For $p = 3$, $2p + 1 = 7$ which is prime.
For $p = 5$, $2p + 1 = 11$ which is prime.
For $p = 7$, $2p + 1 = 15$ which is not prime.
The statement is false.