Methods of Proof

Many laws in logic can be applied to proof in mathematics. There are many methods of proof deduced from laws of logic as follows.

1. Direct proof
2. Proof statement $p \leftrightarrow q$
3. Proof by cases
4. Proof by contrapositive
5. Proof by contradiction
6. Prove by mathematical Induction
7. Proving a statement in the form, $p \rightarrow (q \vee r)$.
8. Proof by counter example
9. Proof of existence

1. Direct proof : Proof that $p \rightarrow q$ is true.

Method : Accept that p is true and apply a sequence of logical implication until the result is q. Then , we can conclude that $p \rightarrow q$ is true.

> Proof: accept the p is true
>
> ....
>
> .... } use p, definitions, axioms, theorems and logical implication
>
> ....
>
> Therefore, q.
>
> So, $p \rightarrow q$ is true.

Example 1 Prove that $\forall a \in I$ if a is even, then a^2 is even.

Proof : Let a be even . (p)

$a = 2k, \quad k \in I$ (definition)

$a^2 = (2k)^2$ (Theorem)

$a^2 = 4k^2 = 2(2k^2)$

$2k^2 \in I$ (Theorem)

a^2 is even (Definition). (q)

So, the statement if a is even, then a^2 is even is true.

Example 2 : Prove that if a and b are odd, then a + b is even.

Solution : Given a and b are odd (p)

Let a = 2k + 1, k = integer

b = 2m + 1, m = integer

$\therefore$ a + b = (2k + 1) + (2m + 1)

= 2k + 2m + 2

= 2(k+m+1), k + m + 1 = integer

So, a + b is even (q)

Therefore , $p \to q$ is true.

That is the statement, if a and b are odd, then a + b is even, is true.

Exercises (direct proof)

Prove that

1. If a and b are odd, then a + b is even
2. If a and b are odd, then ab is odd.
3. If a and b are even, then ab is even
4. If a is odd, then a^2 is odd.
5. If x and y are positive real numbers and $x < y$, then $x^2 < y^2$.
6. If a, b, c and d are positive real numbers and $a < b$ and $c < d$ then $ab < cd$.

2. Proving statements $p \leftrightarrow q$

We can use logical equivalence $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ in proving $p \leftrightarrow q$ by proving $(p \to q) \wedge (q \to p)$.

Example 3 : prove that a is even if and only if a + 1 is odd.

Solution : Let p : a is even, q : a + 1 is odd.

To prove that $p \leftrightarrow q$ is true, we will prove that $p \to q$ is true and $q \to p$ is true.

1) To prove $p \to q$

Accept that a is even (p).

So, a = 2k, k = any integers

a + 1 = 2k + 1

2k + 1 is odd (definition)

a + 1 is odd (q)

therefore, $p \rightarrow q$ is true.

2) To prove $q \rightarrow p$

Accept that a + 1 is odd (q)

So, a + 1 = 2k + 1, k = any integers

a = 2k

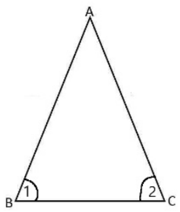
so, a is even (p)

therefore $q \rightarrow p$ is true .

From 1) and 2), $p \leftrightarrow q$ is true.

That is a I even iff a + 1 is odd.

Example 4 From ΔABC below, prove that $m(1) = m(2) \leftrightarrow AB = AC$.



Proof : Let p : $m(1) = m(2)$

q : $AB = AC$

We will prove $(p \rightarrow q) \wedge (q \rightarrow p)$.

1) Prove $p \rightarrow q$

Assume $m(1) = m(2)$

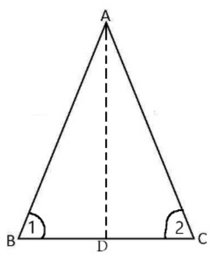
Consider ΔABC and ΔACB

$\Delta ABC \cong \Delta ACB$ (ASA)

So, AB = AC (Congruence of Δ)

That is $p \rightarrow q$

2) To prove if AB = AC, then m(1) = m(2).



