PROOF BY CONTRADICTION & CONTRAPOSITION

PROOF BY CONTRADICTION:

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

THEOREM:

There is no greatest integer.

PROOF:

Suppose there is a greatest integer N. Then $n \le N$ for every integer n.

Let $M = N + 1$

Now M is an integer since it is a sum of integers.

Also $M > N$ since $M = N + 1$

Thus M is an integer that is greater than the greatest integer, which is a contradiction. Hence our supposition is not true and so there is no greatest integer.

EXERCISE:

Give a proof by contradiction for the statement:
"If n^2 is an even integer then n is an even integer."

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.
Hence $n = 2k + 1$ for some integer k.

Now
$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\cdot(2k^2 + 2k) + 1 \\ &= 2r + 1 \qquad \text{where } r = (2k^2 + 2k) \in Z \end{aligned}$$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

EXERCISE:

Prove by contradiction method, the statement: If n and m are odd integers, then n + m is an even integer.

SOLUTION:

Suppose n and m are odd and n + m is not even (odd i.e by taking contradiction).

Now $n = 2p + 1$ for some integer p

and $m = 2q + 1$ for some integer q

Hence $n + m = (2p + 1) + (2q + 1)$

$= 2p + 2q + 2 = 2\cdot (p + q + 1)$

which is even, contradicting the assumption that n + m is odd.

THEOREM:

The sum of any rational number and any irrational number is irrational.

PROOF:

We suppose that the negation of the statement is true. That is, we suppose that there is a rational number r and an irrational number s such that r + s is rational. By definition of ration

$$r = \frac{a}{b} \qquad \ldots\ldots\ldots\ldots\ldots(1)$$

and

$$r + s = \frac{c}{d} \qquad \ldots\ldots\ldots\ldots\ldots(2)$$

for some integers a, b, c and d with $b \neq 0$ and $d \neq 0$.

Using (1) in (2), we get

$$\frac{a}{b} + s = \frac{c}{d}$$

$$\Rightarrow \quad s = \frac{c}{d} - \frac{a}{b}$$

$$s = \frac{bc - ad}{bd} \qquad (bd \neq 0)$$

Now bc - ad and bd are both integers, since products and difference of integers are integers. Hence s is a quotient of two integers bc-ad and bd with bd ≠ 0. So by definition of rational, s is rational.
This contradicts the supposition that s is irrational. Hence the supposition is false and the theorem is true.

EXERCISE:

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

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

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

that
Squaring both sides gives

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

Or $m^2 = 2n^2$ ………………………(1)
This implies that m^2 is even (by definition of even). It follows that m is even. Hence
m = 2 k for some integer k (2)
Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$
$$\Rightarrow \quad 4k^2 = 2n^2$$
$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

EXERCISE:

Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.

PROOF:

Suppose $6 - 7\sqrt{2}$ is rational.
Then by definition of rational,

$$6 - 7\sqrt{2} = \frac{a}{b}$$

for some integers a and b with $b \neq 0$.
Now consider,

$$7\sqrt{2} = 6 - \frac{a}{b}$$

$$\Rightarrow \quad 7\sqrt{2} = \frac{6b-a}{b}$$

$$\Rightarrow \quad \sqrt{2} = \frac{6b-a}{7b}$$

Since **a** and **b** are integers, so are **6b-a** and **7b** and **7b≠0**;
Hence $\sqrt{2}$ is a quotient of the two integers 6b-a and 7b with $7b \neq 0$.
Accordingly, $\sqrt{2}$ is rational (by definition of rational).
This contradicts the fact because $\sqrt{2}$ is irrational.
Hence our supposition is false and so $6 - 7\sqrt{2}$ is irrational.

EXERCISE:

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

SOLUTION:

Suppose $\sqrt{2} + \sqrt{3}$ is rational. Then, by definition of rational, there exists integers a and b with $b \neq 0$ such that

$$\sqrt{2} + \sqrt{3} = \frac{a}{b}$$

Squaring both sides, we get

$$2 + 3 + 2\sqrt{2}\sqrt{3} = \frac{a^2}{b^2}$$

$$\Rightarrow \quad 2\sqrt{2 \times 3} = \frac{a^2}{b^2} - 5$$

$$\Rightarrow \quad 2\sqrt{6} = \frac{a^2 - 5b^2}{b^2}$$

$$\Rightarrow \quad \sqrt{6} = \frac{a^2 - 5b^2}{2b^2}$$

Since a and b are integers, so are therefore $a^2 - 5b^2$ and $2b^2$ with $2b^2 \neq 0$.

