01/07/22

** Fundamental Theorem on Equivalence relation:

Statement: If A is any non-empty set, then.

i) Any equivalence relation R on A induces partition of A
ii) Any partition of A gives rise to an equivalence relation R on A.

Proof:

i) Given that R is an equivalence relation,
⇒ R is reflexive, symmetric and transitive.
Let us consider a set P of all distinct equivalence classes.
ie $P = \{[a] : a \in A\}$.
where $[a] = \{x : xRa\}$.
We need to prove that, P is a partition of A, it means that P has to satisfy two condition of difinition of partition.
1) Since R is reflexive relation
⇒ $aRa \quad \forall a \in A$
⇒ $a \in [a] \quad \forall a \in A$.
⇒ Union of all equivalence class gives A.
⇒ $A = \bigcup_{a \in A} [a]$.

2) We know that,
"Any two equivalence classes of A are either identical or disjoint".
Since P has distinct equivalence class, Intersection of 2 distinct equivalence classes is empty.
∴ P is partition of set A.

ii) Suppose $P = \{A_1, A_2, A_3, \ldots A_n\}$ is a partition of A. Define a relation R on set A, such that aRb if and only if, (a,b) ∈ same block of P.

We need to prove that R is equivalence relation.

1) Reflexive relation:

Let us take element $a \in A$

$\Rightarrow a \in A_i$, for only one $i = 1, 2, 3 \ldots n$

$\Rightarrow aRa$, as 'a' belongs to same block.

$\Rightarrow aRa \; \forall \; a \in A$

∴ R is reflexive relation.

2) Symmetric relation:

If $aRb \Rightarrow a, b \in$ same block.

$\Rightarrow b, a \in$ same block.

$\Rightarrow bRa$

∴ R is symmetric relation

3) Transitive Relation:

If aRb and bRc

$\Rightarrow a, b \in$ same block & $b, c \in$ same block.

$\Rightarrow a, b, c \in$ same block

$\Rightarrow a, c \in$ same block

$\Rightarrow aRc$.

∴ R is transitive relation.

∴ R is an equivalence relation.

* Examples:

(1) For the equivalence relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)\}$ defined on set $A = \{1,2,3,4\}$. Determine the partition induced by R.

Sol^n: Let $A = \{1,2,3,4\}$.

Equivalence relation on R is:

$\{(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)\}$.

Equivalence class of set A is are,

$[a] = \{x : xRa\} = \{x : (x,a) \in R\}$.

$[1] = \{x : (x,1) \in R\} = \{1,2\}$

$[2] = \{x : (x,2) \in R\} = \{1,2\}$

$[3] = \{x : (x,3) \in R\} = \{3,4\}$

$[4] = \{x : (x,4) \in R\} = \{3,4\}$.

Partition induced by R is

$P = \{[1], [3]\} = \{\{1,2\}, \{3,4\}\}$.

04/06/22

(2) For a set $A = \{1,2,3, \cdots\}$ consider the relation R on A defined as aRb iff if and only if $a-b$ is ~~defined~~ divisible by 5. Find the partition of A induced by R.

Sol^n: Let $A = \{1,2,3, \cdots\}$.

$R = \{(a,b) : (a-b) \text{ is divisible by } 5\}$

$R = \{(a,b) : 5 \mid (a-b)\}$.

i) Reflexive Relation:

aRa as $5 \mid (a-a)$, $\forall a \in A$.

$(a,a) \in R$

$\therefore$ R is reflexive relation.

ii) Symmetric Relation:

If $aRb \Rightarrow 5 \mid a-b$

$\Rightarrow 5 \mid -(b-a)$

$\Rightarrow 5 \mid (b-a)$.

$\Rightarrow bRa$.

$\therefore$ R is symmetric Relation

iii) Transitive relation.

If aRb and bRc

$\Rightarrow 5 \mid (a-b)$ and $5 \mid (b-c)$.

$\Rightarrow 5 \mid (a-b)+(b-c)$

$\Rightarrow 5 \mid (a-b+b-c)$

$\Rightarrow 5 \mid (a-c)$

$\therefore aRc$

$\therefore$ R is transitive Relation

$\therefore$ R is an equivalence Relation.

Now, equivalences classes of set A are,

$[a] = \{x : xRa\} = \{x : (x,a) \in R\}$

$[a] = \{x : 5 \mid (x-a)\}$

$[a] = \{x : (x-a) = 5n\}$, $\forall n \in Z$, provided $x \in A$.