Given AB = AC (p)

D is a mid – point of $\overline{BC}$

$\Delta ABD \cong \Delta ACD$ (SSS)

$\therefore p \rightarrow q$ is true.

From 1) and 2), $p \leftrightarrow q$ is true.

Exercise (prove $p \leftrightarrow q$)

Prove that

1. a is odd iff a + 1 is even
2. a is odd iff a^2 is odd.
3. a + 1 is even iff $a^2 + 1$ is even.
4. a is odd iff $a^2 - 1$ is even.
5. a + b is even iff a – b is even.
6. a^2 is odd iff a + 2 is odd.

3. Proof by Cases

From logical equivalence $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$. To prove that $(p \vee q) \to r$ is true, we just prove that both $(p \to r)$ and $(q \to r)$ are true.

Example 5 Prove that $a^2 \geq 0, \ \forall a \in R$.

We split into two cases, $a \geq 0$ or $a < 0$.

Case I : Let $a \geq 0$ (p)

$a.a \geq a.0$ (multiply both sides by $a \geq 0$)

$a^2 \geq 0$ (r)

So, if $a \geq 0$ then $a^2 \geq 0$.

Case II : Let $a < 0$ (q)

$a.a > a.0$ (multiply both sides by $a < 0$)

$a^2 > 0$, $a^2 \geq 0$ (r)

So, if $a < 0$ then $a^2 \geq 0$.

From both cases, we conclude that if a > 0, (p) then $a^2 \geq 0$ (r) and

If a < 0, (q) then $a^2 > 0$

So, $[\forall a \in R], a^2 \geq 0$. $(p \vee q) \to r$.

Example 6 Prove that if $a = 0$ or $b = 0$ then $ab = 0$.

Case I We Will prove that if $a = 0$, then $ab = 0$.

IF $a = 0$ (p)

$\therefore ab = 0.b = 0$ (r)

So, $p \to r$ is true.

Case II We Will prove that if $b = 0$, then $ab = 0$.

IF $b = 0$ (q)

$\therefore ab = a.0 = 0$ (r)

So, $q \to r$ is true.

So, from case I and case II , we conclude that if $a = 0$ or $b = 0$ then $ab = 0$ (Proof by cases).

NOTE. Proof by cases can be extended to more than two cases as follows.

$$(p_1 \vee p_2 \vee .... \vee p_n) \to r \equiv (p_1 \to r) \wedge (p_2 \to r) \wedge ... \wedge (p_n \to r)$$

EXERCISES

Use proof by cases to prove the following.

1. If x is a real number, then $|-x| = |x|$.
2. If x is a real number, then $|x^2| = |x|^2$.
3. For every real number x, $x \leq |x|$.
4. If x and y are real numbers, then $|xy| = |x| \cdot |y|$. Hint: One or both of x, y is zero or both are nonzero.
5. If $a > 0$, then $|x| < a$ iff $-a < x < a$.
6. If $a > 0$, then $|x| > a$ iff $x > a \vee x < -a$.
7. If x and y are real numbers, then $|x + y| \leq |x| + |y|$.

4. Proof by contrapositive

From logical equivalence $p \to q \equiv \sim q \to \sim p$, if it is difficult

to prove that $p \to q$ is true , we prove $\sim q \to \sim p$ is true as follows.

assume $\sim q$ is true

....

....

....

use $\sim q$, definitions, axioms, theorems and logical implication

deduce $\sim p$

That is $\sim q \to \sim p$ (true).

So, $p \to q$ is true. (by contrapositive)-

Example 7 Prove that for any integer a ,if a^2 is even, then a is even .

Let $p : a^2$ is even , $q : a$ is even

If $a \in I$ then a is even or odd.

$\sim p : a^2$ is odd, $\sim q : a$ is odd

We will prove that $\sim q \rightarrow \sim p$ is true.