Hence $\sqrt{6}$ is the quotient of two integers $a^2 - 2b^2$ and $2b^2$ with $2^2 \neq 0$.
Accordingly, $\sqrt{6}$ is rational.
But this is a contradiction, since $\sqrt{6}$ is not rational.
Hence our supposition is false and so
$\sqrt{2}+\sqrt{3}$ is irrational.

REMARK:

The sum of two irrational numbers need not be irrational in general for which

$$(6-7\sqrt{2})+(6+7\sqrt{2})=6+6=12$$

is rational.

EXERCISE:

Prove that for any integer **a** and any prime number **p**, if $p|a$, then
$P \nmid (a + 1)$.

PROOF:

Suppose there exists an integer **a** and a prime number **p** such that $p|a$ and $p|(a+1)$.
Then by definition of divisibility there exist integer r and s so that

$$a = p \cdot r \text{ and } \quad a + 1 = p \cdot s$$

It follows that

$$\begin{aligned} 1 &= (a + 1) - a \\ &= p \cdot s - p \cdot r \\ &= p \cdot (s-r) \qquad \text{where } s - r \in Z \end{aligned}$$

This implies $p|1$.
But the only integer divisors of 1 are 1 and -1 and since p is prime $p>1$. This is a contradiction.
Hence the supposition is false, and the given statement is true.

THEOREM:

The set of prime numbers is infinite.

PROOF:

Suppose the set of prime numbers is finite.
Then, all the prime numbers can be listed, say, in ascending order:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots,\ p_n$$

Consider the integer

$$N = p_1.p_2.p_3. \ldots . p_n + 1$$

Then $N > 1$. Since any integer greater than 1 is divisible by some prime number p, therefore $p \mid N$.
Also since p is prime, p must equal one of the prime numbers
$p_1, p_2, p_3, \ldots, p_n$.
Thus
$p \mid (p_1, p_2, p_3, \ldots, p_n)$

But then

$$p \nmid (p_1, p_2, p_3, \ldots, p_n + 1)$$

So $p \nmid N$

Thus $p \mid N$ and $p \nmid N$, which is a contradiction.

Hence the supposition is false and the theorem is true.

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2\cdot(2k^2 + 2k) + 1$

$= 2\cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE:

Prove that if $3n + 2$ is odd, then n is odd.

PROOF:

The contrapositive of the given conditional statement is

" if n is even then $3n + 2$ is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence $3n + 2$ is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore $n^2 = n.n$ is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"
Suppose n is divisible by 5. Then by definition of divisibility

$n = 5 \cdot k$ for some integer k

Squaring both sides

$n^2 = 25 \cdot k^2$ where $k^2 \in Z$

n^2 is divisible by 25

.

EXERCISE:

Prove that if $|x| > 1$ then $x > 1$ or $x < -1$ for all $x \in R$.

PROOF:

The contrapositive statement is:

if $x \leq 1$ and $x \geq -1$ then $|x| \leq 1$ for $x \in R$.

Suppose that $x \leq 1$ and $x \geq -1$

$\Rightarrow$ $x \leq 1$ and $x \geq -1$

$\Rightarrow$ $-1 \leq x \leq 1$

and so

$|x| \leq 1$

Equivalently $|x| > 1$

EXERCISE:

Prove the statement by contraposition:

For all integers m and n, if m + n is even then m and n are both even or m and n are both odd.

PROOF:

The contrapositive statement is:

"For all integers m and n, if m and n are not both even and m and n are not both odd, then m + n is not even.

Or more simply,

"For all integers m and n, if one of m and n is even and the other is odd, then m + n is odd"

Suppose m is even and n is odd. Then

$m = 2p$ for some integer p

and $n = 2q + 1$ for some integer q

Now $m + n = (2p) + (2q + 1)$

$= 2 \cdot (p+q) + 1$

$= 2 \cdot r + 1$ where $r = p+q$ is an integer

Hence m + n is odd.

Similarly, taking m as odd and n even, we again arrive at the result that m + n is odd.

Thus, the contrapositive statement is true. Since an implication is logically equivalent to its contrapositive so the given implication is true.