$[a] = \{x : x = 5n+a\}$, $\forall n \in Z$, provided $x \in A$.

$[a] = \{5n+a\}$, $\forall n \in Z$, provided $5n+a \in A$.

$[a] = \{5n+1\}$, $\forall n \in Z$, provided $(5n+1) \in A$.

$[1] = \{1, 6, 11, 16, 21, 26, 31, \ldots\}$ $(\because \forall n = 0, 1, 2 \ldots)$

$[2] = \{5n+2\}$, $\forall n \in Z$, provided $(5n+2) \in A$.

$[2] = \{2, 7, 12, 17, 22, 27, \ldots\}$

$[3] = \{5n+3\}$, $\forall n \in Z$, provided $(5n+3) \in A$.

$[3] = \{3, 8, 13, 18, 23, 28, \ldots\}$

$[4] = \{5n+4\}$, $\forall n \in Z$, provided $(5n+4) \in A$

$[4] = \{4, 9, 14, 19, 24, 29, \ldots\}$

$[5] = \{5n+5\}$, $\forall n \in Z$, provided $(5n+5) \in A$.

$[5] = \{5, 10, 15, 20, 25, 30, \ldots\}$

$\therefore [1], [2], [3], [4]$ & $[5]$ are the only distinct equivalence classes of set A induced by the relation R.

∴ Partition of set A induced by relation R is,
$R = \{[1], [2], [3], [4], [5]\}$.

(3) On the set of all integers Z, the relation R is defined by aRb if and only if $a^2 - b^2$ is an even integer.

i) Show that R is an equivalence relation.

ii) Find the partition of A induced by R.

Sol:- Let $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$.

or $I = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

$R = \{(a,b) : (a^2 - b^2)$ is an even integer$\}$.

$R = \{(a,b) : (a^2 - b^2)$ is divisible by $2\}$

$R = \{(a,b) : 2 | (a^2 - b^2)\}$.

i) Reflexive Relation:

aRa as $2 | (a^2 - a^2)$ $\forall$ $a \in \mathbb{Z}$.

R is reflexive relation.

ii) Symmetric Relation

If $aRb \Rightarrow 2 | (a^2 - b^2)$

$\Rightarrow 2 | -(b^2 - a^2)$

$\Rightarrow 2 | (b^2 - a^2)$

$\Rightarrow bRa$

∴ R is symmetric relation.

iii) Transitive relation

If aRb and bRc

$\Rightarrow 2 | (a^2 - b^2)$ and $2 | (b^2 - c^2)$

$\Rightarrow 2 | (a^2 - b^2) + (b^2 - c^2)$

$\Rightarrow 2 | (a^2 - b^2 + b^2 - c^2)$

$\Rightarrow 2 | (a^2 - c^2)$

$\Rightarrow aRc$

∴ R is transitive relation

∴ R is equivalence relation.

Now, equivalence class of set $\mathbb{Z}$ are,

$[a] = \{x : xRa\} = \{x : (x,a) \in R\}$.

$[a] = \{x : 2 \mid (x^2 - a^2)\}$.

$[a] = \{x : (x^2 - a^2) = 2n\}$, $\forall n \in \mathbb{Z}$, provided $x \in \mathbb{Z}$.

$[a] = \{x : x^2 = 2n + a^2\}$, $\forall n \in \mathbb{Z}$, provided $x \in \mathbb{Z}$.

$[a] = \{x : x = \pm\sqrt{2n+a^2}\}$, $\forall n \in \mathbb{Z}$, provide $x \in \mathbb{Z}$.

$[a] = \{-\sqrt{2n+a^2}, \sqrt{2n+a^2}\}$, $\forall n \in \mathbb{Z}$, provided $\sqrt{2n+a^2} \in \mathbb{Z}$.

$[1] = \{-\sqrt{2n+1}, \sqrt{2n+1}\}$, $\forall n \in \mathbb{Z}$, provided $\sqrt{2n+a^2} \in \mathbb{Z}$.

$[1] = \{-1, 1, -3, 3, -5, 5, -7, 7, \ldots\}$.

$[1] = \{\ldots\ldots -7, -5, -3, -1, 1, 3, 5, 7, \ldots\ldots\}$

$[2] = \{-\sqrt{2n+4}, \sqrt{2n+4}\}$, $\forall n \in \mathbb{Z}$, provided $\sqrt{2n+4} \in \mathbb{Z}$.

$[2] = \{0, -2, 2, -4, 4, -6, 6, \ldots\}$

$[2] = \{\ldots -6, -4, -2, 0, 2, 4, 6 \ldots\}$.

