# Proof and Elementary Number Theory

Prerequisites: Basic arithmetic, algebra, geometry and calculus.

Maths Applications: Proving and disproving statements.

Real-World Applications: How to think and argue logically.

## Sentences and Statements

Maths is based on the rules of logic. These rules apply to certain special types of objects.

Definition:

A **sentence** is any meaningful string of symbols or letters.

Example 1

' Red is a colour ', ' Maths is fun ' and ' 9 is a prime number ' are all sentences, as they are each a meaningful string of letters and symbols.

Note that sentences can be **true** or **false**, but do not have to be (it doesn't really make sense to ask if the second sentence in Example 1 is true or false; it is very subjective).

Definition:

A **statement** (aka **proposition**) is a sentence that is either true or false (but not both).

Example 2

Referring to Example 1, ' Red is a colour ' is a true statement, according to the meanings of the words in that order. ' 9 is a prime number ' is a false statement, as 3 is a factor of 9. ' Maths is fun ' is not a statement, as there is no way to decide whether the statement is true or false without further information (such as who is speaking, when the sentence was stated, etc.).

Example 3

' Stop running ! ' is not a statement, as it makes no sense to ask for the truth or falsity. It is more of an instruction.

Example 4

' What is your name ? ' is not a statement; it's a question.

Example 5

' This sentence is false '. Is the sentence true or false ? If it is true, then according to the sentence, it is false. However, if it is false, then it is true. So, it is not a statement.

Note that outwith mathematics, the sentences in all the examples above would be regarded as ' statements ', but according to the above definition they are not.

## *Types of Statements*

Definition:

A **compound statement** is a combination of statements.

Two special types of compound statements occur frequently and they have special names.

Definition:

The **conjunction** of 2 statements S and T is the statement ' S and T ', and is true when both S and T are true.

The conjunction of 2 statements can be true or false.

Example 6

The compound statement ' Red is a colour and 9 is a prime number ' is false, as both statements need to be true.

Definition:

The **disjunction** of 2 statements S and T is the statement ' S or T ', and is true when at least one of S or T is true.

The disjunction of 2 statements can be true or false.

Example 7

The compound statement ' Red is a colour or 9 is a prime number ' is true, as at least one of the statements is true.

Definition:

The **negation** of a statement S is the statement ' not S ', denoted $\sim S$, and is true when S is false (and vice versa).

Example 8

If S is the statement ' 9 is a prime number ' (which, remember, is false), then $\sim S$ is the statement ' 9 is not a prime number ' (which is true).

Many important statements in maths are classed as **quantified**. There are 2 types.

Definition:

A **universal statement** is one that refers to all elements of a set.

The symbol $\forall$ (' upside down A ') is called the **universal quantifier** and means ' for all '.

Example 9

The universal statement $x^2 > 0$ ($\forall\, x \in \mathbb{R}$) is false (take $x = 0$).

Example 10

The universal statement ' All squares and triangles are polygons ' is true.

Definition:

An **existential statement** is one that refers to the existence of at least one element of a set.

The symbol ∃ (' reflected E ') is called the **existential quantifier** and means ' there exists '.

Example 11

The existential statement ' There exists a negative number $y$ such that $y^3 = 27$ ' is false.

Example 12

The existential statement ' There is a planet that supports life ' is true (for example, Earth).

Note that some statements in real-life may be true or false depending on when the statement was made. For example, ' Earth is the only planet that has life ' is a statement that we believe to be true, but may be false at the moment (there may be life elsewhere, but we haven't discovered it) or may be false in the future (maybe there is a planet that is in the process of forming life).

## Proofs and Counterexamples

Definition:

A **proof** is a logically convincing argument that a given statement is true.

In a proof, we use starting points and reach an end point.

Definition:

An **axiom** (aka **assumption** or **hypothesis** or **postulate** or **premise**) is a statement that is taken to be true (not requiring proof) and used before the end of an argument.

Definition:

A **conclusion** (aka **thesis**) is a statement that is reached at the end of an argument.