Assume a is odd. $(\sim q)$

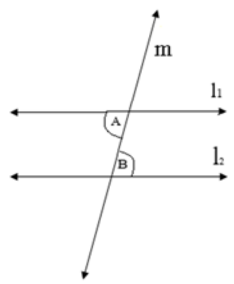
$\therefore a = (2k+1)^2 \; k \in I$

$a^2 = (2k+1)^2 = 4k^2 + 2k + 1 = 2(2k+1) + 1, \; (2k+1) \in I$

So, a^2 is odd $(\sim p)$. Therefore, $\sim q \rightarrow \sim p$ (true).

So, $p \rightarrow q$ is true (by contrapositive). That is, if a^2 is even , then a is even.

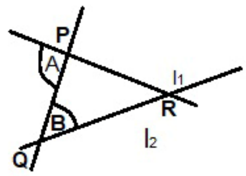
Example 8 From figure below, prove that if $m(\angle A) = m(\angle B)$ (p) then $l_1 \parallel l_2$



Prove : By using contrapositive, we will prove that if $l_1 \not\parallel l_2 \; (\sim q)$ then

$m(\angle A) \neq m(\angle B) \; (\sim p)$.

Assume $l_1 \not\parallel l_2 \quad (\sim q)$. Therefore, l_1 and l_2 intersect at R.



In ΔPQR, $m(\angle A) > m(\angle B)$ (Then.)

So, $m(\angle A) \neq m(\angle B) \quad (\sim p)$. So, $\sim q \rightarrow \sim p$ is true.

Therefore $q \rightarrow p$ is true.

That is if $m(A) = m(B)$, then $l_1 \parallel l_2$.

5. Proof by contradiction

From tautology $[\sim p \rightarrow (q \wedge \sim q)] \rightarrow p$ (proof by contradiction), we use it as a way to prove that a statement p is true as the following.

> Proof: assume $\sim p$ is true
>
> ………………………
> ………………………
> ……………………… } use, $\sim p$ definitions, axioms, previously prove theorem
>
> Therefore, $q \wedge \sim q$ (contradiction).
>
> That is $\sim p \rightarrow (q \wedge \sim q)$.
>
> So, we can conclude that p is true. (by proof by contradiction)

Example 9 : Prove that the sum of rational number X and irrational number Y is irrational .

Proof Let $z = x + y$ and p : Z is irrational

Assume Z is rational ($\sim p$). So, $z + (-y) = x$ (Theorem)

But $z + (-y)$ is rational. (Theorem)

So, X is rational. (q)

But, X is irrational (given). ($\sim q$).

Therefore, $q \wedge \sim q$, a contradiction. That is $\sim p \rightarrow (q \wedge \sim q)$

So, p is true (by proof by contradiction). That is $x + y$ is irrational.

Example 10 : Prove that for every $x > 0, x + \frac{1}{2} \geq 2.$

prove : Assume $x + \frac{1}{x} \ngeq 2 \quad (\sim p)$

So, $x + \frac{1}{x} < 2$

$x^2 + 1 < 2x$ (multiply both sides by x)

$x^2 - 2x + 1 < 0$

$$(x-1)^2 < 0 \quad (q)$$

a contradiction to the fact that

$$(x-1)^2 \geq 0, \text{ for all real } x \quad (\sim q)$$

So, $x + \dfrac{1}{x} \geq 2$ (proof by contradiction)

Example 11 : prove that $(p \wedge q) \rightarrow p$ is a tautology.

Prove : Assume $(p \wedge q) \rightarrow p$ is not a tautology $(\sim p)$

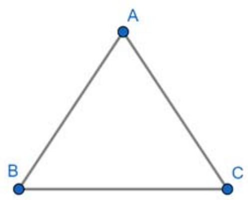
So, there is a case where $(p \wedge q)$ is true and p is false

So, there is a case

where p is true (r), q is true, p is not true $(\sim r)$. A contradiction

So, $(p \wedge q) \rightarrow p$ is a tautology.