$\therefore$ $[1]$, $[2]$ are the only 2 distinct equivalence classes of set $\mathbb{Z}$ induced by the relation R.

$\therefore$ Partition of set $\mathbb{Z}$ induced by relation R is,

$R = \{[1], [2]\}$.

6/07/22

④ If $A = \{1,2,3,4,5\}$ and R is the equivalence relation on A that induces the partition $A = \{1,2\} \cup \{3,4\} \cup \{5\}$, then find R.

Sol^n: Let $A = \{1,2,3,4,5\}$.

Partition of A is

$P = \{\{1,2\}, \{3,4\}, \{5\}\}$.

$\therefore$ Equivalence relation R on A by the above partition P is,

$R = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,4), (4,3), (5,5)\}$.

[$\because$ aRb if & only if $(a,b) \in$ same block).

★ Partial Ordering Relation:

A relation R, on set A is said to be partial ordering relation, if it satisfies reflexive, anti-symmetric and transitive relation.

★ Partial ordered Set (or) Poset:

A set A, with partial ordering relation R, defined on it is called Partial ordered set of A (or) Poset of and is denoted by (A, R).

★ Hasse Diagram:

The Hasse diagram of a finite partial ordered set A (poset A) is a diagram whose vertices represent elements of A. If (a, b) ∈ A and b is immediate successor of a (a < b), then an edge (line) is drawn directed from a to b by placing element b at a higher level than element b.

To draw Hasse Diagram of Poset (A, R), a digraph of the given partial ordering relation R is drawn and remove the following:

1) All the loops
2) All the edges implied by transitive relation.

★ Examples:

(1) Let A = {1, 2, 3, 5, 6, 10, 15, 30} and R be the relation on A defined by xRy if and only if x divides y. Verify R is partial ordering relation and draw its Hasse diagram

Sol^n: Let A = {1, 2, 3, 5, 6, 10, 15, 30}.

R = {(x, y) : x divides y}

R = {(x, y) : x/y}

i) Reflexive Relation

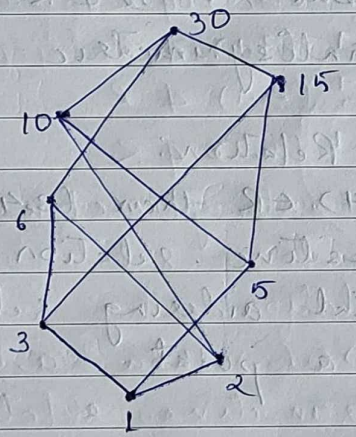
xRx as x/x, ∀ x ∈ A

∴ R is reflexive.

ii) Anti-Symmetric:
whenever $x \neq y$ and xRy, then yRx.
$\therefore$ R is anti-symmetric relation.

iii) Transitive relation:
If xRy and yRz.
$\Rightarrow$ $x|y$ and $y|z$.
$\Rightarrow$ $x|z$.
$\Rightarrow$ xRz.
$\therefore$ R is transitive relation.
$\therefore$ R is partial ordering relation
$\therefore$ (A, R) is poset.

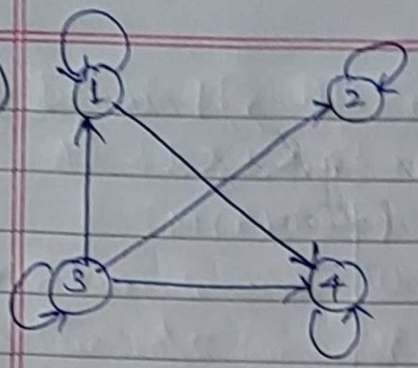
Hasse diagram: of (A, R) is



08-04-22

② The diagraph of a relation defined on set $A = \{1, 2, 3, 4\}$ in as shown below, verify that (A, R) is a poset and draw corresponding Hasse diagram.

a)



Sol:- Relation R on set $A = \{1,2,3,4\}$ defined by above diagraph is,

$R = \{(1,1), (1,4), (2,2), (3,1), (3,2), (3,3), (3,4), (4,4)\}$.

i) Reflexive relation:

$(1,1), (2,2), (3,3), (4,4) \in R$

$\therefore$ R is reflexive.

ii) Antisymmetric relation:

Since $(1,4) \in R$ but $(4,1) \notin R$

$(3,1) \in R$ but $(1,3) \notin R$

$(3,2) \in R$ but $(2,3) \notin R$

$(3,4) \in R$ but $(4,3) \notin R$.