## *Implication*

It is important to know when one statement follows from another. This process gives another type of statement.

Definition:

The statement ' If A, then B ' is called a **(material) implication** (aka **if, then statement** or **conditional** or **implication**) and written $A \Rightarrow B$ (read ' **A implies B** ' or ' **B is implied by A** '). $A \Rightarrow B$ is true except when A is true and B is false (a true statement cannot imply a false one).

A is called the **implicant** (aka **antecedent**) and B the **implicand** (aka **consequent**). The symbol $\Rightarrow$ is the **implication symbol** and means ' implies '.

Everyday examples of this can be weird, but the definition serves mathematical purposes. Remember, a true statement cannot imply a false one; anything else is allowed.

Example 13

Technically, the implication ' The Pope has walked on the Moon $\Rightarrow$ Apes rule the planet ' is true (even though both statements are false, at the moment).

Example 14

The implication ' $2 + 2 = 7 \Rightarrow 3$ is a prime number ' is true.

Example 15

The implication ' $n$ is odd $\Rightarrow$ $n^2$ is odd ' is true.

Examples like 13 and 14 will not be considered in this course, but it is instructive to be aware of what can happen logically.

Definition:

Statements A and B are **equivalent**, denoted $A \Leftrightarrow$ B (read, ' $A$ **if and only if** B '), if $A \Rightarrow$ B and B $\Rightarrow A$.

The statement $A \Leftrightarrow$ B is called a **biconditional** or **double implication**.

Example 16

The double implication ' P is a parallelogram $\Leftrightarrow$ P is a quadrilateral ' is false. ' P is a parallelogram $\Rightarrow$ P is a quadrilateral ' is true, but ' P is a quadrilateral $\Rightarrow$ P is a parallelogram ' is false, as not all quadrilaterals are parallelograms.

Example 17

The biconditional ' $x = 3$ or $x = -3 \Leftrightarrow x^2 = 9$ ' is true.

Definition:

The **converse** of the statement $A \Rightarrow$ B is B $\Rightarrow A$.

The converse of a statement may be true or false.

Example 18

The converse of ' T is a triangle $\Rightarrow$ T is a polygon ' (which is true) is ' T is a polygon $\Rightarrow$ T is a triangle ' (which is false).

Example 19

The converse of ' $n$ is an even number $\Rightarrow n$ is divisible by 2 ' (true) is '$n$ is divisible by 2 $\Rightarrow n$ is an even number ' (true).

Definition:

The **inverse** of the statement $A \Rightarrow$ B is $\sim A \Rightarrow \sim$B.

The inverse of a statement may be true or false.

Example 20

The inverse of ' T is a triangle $\Rightarrow$ T is a polygon ' (true) is ' T is not a triangle $\Rightarrow$ T is not a polygon ' (may be false, for example, a square).

Example 21

The inverse of ' $n$ is an even number $\Rightarrow$ $n$ is divisible by 2 ' (true) is ' $n$ is not an even number $\Rightarrow$ $n$ is not divisible by 2 ' (true).

Definition:

The **contrapositive** of the statement A $\Rightarrow$ B is $\sim$B $\Rightarrow$ $\sim$A and is equivalent to the statement A $\Rightarrow$ B.

So, the contrapositive of a given statement has the same truth value (true or false) as the given statement.

Example 22

The contrapositive of ' T is a triangle $\Rightarrow$ T is a polygon ' (true) is ' T is not a polygon $\Rightarrow$ T is not a triangle ' (true).

Example 23

The contrapositive of ' $n$ is even $\Rightarrow$ $n + 1$ is even ' (false) is '$n + 1$ is odd $\Rightarrow$ $n$ is odd ' (false).

Definition:

An **example** (aka **instance**) is something that satisfies a given statement.

An existential statement can be proved by citing an example.

Example 24

$\exists n \in \mathbb{N}$ such that $n^2 + 1$ is even.