Example 12 : Prove that in ΔABC, if AB = AC then $\hat{B} = \hat{C}$.



Given $AB = AC$ (q)

Assume $\hat{B} \neq \hat{C}$ $(\sim p)$

Therefore $\hat{B} > \hat{C}$ or $\hat{B} < \hat{C}$

Implies $AC > AB$ or $AC < AB$ $(\sim q)$

A contradiction to given

So, $\hat{B} = \hat{C}$ (p)

Exercises : Use prove by contradiction to prove the following.

1. If x is irrational any $y \neq 0$ is rational, prove that xy is irrational.
2. If $x \neq 0$ and $y \neq 0$, then $xy \neq 0$.
3. If $x > 0$, then $\dfrac{1}{x} > 0$. (use the theorem that 1 > 0)
4. If $x < 0$, then $\dfrac{1}{x} < 0$.
5. $\sqrt{2}$ is irrational. (The proof appears in many secondary math text book. Consult them.)

6. Prove by Mathematical Induction

The proof is use for proving that statement of the type $\forall n, P(n)$ or $\forall n[P(n)]$ is true where $P(n)$ is a statement concerning natural number n.

Example 13 Statement concerning $n \in N$

1. $P(n): 1+2+3+\ldots+n = \dfrac{n(n+1)}{2}, \forall n \in N$
2. $P_1(n): 1^2+2^2+3^2+\ldots+n^2 = \dfrac{n(n^2+1)(2n+1)}{6}, \forall n \in N$
3. $R(n): z^n \leq nz^n, n \in N$
4. $S(n):$ Given n points on the plane where no three of which are on the same line, there will be $\dfrac{n(n-1)}{2}$ line segments joining those n points.

One way to prove statement of this type, $\forall n, P(n)$ is true by mathematical induction.

The following is the mathematical induction which mathematicians accept as an axiom

$$P(1) \wedge \forall[P(k) \rightarrow P(k+1)] \rightarrow \forall n[P(n)]$$

If we can prove 2 steps :

1) $P(1)$ is true and
2) $\forall k[P(k) \rightarrow P(k+1)]$ is true ,

Then by Modus Ponens, we can deduce $\forall n[P(n)]$ is true.

Thus there were two steps in the proof $\forall n[P(n)]$;

1. Basis Step : Prove $P(1)$ is true.
2. Induction Step : Prove $\forall k[P(k) \rightarrow P(k+1)]$ is true.

That is, we prove P(1) and for every k, $P(k) \rightarrow P(k+1)$.

Then, we have an endless sequence of sentences.

$P(1)$ is true.

$$\left.\begin{array}{l} P(1) \to P(2) \\ P(2) \to P(3) \\ \quad . \\ \quad . \\ \quad . \\ P(k-1) \to P(k) \\ \quad . \end{array}\right\} \quad \forall k[p(k) \to P(k+1)]$$

The process becomes.

$$\frac{\begin{array}{l} P(1) \\ P(1) \to P(2), \end{array}}{\therefore P(2)} \qquad \frac{\begin{array}{l} P(2) \\ P(2) \to P(3), \end{array}}{\therefore P(3)} \qquad \frac{\begin{array}{l} P(3) \\ P(3) \to P(4) \end{array}}{\therefore P(4)}$$ ... and so on,

producing the endless sequence

$P(1), P(2), P(3), \ldots P(n), \ldots;$ That is, we have proved $\forall n[P(n)]$ is true.

Example 14 Use mathematical Induction to prove that

$$1+2+3+\ldots+n = \frac{n(n+1)}{2}, \forall n \in N.$$

Proof : Let $P(n): 1+2+3+\ldots+n^2 = \frac{n(n+1)}{2}$

Basis Step : $P(1)$: $1 = \frac{1(1+1)}{2}$

$= 1$

$\therefore P(1)$ is true.

