METHODS OF PROOF

Aside from examples and counterexamples (which can be used to prove the truth of a 'there exists' statement or the falsehood of a 'for all' statement), a mathematical proof typically consists of a sequence of statements with each statement following directly from either definitions, previous steps, or established results. In this section, several common strategies of constructing proofs are illustrated:

As many of the statements proved are concerned with even and odd numbers, and divisibility more generally, it is necessary to be familiar with the following definitions:

- an integer n he said to be **even** if $n = 2k$ for some integer k

  e.g. 10 is even since 10 can be written as 2 multiplied by some integer, namely 5.

- similarly an integer is said to be **odd** if $n = 2k + 1$ for some integer k

  e.g. 11 is odd since it can be written as 1 more than 2 multiplied by some integer, namely 5

- an integer and is said to be **divisible** by the integer m if $n = mk$ for some integer k

  e.g. 15 is divisible by 5 since 15 can be expressed as 5 multiplied by some integers namely 3

Direct proof

The most straightforward way to prove a statement is to use a direct proof. A direct proof typically starts with introducing any relevant variables, clearly states any assumptions, and then establishes the desired result logical sequence of valid statements. Note that if the statements to be proved has the form 'if P then Q', then you assumed that P is true, and then proceed to show that Q must be true.

Example 8

Use a direct proof to prove that if a number is odd, then its square is also odd.

Solution

Let p be an odd integer.

Hence $p = 2k + 1$ for some integer k.

Consider p^2, which is to be proved odd:

$$p^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

As $2k^2 + 2k$ is an integer then $2(2k^2 + 2k)$ is even and $2(2k^2 + 2k) + 1$ is odd.

Hence p^2 is odd.

Proof by contraposition

Recall that the contrapositive of the statement $P \Rightarrow Q$ is $not\ Q \Rightarrow not\ P$. As the contrapositive is logically equivalent to the original statement, the original statement, $P \Rightarrow Q$, can be proved in directly by proving $not\ Q \Rightarrow not\ P$; that is by assuming that Q is false, and then proceeding to show that P must be false.

Example 9

Use a contrapositive proof to prove that if $5n + 3$ is odd, then n is even.

Solution

The contrapositive statement is: if n is not even, then $5n + 3$ is not odd. In other words, if n is odd, then $5n + 3$ is even.

Let n be an odd integer.

Hence $n = 2k + 1$ for some integer k.

$$
\begin{aligned}
5n + 3 &= 5(2k + 1) + 3 \\
&= 10k + 5 + 3 \\
&= 10k + 8 \\
&= 2(5k + 4)
\end{aligned}
$$

Since $5k + 4$ is an integer then $2(5k + 4)$ must be an even integer.

Hence $5n + 3$ is even.

Proof by contradiction

Another form of indirect proof but one that is not restricted to proving conditional statements is 'proof by contradiction'.

The basic idea of such a proof is to assume that the statement needing to be proved is false, and then show that this assumption leads to an absurd and impossible result; this then must mean that the initial assumption that the result was false cannot be true meaning that it must be true.

Example 10

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

(a) $\sqrt{2}$ is irrational. **(b)** If $5n + 3$ is odd, then n is even.

Solution

(a) Assume, for a contradiction, that $\sqrt{2}$ is rational.

Let $\sqrt{2} = \frac{p}{q}$ for integers p and q, with p and q having no common factors other than 1.

(p and q are relatively prime.)

Square both sides: $2 = \frac{p^2}{q^2}$

Rearrange: $p^2 = 2q^2$ and hence p^2 is divisible by 2.

If p^2 is divisible by 2 then p is divisible by 2.

Therefore, you can write $p = 2m$ for some integer m.

Substitute in $p^2 = 2q^2$: $4m^2 = 2q^2$

$2m^2 = q^2$

Hence q^2 is divisible by 2, so q is divisible by 2.

Since p and q are divisible by 2, this gives a contradiction to the original assumption that p and q had no common factors other than 1.

Hence the original assumption that $\sqrt{2}$ is rational is false.

Hence $\sqrt{2}$ is irrational.

(b) Assume, for a contradiction that $5n + 3$ is odd and n is odd.

Since n is odd: $n = 2k + 1$ for some integer k.

$$\begin{aligned} 5n + 3 &= 5(2k + 1) + 3 \\ &= 10k + 5 + 3 \\ &= 10k + 8 \\ &= 2(5k + 4) \end{aligned}$$

Since $5k + 4$ is an integer then $2(5k + 4)$ is even.

Hence $5n + 3$ is even and it can't be both odd and even.

Hence the assumption for n must be wrong, n cannot be odd so it must be even.

Note that the proof in part a) of the previous example used the fact that if the square of an integer is divisible by 2, then the original integer must also be divisible by 2. This fact is true not just for the number 2 but for any integers with no perfect squares factors over than 1.

You may use this fact when modifying the previous proof to prove the irrationality of other surds in the subsequent exercise.

Proving logical equivalences

The simplest method to prove a statement of the form $P \Leftrightarrow Q$ is to separately prove both $P \Rightarrow Q$ and $Q \Rightarrow P$, as demonstrated in the following example:

Example 11

Let n be a positive integer. Prove that $n + 9$ is odd if and only if $n - 8$ is even.

Solution

(i) Assume that $n + 9$ is odd.
Thus $n + 9 = 2k + 1$ for some integer k.

$$\begin{aligned} n - 8 &= n + 9 - 17 \\ &= 2k + 1 - 17 \\ &= 2k - 16 \\ &= 2(k - 8) \end{aligned}$$

Hence $n - 8$ is even as $2(k - 8)$ is even.

(ii) Conversely, assume that $n - 8$ is even.
Thus $n - 8 = 2k$ for some integer k.

$$\begin{aligned} n + 9 &= n - 8 + 17 \\ &= 2k + 17 \\ &= 2(k + 8) + 1 \end{aligned}$$

Hence $n + 9$ is odd since as $(2(k + 8) + 1)$ is odd.

The final example presented is a more complex proof of a well-known divisibility result:

Example 12

Prove that a three-digit number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution

(i) Let a, b and c be the digits, in order, of a three-digit number, N.
The number is: $N = 100a + 10b + c$
If N is divisible by 3, then $100a + 10b + c = 3k$ for some integer k.
Rearrange to create factors of 3:

$$\begin{aligned} 99a + 9b + a + b + c &= 3k \\ a + b + c &= 3k - 99a - 9b \\ a + b + c &= 3(k - 33a - 3b) \end{aligned}$$

Hence the sum of the digits is divisible by 3.

(ii) Conversely, assume that the sum of the digits is divisible by 3:
$a + b + c = 3k$ for some integer k.

$$\begin{aligned} N &= 100a + 10b + c \\ &= 99a + 9b + a + b + c \\ &= 99a + 9b + 3k \\ &= 3(33a + 3b + k) \end{aligned}$$

Hence N is divisible by 3.