For $n^2 + 1$ to be even, $n^2$ must be odd. So, for example, pick $n = 3$. Then $3^2 + 1 = 10$, which is even. So, the example $n = 3$ will work.

Definition:

A **counterexample** is an exception to a proposed statement.

Definition:

To **disprove** a statement means proving a statement false.

A universal statement can be disproved by citing a counterexample.

Example 25

$n^3 + n + 5$ is prime $(\forall\, n \in \mathbb{N})$.

Pick values of $n$ until one is reached that makes the statement false. $n$ = 1 gives 7, $n$ = 2 gives 15, which is clearly not prime. So, $n$ = 2 is a counterexample to the given statement.

There are different proof techniques. The ones we will study fall into the following categories.

- Direct Proof.
- Indirect Proof.
- Mathematical Induction Proof.

The end of a proof is often denoted by various symbols. These include **I**, ■, □ and *Q. E. D.* (*Quod Erat Demonstrandum*, latin for ' that which was to be demonstrated ').

## Direct Proof

Definition:

A **direct proof** is a proof that involves starting from assumptions and reaching a conclusion by a chain of directly flowing logical steps (often a string of equalities or inequalities).

Example 26

Prove that the sum of two rational numbers is rational.

Let $p, q \in \mathbb{Q}$. Then $\exists\ a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$ such that $p = \frac{a}{b}$ and $q = \frac{c}{d}$. Then,

$$p + q = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad + bc}{bd}$$

As $a, b, c, d \in \mathbb{Z}$, $ad + bc, bd \in \mathbb{Z}$; also, $b, d \neq 0 \Rightarrow bd \neq 0$. So, $p + q$ is one integer divided by a non-zero integer. Hence, $p + q \in \mathbb{Q}$.

Example 27

Prove that the square of an even number is even.

Let $n$ be an even number. Then $\exists\, k \in \mathbb{Z}$ s.t. (such that) $n = 2k$. Hence,

$$n^2 = (2k)^2$$

$$n^2 = 4k^2$$

$$n^2 = 2(2k^2)$$

As $k \in \mathbb{Z}$, $2k^2 \in \mathbb{Z}$, so $n^2$ is 2 times an integer; thus $n$ is even.

Example 28

Prove that if $a$ divides $b$ and $b$ divides $c$, then $a$ divides $c$.

If $a$ divides $b$, then $\exists\, m \in \mathbb{Z}$ s.t. $b = am$. Similarly, $b$ divides $c \Rightarrow \exists\, n \in \mathbb{Z}$ s.t. $c = bn$. The first equality gives $bn = amn$, and this together with the second equality yields,

$$c = amn$$

As $m, n \in \mathbb{Z}$, $mn \in \mathbb{Z}$. Thus, $a$ divides $c$.

Example 29

Prove that if $a$ divides $p$ and $a$ divides $q$, then $a$ divides $p - q$.

If $a$ divides $p$, then $\exists\, m \in \mathbb{Z}$ s.t. $p = am$. Similarly, $a$ divides $q \Rightarrow \exists\, n \in \mathbb{Z}$ s.t. $q = an$. Then,

$$p - q = am - an$$

$$p - q = a(m - n)$$

Hence, as $m, n \in \mathbb{Z}$, $m - n \in \mathbb{Z}$. Thus, $a$ divides $p - q$.

Example 30

Prove that if $x_1$ and $x_2$ are the 2 roots of the quadratic equation $ax^2 + bx + c = 0$, then $x_1 + x_2 = -\frac{b}{a}$ and $x_1 x_2 = \frac{c}{a}$.

According to the quadratic formula, the roots are given by,

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \qquad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

Adding $x_1$ and $x_2$ gives,

$$x_1 + x_2 = \frac{-b + \sqrt{b^2 - 4ac} - b - \sqrt{b^2 - 4ac}}{2a}$$

$$= \frac{-b - b}{2a}$$

$$= -\frac{b}{a}$$

Multiplying $x_1$ and $x_2$ gives,

$$x_1 x_2 = \frac{\left(-b + \sqrt{b^2 - 4ac}\right)\left(-b - \sqrt{b^2 - 4ac}\right)}{4a^2}$$

$$= \frac{b^2 - (b^2 - 4ac)}{4a^2}$$

$$= \frac{c}{a}$$

## Indirect Proof

Definition:

An **indirect proof** is a proof that involves assuming the negation of the conclusion.

