

## Methods of Proof

Here we try to establish the correctness, or otherwise, of a statement through using a logical sequence of steps leading to a conclusion. We consider 5 types of approach.

### 1 Proof by exhaustion.

Here you consider all possible cases and check whether the statement is true or not.

**Example:** Given that  $p$  is a prime such that  $3 < p < 25$  prove, by exhaustion, the statement

$$“(p-1)(p+1) \text{ is divisible by } 12”.$$

We first establish the set of primes that satisfy the condition  $3 < p < 25$ , The list of primes is 2,3,5,7,11,13,17,19,23,29..... The primes we are interested in are 5,7,13,17,19 and 23. The function values are

$p$	5	7	13	17	19	23
$(p-1)(p+1) = (p^2-1)$	24	48	168	288	360	528

All of the function values are divisible by 12. Thus, we have proved the statement is true by exhaustion, i.e., by checking its validity for all cases.

### 2 Disprove by counter example

Here we investigate the statement being made to see if we can find a case which is untrue.

**Example:** Consider the statement,

$$“n^2 - n + 1 \text{ is a prime number for all values of } n \geq 2”.$$

If you take  $n = 8$  we obtain  $n^2 - n + 1 = 64 - 8 + 1 = 57 = 3 \times 19$  and so is not divisible by 12. This one counter example proves the statement is false.

### 3 Proof by contradiction

**Example:** Prove that  $\sqrt{2}$  is irrational, i.e., it cannot be written as a ratio of integers.

Suppose  $\sqrt{2}$  was rational, i.e., there exists integers  $A$  and  $B$ , with no common factors, such that  $\sqrt{2} = \frac{A}{B}$ .

Squaring we have  $\frac{A^2}{B^2} = 2$  or  $A^2 = 2B^2$ . This shows that  $A^2$ , and hence  $A$ , is divisible by 2. So we write  $A = 2D$  where  $D$  is an integer. Then  $A^2 = 4D^2$  or  $B^2 = 2D$ . By the same argument as for  $A$ , we can deduce that  $B$  has a factor of 2. Thus both  $A$  and  $B$  have a common factor of 2. This is a contradiction and so we deduce that  $\sqrt{2}$  is irrational.

### 4 Proof by deduction

Here we prove a statement by a logical sequence of mathematical steps. For example, suppose the statement is

$$“\text{the function } x^2 + 2x + 1 \text{ is greater than } 0 \text{ for all } x”$$

There are a number of ways to proceed but suppose we complete the square to give

$$x^2 + 2x + 2 = (x + 1)^2 + 1$$

Now  $(x + 1)^2 \geq 0$  for all  $x$ , only being 0 when  $x = -1$ . Thus, by adding 1, we can conclude that  $x^2 + 2x + 2 = (x + 1)^2 + 1 > 0$  for all values of  $x$ .

**Example:** For positive integers  $a, b$  and  $c$ , prove that

$$a^2 + b^2 < (a + b)^2 \quad \text{and deduce that} \quad a^2 + b^2 + c^2 < (a + b + c)^2$$

Expanding  $(a + b)^2$  gives  $(a + b)^2 = a^2 + b^2 + 2ab$ . But  $a$  and  $b$  are positive and so we can write  $2ab > 0$ . It therefore follows that  $(a + b)^2 = a^2 + b^2 + 2ab > a^2 + b^2$ .

Now let  $(a + b) = d$ , then  $(a + b + c)^2 = (d + c)^2 > d^2 + c^2$  by the earlier proof.

Also  $d^2 = (a + b)^2 > a^2 + b^2$  and so combining the results gives

$$(a + b + c)^2 > d^2 + c^2 > a^2 + b^2 + c^2$$

The desired result.

## 5 Proof by induction

Here we have a proposition  $P(n)$ , which depends on the positive integer  $n$ . Suppose we can show  $P(1)$  to be true and that the truth of  $P(n)$  implies the truth of  $P(n+1)$ . We are then able to deduce that  $P(n)$  is true for all positive integers  $n$ .

Before we give an example let us establish the logic of the above method. We use the method of contradiction, or proof by counter example.

Suppose there is a set of values of  $n$  for which the proposition is false. Let  $m$  be the minimum of that set, i.e.,  $P(m)$  is false but  $P(m-1)$  is true. We have, however, established that if  $P(n)$  is true then  $P(n+1)$  is true. Therefore, if  $P(m-1)$  is true then so is  $P(m)$ , a contradiction. Therefore, there can be no such set of  $n$  values for which the proposition is false.

**Example:** Show that, for all positive  $n$ ,  $2^{4n} - 1$  is divisible by 15.

Let  $P(m)$  be the proposition that it is divisible by 15 when  $n = m$ , i.e., there exists an integer  $k$  for which  $2^{4m} - 1 = 15k$ . Then for  $n = m + 1$  we can write

$$\begin{aligned} 2^{4(m+1)} - 1 &= 2^{4m} 2^4 - 1 = (15k + 1)2^4 - 1 \\ &= (15k)2^4 + (2^4 - 1) = (15k)2^4 + 15 = 15(k2^4 + 1) \end{aligned}$$

This shows that  $2^{4(m+1)} - 1$  is divisible by 15, i.e.,  $P(m+1)$  is true.

When  $n = 1$ ,  $2^{4n} - 1 = 2^4 - 1 = 16 - 1 = 15$ , and so  $P(1)$  is true. By the inductive hypothesis we can conclude that the proposition is true for all  $n$ .