$\therefore$ R is an antisymmetric relation

iii) Transitive Relation:

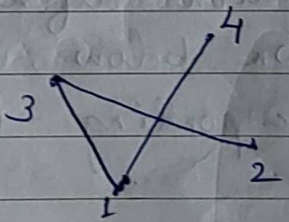
$(3,1), \in R$ & $(1,4) \in R$ then $(3,4) \in R$.

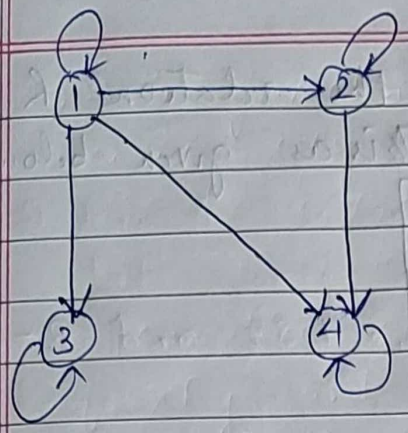
$\therefore$ R is transitive relation.

$\therefore$ R is partial ordering relation.

(A,R) is a poset

Hasse diagram is;



b) 

Sol:- Relation R on set A = {1, 2, 3, 4} defined by above diagraph is,

R = {(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)}

i) Reflexive Relation:

(1,1), (2,2), (3,3), (4,4) ∈ R

∴ R is Reflexive.

ii) Antisymmetric Relation:

(1,2) ∈ R but (2,1) ∉ R

(1,3) ∈ R but (3,1) ∈ R

(1,4) ∈ R but (4,1) ∉ R

(2,4) ∈ R but (4,2) ∉ R

∴ R is an anti-symmetric relation.

iii) Transitive Relation:

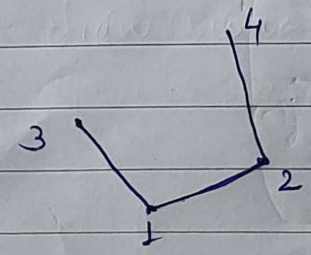
(1,2) ∈ R & (2,4) ∈ R then (1,4) ∈ R

∴ R is transitive relation.

∴ R is partial ordered relation

(A, R) is a poset

Hasse Diagram is,



(3) Draw the Hasse diagram of the relations R on $A = \{1,2,3,4,5\}$ whose matrix is as given below:

$$M(R) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Sol^{n}: Relation R on set $A = \{1,2,3,4,5\}$ defined by above matrix is;

$R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (2,2), (3,3), (4,4), (5,5)\}$

i) Reflexive Relation:

$(1,1), (2,2), (3,3), (4,4), (5,5) \in R$

$\therefore$ R is reflexive relation.

ii) Anti-symmetric Relation:

Since,

$(1,2) \in R$ but $(2,1) \notin R$

$(1,3) \in R$ but $(3,1) \notin R$

$(1,4) \in R$ but $(4,1) \notin R$

$(1,5) \in R$ but $(5,1) \notin R$.

$\therefore$ R is an antisymmetric Relation.

iii) Transitive Relation:

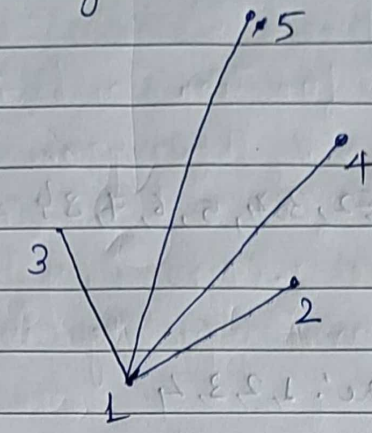
$(a,a) \in R$ & $(a,b) \in R$ then $(a,b) \in R$.

$\therefore$ R is transitive relation.

$\therefore$ R is partial ordering relation.

(A,R) is a poset

Hasse diagram is,



* Lower Bound:
Let A be the poset and B is a subset of A. Then an element $a \in A$ is called lower bound of B if $a \leq b$, $\forall b \in B$.

* Upper Bound:
Let A be the poset and B is a subset of A. Then an element $a \in A$ is called upper bound of B if $a \geq b$, $\forall b \in B$.

* Greatest Lower Bound (GLB):
An element 'a' is called greatest lower bound of subset B of a poset A. If 'a' is a lower bound that is greater than any other lower bounds of B.

* Least Upper Bound (LUB):
An element 'a' is called least upper bound of subset B of a poset A. If 'a' is a upper bound that is less than any other upper

bounds of B.