There are 2 specific types of indirect proof that we will study.

### *Proof by Contradiction*

Definition:

An **proof by contradiction** is a way of proving $A \Rightarrow B$ by assuming $A$ and $\sim B$ and showing that this leads to a contradiction (often, but not always, showing $\sim A$).

Example 31

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

Let's phrase this in the form $A \Rightarrow B$. A: $x = \sqrt{2}$; B: $x \notin \mathbb{Q}$. Now assume the negation of B, i.e., suppose that $x \in \mathbb{Q}$. Then $\exists\, a, b \in \mathbb{Z}$ (with $b \neq 0$) s.t. $x = \frac{a}{b}$. It can be assumed that $\frac{a}{b}$ is in simplest form (as otherwise, any common factors that $a$ and $b$ have can be cancelled out). The 2 expressions for $x$ give,

$$\frac{a}{b} = \sqrt{2}$$

$$a^2 = 2b^2$$

Hence, $a^2$ is even. This implies that $a$ is even (see Example 37), i.e. $\exists\, c \in \mathbb{Z}$ s.t. $a = 2c$. Substituting this into the last expression gives,

$$4c^2 = 2b^2$$

$$b^2 = 2c^2$$

Hence, $b^2$ is even. This implies that $b$ is even. But this contradicts the fact that $a$ and $b$ have no common factor. Hence, the initial assumption that $\sqrt{2}$ is rational is false, i.e. $\sqrt{2}$ is irrational.

Example 32

Prove that there are infinitely many prime numbers.

Let us phrase this in the form A $\Rightarrow$ B. A: T is the set of all prime numbers; B: T is an infinite set. The negation of B is the statement that T is a finite set, i.e., that there exist only a finite number of prime numbers. Let us call these prime numbers $p_1,\ p_2,\ \ldots, p_n$. Next, consider the number $N$ defined by,

$$N = p_1\ p_2\ \ldots\ p_n\ +\ 1$$

By the Fundamental Theorem of Arithmetic, $N$ can be written as a product of primes. Hence, one of the $p_i$ ($1 \le i \le n$) divides $N$. Thus, this $p_i$ divides the difference (by Example 29) $N - p_1\ p_2\ \ldots\ p_n = 1$; but no prime number can divide 1. This is the desired contradiction.

Example 33

Prove that if $a \in \mathbb{Q}$ and $x$ is irrational, then $a + x$ is irrational.

A: $a \in \mathbb{Q}$ and $x$ is irrational; B: $a + x$ is irrational. Assume the negation of B, i.e., that $a + x$ is rational. Then $\exists\, s,\ t \in \mathbb{Z}$ (with $t \neq 0$) s.t.

$$a + x = \frac{s}{t}$$

$$x = \frac{s}{t} - a$$

$$x = \frac{s - at}{t}$$

Hence, $a \in \mathbb{Q}$ and $s, t \in \mathbb{Z}$ imply that $\frac{s - at}{t} = x \in \mathbb{Q}$, which contradicts the assumed irrationality of $x$.

The next example illustrates a very obvious result (which first year pupils often ask about !), but which, nonetheless, requires proof.

Example 34

Prove that there is no greatest whole number.

A: $\mathbb{W}$ is the set of all whole numbers; B: There is no largest element of $\mathbb{W}$. Assume the negation of B, i.e., that $\exists\ n \in \mathbb{W}$ s.t. $n \geq m$ ($\forall\, m \in \mathbb{W}$). However, $n + 1$ is a whole number, so $n + 1 \in \mathbb{W}$ and $n + 1 > n$, contradicting the maximality of $n$. Hence, there is no largest whole number.