Induction Step : Accept that $P(k)$ is true.

So, accept that $1+2+3+\ldots+k = \frac{k(k+1)}{2}$ is true. add (k+1) both sides.

$$1+2+3+...+k+(k+1)=\frac{k(k+1)}{2}+(k+1)$$

$$=\frac{(k+1)[(k+1)+1]}{2} \text{ is true .}$$

Therefore, $P(k+1)$ is true.

So, $1+2+3+...+n=\frac{n(n+1)}{2}, \forall n \in N$

Example 15 Prove that $1^2+2^2+3^2+...+n^2=\frac{n(n+1)(2n+1)}{6}, \forall n \in N$.

Proof : Let $P(n): 1^2+2^2+3^2+...+n^2=\frac{n(n+1)(2n+1)}{6}$

Basis Step : $P(1): 1^2=\frac{1(1+1)(2+1)}{6}$

$1=1$, So, $P(1)$ is true.

Induction Step : accept that $P(k)$ is true.

So, accept that $1^2+2^2+3^2+...+k^2=\frac{k(k+1)(2k+1)}{6}$ is true

Add $(k+1)^2$ both sides. So,

$$1^2+2^2+3^2+...+k^2+(k+1)^2=\frac{k(k+1)(2k+1)}{6}+(k+1)^2$$

$$=\frac{k(k+1)(2k+1)+6(k+1)^2}{6}$$

$$=\frac{(k+1)[k(2k+1)+6(k+1)]}{6}$$

$$=\frac{(k+1)(k+2)(2k+3)}{6}$$

$$=\frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

$$=\frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

$$1^2+2^2+3^2+...+k^2+(k+1)^2=\frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

$\therefore P(k+1)$ is true.

So, we have prove 1) $P(1)$ and 2) $P(k)\rightarrow P(k+1), \forall k\in N$.

Therefore, $P(n)$ is true, $\forall n\in N$. (by Mathematical Induction).

Example 16 Prove that for any n points on the plane where no three of which are on the same line, there will be $\frac{n(n-1)}{2}$ line segments joining those n points.

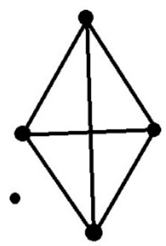
Proof : Let $P(n)$: for any n points on the plane where no three of which are on the same line, there will be $\frac{n(n-1)}{2}$ line segments joining those n points.

Basis Step : $P(1)$: number of line segments $=\frac{(1)(1-1)}{2}=0$

So, $P(1)$ is true

Induction Step : Assume, for any $k\in N$

P(k) : number of line segments = $\frac{k(k-1)}{2}$ is true.



Add one more point (P) satisfying the condition. So,

# of line segments $=\frac{k(k-1)}{2}+k$

$=\frac{(k+1)(k)}{2}$

So, $p(k+1)$ is true.

That is $\forall n\in N, P(n)$ is true .

> Note : $3|n(n^2+2)$ means $n(n^2+2)$ can be divided by 3
>
> $3|12,\ \ 3\nmid 11,\ \ 5|75,\ 7|21,\ 7\nmid 20$
>
> Definition : $a|b\Leftrightarrow b=ka,\ \ k\in I$

Example 17 : Prove that $3 | n(n^2+2), \forall n \in N$

Use mathematical induction .

Let $p(n)$: $3 | n(n^2+2), n \in N$

Basis Step : $p(1)$: $3 | 1(1^2+2)$ or $3|3$ (True)

So, $p(1)$ is true

Induction Step : accept that $p(k)$ is true. That is $3 | k(k^2+2)$.