* Example:

(1) Consider a set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and $B = \{4, 5, 6\}$ is the subset of A.

Sol: Lower Bound of B are: 1, 2, 3, 4
Upper Bound of B are: 6, 7, 8.

Greatest lower Bound of B: 4
least upper Bound of B: 6.

* Lattice:

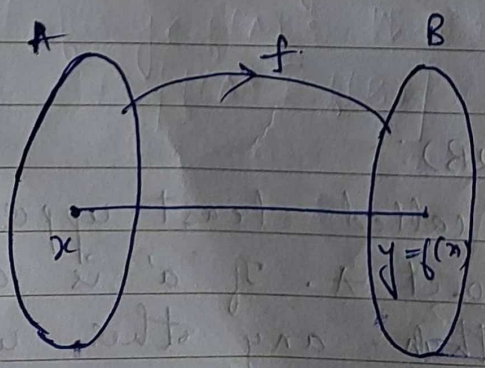
A partial ordering set (A, R) in which every pair of elements has both least upper bound and greatest lower bound. is called lattice.

* Functions:

A relation R from non empty set A to non empty set B is said to be a function (mapping) f from A to B, if each element of A has unique image (relation) in B.

And function is denoted by:

$f: A \rightarrow B$



01/07/22.

★ Types of Functions:

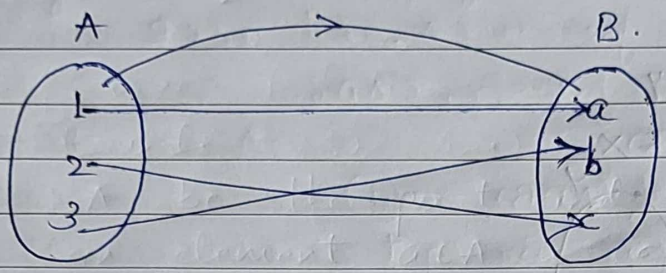
1) One-one function / One-to-one function / Injective

A function $f: A \to B$ is said to be one-one if distinct elements of A should have distinct images in B.

i.e if $x_1 \neq x_2 \in A$, then $f(x_1) \neq f(x_2)$.

or: if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

eg:

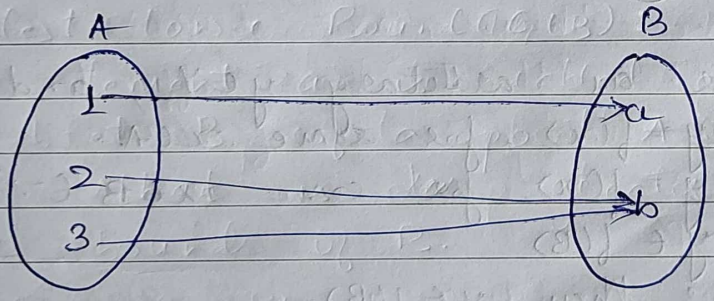


2) Onto function / surjective:

A function $f: A \to B$. is said to be onto if every element $y \in B$ should be the image of atleast one element $x \in A$.

Note: If a function f is onto, then co-domain and range are equal.

eg:



3) Bijective Function:

A function $f: A \to B$ is said to be bijective if f is bothe one-one and onto.

★ Properties of Function:

Theorem-1:

Let $f: X \to Y$ be a function and A and B are non-empty subsets of X. Then prove that,

i) If $A \subseteq B$, then $f(A) \subseteq f(B)$.

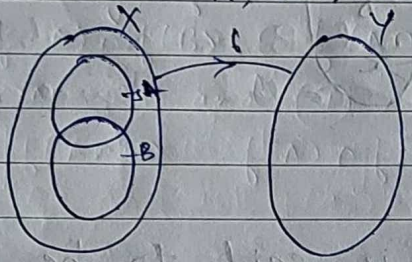
ii) $f(A \cup B) = f(A) \cup f(B)$.

iii) $f(A \cap B) = f(A) \cap f(B)$, and equality holds if f is one-one function.

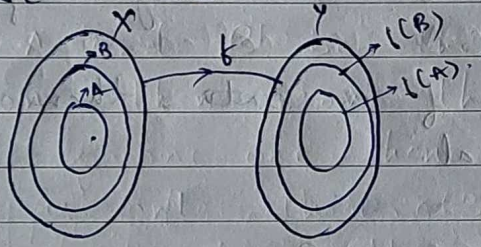
Proof:

Let $f: X \to Y$

Given that $A, B \subseteq X$.



i) Suppose $A \subseteq B$.