## Proof by Contrapositive

Definition:

A **proof by contrapositive** is a way of proving $A \Rightarrow B$ by assuming $A$ and $\sim B$ and showing $\sim A$.

Example 35

Prove that, for $x \in \mathbb{Z}$, if $13x + 5$ is even, then $x$ is odd.

Assume that $13x + 5$ is even and $x$ is even. The latter implies that $\exists\, n \in \mathbb{Z}$ s.t. $x = 2n$. Hence,

$$13x + 5 = 26n + 5$$

$$13x + 5 = 2(13n + 2) + 1$$

As $n \in \mathbb{Z}$, $13n + 2 \in \mathbb{Z}$, so $13x + 5$ is odd; but this contradicts the assumed evenness of $13x + 5$. So, $x$ is odd.

Example 36

Prove that if $x^3 + 7x > 0$, then $x > 0$.

Assume that $x^3 + 7x > 0$ and $x \leq 0$. Then, $x^3 \leq 0$ and $7x \leq 0$. Thus,

$$x^3 + 7x \leq 0 + 0$$

$$x^3 + 7x \leq 0$$

This clearly violates the assumption that $x^3 + 7x > 0$. Hence, $x > 0$.

Example 37

Prove that, for $y \in \mathbb{W}$, $y^2$ even $\Rightarrow y$ even.

Assume that $y^2$ is even and $y$ is odd. Then $\exists n \in \mathbb{Z}$ s.t. $y = 2n + 1$. Then,

$$y^2 = (2n + 1)^2$$

$$y^2 = 4n^2 + 4n + 1$$

$$y^2 = 2(2n^2 + 2n) + 1$$

As $n \in \mathbb{Z}$, $2n^2 + 2n \in \mathbb{Z}$, and so $y^2$ is clearly odd. However, this violates the assumed evenness of $y^2$. Thus, $y$ is even.

## Proof by Mathematical Induction

This proof technique is used to show that a statement about natural numbers is true for all (or all apart from a finite subset of the) natural numbers.

The statement to be proved is denoted by P($n$).

Theorem (Principle of Mathematical Induction):

The **Principle of Mathematical Induction** states that a statement P($n$) is true for all natural numbers $n$ if (i) P(1) is true and for some $k \in \mathbb{N}$ (ii) P($k$) true $\Rightarrow$ P($k + 1$) true.

The first condition is known as the **Base Case** and the second is called the **Inductive Step**. P($k$) is known as the **Inductive Hypothesis**.

Sometimes the Base Case may not be for $n = 1$.

The ' domino analogy ' is useful in understanding the Principle of Mathematical Induction (PMI). Think of the Base Case as knocking down the first domino in a chain of dominoes and the Inductive Step as saying ' if one domino falls, then the one after it will also fall '. Together, these conditions become ' all dominoes are knocked over ' (statement is true for all $n$). For Base Case different from $n = 1$, this analogy is easily adapted.

Example 38

Prove that $3^n > n$ ($\forall\, n \in \mathbb{N}$).

The statement in question is,

$$\mathrm{P}(n) : 3^n > n$$

For the Base Case, evaluate each side of the inequality when $n = 1$ and check to see if the inequality is true. $3^1 = 3$ and this is clearly bigger than 1, i.e., $3^1 > 1$. Hence, P(1) is true. Now assume that P($k$) is true for some natural number $k$ (we don't pick a particular value, instead just working in general with $k$), so, $3^k > k$ (remember, this is the Inductive Hypothesis). Next, write down what we are required to prove (RTP),

$$\mathrm{RTP} : 3^{k+1} > k + 1$$

To prove this, start with the LHS of the inequality, and ***rewrite it so we can use the Inductive Hypothesis***,

$$\begin{aligned} 3^{k+1} &= 3^k \,.\, 3 \\ &> k \,.\, 3 \qquad \text{( Inductive Hypothesis)} \end{aligned}$$

$$\begin{aligned} &= k + 2k \\ &\geq k + 2 \\ &> k + 1 \end{aligned}$$

$$\therefore \quad 3^{k+1} > k + 1$$

Hence, by assuming P($k$) is true, i.e., $3^k > k$, we have shown that P($k + 1$) is true, i.e., $3^{k+1} > k + 1$. Hence, the Inductive Step has been proven. In conclusion, as P(1) is true and P($k$) true $\Rightarrow$ P($k + 1$) true, by the PMI, P($n$) is true $\forall\, n \in \mathbb{N}$.

