Proof Techniques

- Proof is a kind of demonstration to convince that the given mathematical statement is true.
- The statement which is to be proved is called **theorem**. Once a particular theorem is proved then it can be used to prove further statements.
- The theorem is also called as **Lemma**.
- The proof can be a deductive proof or inductive proof.
- The deductive proof consist of sequence of statements given with logical reasoning.
- The inductive proof is a recursive kind of proof which consists of sequence or parameterized statements that use the statement itself or the statement with lower values of its parameter.
- Various methods of proofs are-
    - Proof by contradiction
    - Proof by mathematical induction
    - Direct proofs
    - Proof by counter example
    - Proof by contraposition

Proof by Contradiction

- In this type of proof, for the statement of the form if A then B.
- We start with statement A is not true and thus by assuming false A, we try to get the conclusion of statement B.
- When it becomes impossible to reach to statement B, we contradict our self and accept that A is true.
- For example,
- Prove $P \cup Q = Q \cup P$

Prove $P \cup Q = Q \cup P$

- Proof
  - Initially we assume that $P \cup Q = Q \cup P$ is not true.
    i.e. $P \cup Q \neq Q \cup P$
  - Now consider that x is in Q, or x is in P. hence we can say x is in $P \cup Q$ (according to definition of union)
  - But this also implies that x is in $Q \cup P$ according to definition of union.
  - Hence the assumption which we made initially is false.
  - Thus $P \cup Q = Q \cup P$ is proved.

Prove by contradiction. There exist two irrational numbers x and y such that x^y is rational.

- Solution:
- An irrational number is any number that cannot be expressed as a/b where a and b are integers and value b is non zero. To prove that x^y is rational when x and y are irrational we have two choices –
- 1. x^y is rational
- 2. x^y is irrational
- Case 1 : $\sqrt{2}$ is a rational number then $x = \sqrt{2}$ and $y = \sqrt{2}$ is a irrational number, hence there exists teo irrational numbers x and y such that x^y is rational

- Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. We will consider two irrational numbers.
  - $X = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$
  - $X^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$
  - $= (\sqrt{2})^{\sqrt{2}\sqrt{2}}$
  - $= (\sqrt{2})^{2}$
  - $= 2$
  - Which is a rational number. Here we have x and y as irrational numbers but 2 as rational number.
  - From the two cases it it proved that if x and y are two irrational numbers then x^y is a rational number.

Proof by Mathematical Induction

- Inductive proofs are special proofs based on some observations.
- It is used to prove recursively defined objects. This type of proof is also called as proof by mathematical induction.
- The proof by mathematical induction can be carried out using following steps:
  - Basic: in this step, we assume the lowest possible value. This is an initial step in the proof by mathematical induction.

    For example, we can prove that the result is true for n = 0 or n = 1
  - Induction Hypothesis: in this step, we assign value of n to some other value k. that mean, we will check whether the result is true for n – k or not.
  - Inductive Step: in this step, if n = k is true then we check whether the result is true for n = k + 1 or not.
  - If we get the same result at n = k + 1 then we can state that given proof is true by principle of mathematical induction

Example : 1
Prove: $1 + 2 + 3 \dots + n = n (n + 1) / 2$

- Solution: initially,
- 1) Basis of induction –
- Assume, $n = 1$ then
- L. H. S. $= n = 1$
- R. H. S. $= n (n + 1) / 2 = 1 (1 + 1) / 2 = 2 / 2 = 1$
- 2) Induction hypothesis –
- Now we will assume $n = K$ and will obtain the result for it. The equation then becomes,
- $1 + 2 + 3 + \dots + K = K (K + 1) / 2$

- 3) Inductive step –
- Now we assume that equation is true for n = K and we will then check if it is also true for n = K +1 or not.
- Consider the equation assuming n = K + 1
- L. H. S. = $\underline{1 + 2 + 3 + \ldots + K} + K + 1$
- $= K (K + 1) / 2 + K + 1$
- $= K (K + 1) + 2 (K + 1) / 2$
- $= (K + 1) (K + 2) / 2$
- i.e. $= (K + 1) (K + 1 + 1) / 2$
- = R. H. S.

Example 2:
Prove : $n! >= 2^{n-1}$

- Solution: Consider,
- 1) Basis of induction -
- Let n = 1 then
- L. H. S. = 1
- R. H. S. = $2^{1-1} = 2^{0} = 1$
- Hence, $n! >= 2^{n-1}$ is proved.

- 2) Induction hypothesis-
- Let n = n +1 then
- $k! = 2^{k-1}$ where k >= 1
- Then
- $(k+1)! = (k+1)\,k!$ By definition of n!
- $= (k+1)\,2^{k-1}$
- $= 2 * 2^{k-1}$
- $= 2^{k}$
- Hence, $n! >= 2^{n-1}$ is proved.

Direct Proofs

- In direct proof, the intended proof can be proved by basic principle or axiom.
- Example - Prove that the negative of any even integer is even.
- Solution : to prove this, let n be any positive even number. Hence we can write n as
- $n = 2m$ where m can be any number
- If we multiply both side by -1, we get
- $-n = -2m$
- $-n = 2(-m)$
- Multiplying any number by 2 makes it an even number.
- Hence, -n is even.
- Thus proves that the negative of any even integer is even.

Proof by Counter-example

- In order to prove certain statements, we need to see **all possible conditions** in which that statement remains true.
- There are some situations in which the statement can not be true.
- **For example: Theorem**: there is no such pair of integers such that
- a mod b = b mod a
- **Proof**: consider a = 2 and b =3 then 2 mod 3 $\neq 3\ mod\ 2$
- Thus the given pair is true for any pair of integers but
- if a =b then naturally a mod b = b mod a
- Thus we need to change the statement slightly. We can say
- a mod b = b mod a, when a =b
- This type of proof is called **counter example**.
- Such proof is true only at some specific condition.

Proof by Contraposition

- This is a technique of proof in which A $\longrightarrow$ B is true if ~ A $\longrightarrow$ ~ B.
- If negative statement of given statement is true then the given statement becomes automatically true.
- Example: prove by contraposition that x + 8 is odd.
- Solution: Step 1: we assume that x is not odd
- Step 2: that means x is even. By definition of even numbers 2 * any number = even number
- x = 2 * m where m can be any number
- Step 3: we can write x + 8 as 2 * m + 8 = 2 (m + 4) = even number
- Thus x + 8 is even. That means (x + 8) is not odd.
- From step 1 and 3, we can state that if x is not odd then (x +8) is also not odd.
- Hence by contraposition theorem, we can say that x + 8 is odd if x is odd.