Consider $(k+1)[(k+1)^2+2]$ = $(k+1)[k^2+2k+3]$

= $k^3+2k^2+3k+k^2+2k+3$

= $(k^3+2k)+3k^2+3k+3$

= $k(k^2+2)+3(k^2+k+1)$

$3 | k(k^2+2)$ and $3 | 3(k^2+k+1)$

So, $3 | (k+1)[(k+1)^2+2]$

Therefore $P(k+1)$ is true

That is $P(n)$ is true for all n in N

EXERCISES

✓Prove the following by mathematical induction.

1. $\forall n \in N$, $2^n > n$.
2. $\forall n \in N$, $3^n > n$.
3. $\forall n \in N$, $2 \leq 2^n$
4. $\forall n \in N$, $2n \leq 2^n$ Hint: Use Exercise 3.
5. $\forall n \in N$, $n < n+1$.
6. $\forall n \in N$, $2^{n-1} \leq n!$ Hint: $(k+1)! = (k+1)k!$
7. $\forall n \geq 4$, $2^n < n!$ Prove $2^n < n!$ false when $n \leq 3$.

7. Proving a statement in the form, $p \to (q \vee r)$.

We use equivalence $p \to (q \vee r) \equiv (p \wedge \sim q) \to r$.

Example 18 Prove that if $ab = 0$, then $a = 0$ or $b = 0$.

Proof : let $p: ab = 0,\ q: a = 0,$ and $r: b = 0$

Want to proof that $p \to (q \vee r)$ is true.

We will proof that its equivalent statement that $(p \wedge \sim q) \to r$ is true.

Assume 1) $ab = 0$ (p)------------------ (1)

And 2) $\sim q: a \neq 0$ $(\sim q)$

So, $\frac{1}{a}$ exists.

$$\frac{1}{a}(ab) = \frac{1}{a}(0) \qquad \text{(Multiply (1) both side by } \frac{1}{a}\text{)}$$

$$b = 0 \qquad \text{(r)}$$

So, $(p \wedge \sim q) \to r$ is true.

Therefore, $p \to (q \vee r)$ is true.

8. Proof by counter example

From a tautology of quantified statements.

$$\sim \forall x[P(x)] \equiv \exists x[\sim P(x)]$$

We use it to prove that $\forall x[P(x)]$ is false by proving that $\exists x[\sim P(x)]$ is true.

Example 19 : prove that the statement, all of prime numbers are odd, is false.

Solution : Let U : set of all prime numbers

and p(x) : x is odd, $x \in U$

So, $\forall x[P(x)]$: all prime numbers are odd

Consider $[p(2)]$: 2 is odd (F)

So, $\sim [p(2)]$ is true. Therefore, $\exists x[\sim P(x)]$ is true

So, $\sim \forall x[P(x)]$ is true and $\forall x[P(x)]$ is false.

So, all prime numbers are odd is false.

Exercise

Disprove the followings by counter example.

1. The sum of two irrational numbers is an irrational number.
2. The product of irrational numbers is an irrational number.
3. The product of a rational number and an irrational number is an irrational numbers.
4. Each square matrix has an multiplicative inverse.
5. For all real numbers x , the equation $\sqrt{-x-15} = 2$ has no solution.

9. Proof of Existence

From tautology of quantified statement, $p(a) \to \exists x[P(x)]$ (T)

That is when p(a) is true, then $\exists x[P(x)]$ is true.

Example 20 : Prove that in the set of real numbers, there exist a number which itself is the inverse for addition.

Solution : Let P(a) : a is itself inverse for addition

Want to prove that $\exists x[P(x)]$ is true.

Consider the number 0. It is true that 0 + 0 = 0.

So, 0 is itself inverse for addition.

Therefore, $[P(0)]$ is true.

That is $\exists x[P(x)]$ is true.

Exercise

Prove the followings:

1. There is a real number x such that $5 + \sqrt{x+7} = x$.
2. There exists a positive integer x such that $90 < x^2 < 110$.
3. For any real number x, there exists a real number y such that x + y = 0.
4. There exits only one integer x such that x + 3 = 10.
5. For any real number y, there exists only one real number x such that x + y = y.