Example 39

Prove that $5^n > 4^n$ for all natural numbers $n$.

$$\text{P}(n) : 5^n > 4^n$$

As $5 > 4$, P(1) is true, so the Base Case holds. Assume that P($k$) is true for some natural number $k$, i.e., $5^k > 4^k$. The RTP statement is,

$$\text{RTP} : 5^{k+1} > 4^{k+1}$$

So,

$$\begin{aligned} 5^{k+1} &= 5^k \,.\, 5 \\ &> 4^k \,.\, 5 \\ &> 4^k \,.\, 4 \\ &= 4^{k+1} \end{aligned}$$

$$\therefore \quad 5^{k+1} > 4^{k+1}$$

Hence, we have shown that $5^k > 4^k \Rightarrow 5^{k+1} > 4^{k+1}$, i.e., that P($k$) true $\Rightarrow$ P($k + 1$) true. Together with the fact that P(1) is true, the PMI shows that $5^n > 4^n$ ($\forall\, n \in \mathbb{N}$).

Example 40

Prove that $4^n - 1$ is divisible by 3 ($\forall\, n \in \mathbb{N}$).

This can be rephrased as,

$$P(n) : \exists\, p \in \mathbb{N} \;\text{ s.t. }\; 4^n - 1 = 3p$$

As $4^1 - 1 = 3 = 3 \,.\, 1$, P(1) is true. Assume that P($k$) is true for some natural number $k$, i.e., assume that $\exists\, q \in \mathbb{N}$ s.t. $4^k - 1 = 3q$. The RTP statement is,

$$\text{RTP} : \exists\, r \in \mathbb{N} \;\text{ s.t. }\; 4^{k+1} - 1 = 3r$$

So,

$$4^{k+1} - 1 = 4^k \,.\, 4 - 1$$

$$4^{k+1} - 1 = (3q + 1) \,.\, 4 - 1$$

$$4^{k+1} - 1 = 3 \,.\, 4q + 4 - 1$$

$$4^{k+1} - 1 = 3\,(4q + 1)$$

Taking $r$ to be $4q + 1$ (which is a natural number, since $q$ is), we have thus shown that P($k$) true $\Rightarrow$ P($k + 1$) true. Hence, as P(1) is true and P($k$) true $\Rightarrow$ P($k + 1$) true, the PMI implies that P($n$) is true ($\forall\, n \in \mathbb{N}$).

Example 41

Prove that $n! > 2^n$ for all natural numbers $n \geq 4$.

$$P(n) : n! > 2^n$$

The Base Case this time is $n = 4$ (start by pinging the fourth domino !). The LHS is $4! = 24$. The RHS is $2^4 = 16$. Hence, as $24 > 16$, P(4) is true. Assume that P($k$) is true for some natural number $k$, i.e., $k! > 2^k$. The RTP statement is,

$$\text{RTP} : (k + 1)! > 2^{k+1}$$

So,

$$\begin{aligned} (k + 1)! &= (k + 1) . k! \\ &> (k + 1) . 2^k \\ &\geq 2 . 2^k \\ &= 2^{k+1} \\ \therefore \qquad (k + 1)! &> 2^{k+1} \end{aligned}$$

Thus, P($k$) true $\Rightarrow$ P($k + 1$) true. So, P(1) is true and P($k$) true $\Rightarrow$ P($k + 1$) true imply, via the PMI, that P($n$) is true ($\forall\, n \in \mathbb{N}$).

Example 42

Prove that $\frac{d^n}{dx^n}(\ln x) = (-1)^{n+1}\frac{(n - 1)!}{x^n}$ ($\forall\, n \in \mathbb{N}$).

$$\text{P}(n) : \frac{d^n}{dx^n}(\ln x) = (-1)^{n+1}\frac{(n - 1)!}{x^n}$$

Verifying the Base Case requires more effort this time. For $n = 1$, the LHS becomes $\frac{d^1}{dx^1}(\ln x) = \frac{d}{dx}(\ln x)$ and the RHS becomes $(-1)^{1+1}\frac{(1 - 1)!}{x^1} = (-1)^2\frac{0!}{x} = \frac{1}{x}$. As $\frac{d}{dx}(\ln x) = \frac{1}{x}$, P(1) is true. Assume that P($k$) is true for some natural number $k$, i.e., $\frac{d^k}{dx^k}(\ln x) = (-1)^{k+1}\frac{(k - 1)!}{x^k}$. The RTP statement is,

$$\text{RTP} : \frac{d^{k+1}}{dx^{k+1}}(\ln x) = (-1)^{(k+1)+1}\frac{((k + 1) - 1)!}{x^{k+1}}.$$

So,

$$\frac{d^{k+1}}{dx^{k+1}}(\ln x) = \frac{d}{dx}\left(\frac{d^k}{dx^k}(\ln x)\right)$$

$$= \frac{d}{dx}\left( (-1)^{k+1}\ \frac{(k\ -\ 1)!}{x^k} \right)$$

$$= (-1)^{k+1}\ (k\ -\ 1)!\ \frac{d}{dx}\ x^{-k}$$

$$= (-1)^{k+1}\ (k\ -\ 1)!\ (-k\ x^{-k-1})$$

$$= (-1)(-1)^{k+1}\ k\ .\ (k\ -\ 1)!\ \ x^{-(k+1)}$$

$$= (-1)^{k+2}\ k!\ \ x^{-(k+1)}$$

$$\therefore \qquad \frac{d^{k+1}}{dx^{k+1}}\ (\ln x)\ =\ (-1)^{(k+1)+1}\ \frac{((k\ +\ 1)\ -\ 1)!}{x^{k+1}}$$

Thus, P($k$) true $\Rightarrow$ P($k$ + 1) true. So, P(1) is true and P($k$) true $\Rightarrow$ P($k$ + 1) true imply, via the PMI, that P($n$) is true ($\forall\ n \in \mathbb{N}$).

Example 43

Prove that $2^n > n^3$ ($\forall\ n > 9$).

$$\text{P}(n) : 2^n > n^3$$

The Base Case is $n = 10$ (ping the tenth domino to get going). The LHS is $2^{10} = 1\,024$ while the RHS is $10^3 = 1\,000$. So, as $1\,024 > 1\,000$, P(10) is true. Assume that P($k$) is true for some natural number $k$, i.e., $2^k > k^3$ . The RTP statement is,

$$\text{RTP} : 2^{k+1} > (k + 1)^3$$

Before proceeding, note that $(k + 1)^3 = k^3 + 3k^2 + 3k + 1$. Also, $k > 9 \Rightarrow k^2 > 9k$ and $k^3 > 9k^2$. Now,

$$2^{k+1} = 2^k . 2$$

$$> k^3 . 2$$

$$= k^3 + k^3$$

$$
\begin{aligned}
&> k^3 + 9k^2 \\
&= k^3 + 3k^2 + 6k^2 \\
&> k^3 + 3k^2 + 54k \\
&= k^3 + 3k^2 + 3k + 51k \\
&> k^3 + 3k^2 + 3k + 459 \\
&> k^3 + 3k^2 + 3k + 1
\end{aligned}
$$

$$\therefore \qquad 2^{k+1} > (k + 1)^3$$

Thus, P($k$) true $\Rightarrow$ P($k + 1$) true. So, P(1) is true and P($k$) true $\Rightarrow$ P($k + 1$) true imply, via the PMI, that P($n$) is true ($\forall\, n \in \mathbb{N}$).

Example 44

Prove that, for $x \in \mathbb{R}$, $\sin\,(x + 180n)^\circ = (-1)^n \sin x^\circ$ ($\forall\, n \in \mathbb{N}$).

$$\text{P}(n) : \sin\,(x + 180n)^\circ = (-1)^n \sin x^\circ$$

When $n = 1$, the LHS becomes $\sin\,(x + 180)^\circ = \sin x^\circ \cos 180^\circ + \cos x^\circ \sin 180^\circ = \sin x^\circ\,(-1) + \cos x^\circ\,(0) = -\sin x^\circ$. The RHS is clearly $-\sin x^\circ$. Thus, P(1) is true. Assume that P($k$) is true for some natural number $k$, i.e., $\sin\,(x + 180k)^\circ = (-1)^k \sin x^\circ$. The RTP statement is,

$$\text{RTP} : \sin\,(x + 180\,(k + 1))^\circ = (-1)^{k+1} \sin x^\circ$$

Now,

$$
\begin{aligned}
\sin\,(x + 180(k + 1))^\circ &= \sin\,((x + 180k) + 180)^\circ \\
&= \sin\,(x + 180k)^\circ \cos 180^\circ \\
&\quad + \cos\,(x + 180k)^\circ \sin 180^\circ \\
&= (-1)^k \sin x^\circ\,(-1) \\
&\quad + \cos\,(x + 180)^\circ\,(0)
\end{aligned}
$$

$$= (-1)^{k+1} \sin x^{\circ}$$

$$\therefore \qquad \sin(x + 180(k + 1))^{\circ} = (-1)^{k+1} \sin x^{\circ}$$

Thus, P($k$) true ⇒ P($k$ + 1) true. So, P(1) is true and P($k$) true ⇒ P($k$ + 1) true imply, via the PMI, that P($n$) is true ($\forall\, n \in \mathbb{N}$).

## The Fundamental Theorem of Arithmetic

The following theorem is a very important result in mathematics.

> Fundamental Theorem of Arithmetic:
>
> Every integer bigger than 1 can be written uniquely (apart from ordering) as a product of prime numbers.

For example, $60 = 2^2 . 3 . 5 = 3 . 5 . 2^2$.

The Fundamental Theorem of Arithmetic can be used to give an alternative proof of the irrationality of $\sqrt{2}$.

Example 45

Using the same notation as in Example 31,

$$a^2 = 2b^2$$

As $a, b \in \mathbb{Z}$, the Fundamental Theorem of Arithmetic says that $a$ and $b$ can be written as,

$$a = 2^{m_1} p_2^{m_2} p_3^{m_3} \dots p_r^{m_r} , \quad b = 2^{n_1} q_2^{n_2} q_3^{n_3} \dots q_s^{n_s}$$

where all $p_i$ and $q_j$ are odd and all $m_i$ , $n_j$ are natural numbers. Using the relation above gives,

$$2^{2m_1} p_2^{2m_2} p_3^{2m_3} \dots p_r^{2m_r} = 2^{2n_1+1} q_2^{2n_2} q_3^{2n_3} \dots q_s^{2n_s}$$

The Fundamental Theorem of Arithmetic says that these 2 factorisations must be identical (apart from possible reordering). Hence, $r = s$, and the $q_j$ equal the $p_i$. After possible relabelling of the $q_j$, we then have,

$$2^{2m_1} p_2^{2m_2} p_3^{2m_3} \dots p_r^{2m_r} = 2^{2n_1+1} p_2^{2n_2} p_3^{2n_3} \dots p_r^{2n_r}$$

Thus, $m_i = n_i$ $(2 \le i \le r)$. Hence,

$$2^{2m_1} = 2^{2n_1+1}$$

Finally,

$$2m_1 = 2n_1 + 1$$

This is a clear contradiction, as it says that an even number equals an odd number. Try proving that $\sqrt{3}$ is irrational by this method. Also, try ' proving ' that $\sqrt{4}$ is irrational and see where the argument breaks down.