Let us consider an arbitary $y \in Y$, and if $y \in f(A)$,

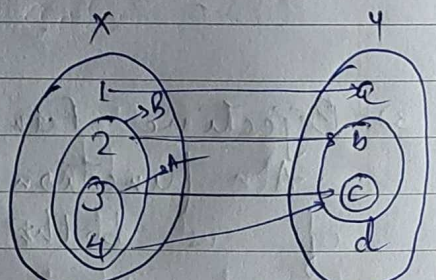
$y \in f(A) \Rightarrow y = f(x)$, for some $x \in A$.

$\Rightarrow y = f(x)$, for some $x \in B$ ($\because A \subseteq B$)

$\Rightarrow y \in f(B)$

$\therefore$ if $y \in f(A)$, then $y \in f(B)$.

$\therefore \boxed{f(A) \subseteq f(B)}$



$c \in f(A) \Rightarrow c = f(x)$, for some $x \in A$

3,4.

ii) If $y \in f(A \cup B) \Rightarrow y = f(x)$ for some $x \in A \cup B$.

$\rightarrow y = f(x)$ for some $x \in A$ or $x \in B$.

$\rightarrow (y = f(x)$, for some $x \in A)$ or $(y = f(x)$, for some $x \in B)$

$\Rightarrow y \in f(A)$ or $y \in f(B)$

$\Rightarrow y \in f(A) \cup f(B)$

$\Rightarrow f(A \cup B) \subseteq f(A) \cup f(B)$ — (1)

Next, we know that,

$A \subseteq A \cup B$ and $B \subseteq A \cup B$.

By the result (i)

$f(A) \subseteq f(A \cup B)$ and $f(B) \subseteq f(A \cup B)$

$\therefore f(A) \cup f(B) \subseteq f(A \cup B) \cup f(A \cup B)$

$f(A) \cup f(B) \subseteq f(A \cup B)$ — (2)

from (1) and (2), we get

$\boxed{f(A \cup B) = f(A) \cup f(B).}$

iii) If $y \in f(A \cap B) \Rightarrow y = f(x)$ for some $x \in A \cap B$

$\Rightarrow y = f(x)$ for some $x \in A$ and $x \in B$.

$\Rightarrow (y = f(x)$, for some $x \in A)$ and $(y = f(x)$, for some $x \in B)$

$\Rightarrow y \in f(A)$ and $y \in f(B)$

$\Rightarrow y \in f(A) \cap f(B)$

$\Rightarrow f(A \cap B) \subseteq f(A) \cap f(B)$ — (3)

Next, we know that,

$A \subseteq A \cap B$ and $B \subseteq A \cap B$.

By result (i)

$f(A) \subseteq f(A \cap B)$ and $f(B) \subseteq f(A \cap B)$.

$\therefore f(A) \cap f(B) \subseteq f(A \cap B) \cap f(A \cap B)$

$f(A) \cap f(B) \subseteq f(A \cap B)$. — (4)

∴ By (3) & (4)

$$\boxed{f(A \cap B) = f(A) \cap f(B)}$$

Given that f is one-one function.

If $y \in f(A) \cap f(B) \Rightarrow y \in f(A)$ and $y \in f(B)$

$\Rightarrow (y = f(x_1)$, for some $x_1 \in A)$ and $(y = f(x_2)$, for some $x_2 \in B)$

$\Rightarrow y = f(x_1) = f(x_2)$, for $x_1 \in A$ & $x_2 \in B$.

$\Rightarrow x_1 = x_2$ as f is one-one function.

$\Rightarrow y = f(x_1)$, for $x_1 \in A$ and $x_1 \in B$.

$\Rightarrow y = f(x_1)$, for $x_1 \in A \cap B$.

$\Rightarrow y \in f(A \cap B)$.

$\therefore f(A) \cap f(B) \subseteq f(A \cap B)$ — (4)

from (3) and (4), we get

$$\boxed{f(A \cap B) = f(A) \cap f(B)}$$

11-07-22:

Theorem-2:

Let A and B be the finite set, and $f: A \to B$ be a function. Then prove that:

i) If f is one-one, then $n(A) \leq n(B)$.

ii) If f is onto, then $n(B) \leq n(A)$.

iii) If f is bijective, then $n(A) = n(B)$.

iv) If $n(A) > n(B)$ then atleast two different elements of A have the same image under f.

Proof:

Let $f: A \to B$.

Let us consider $A = \{a_1, a_2, a_3, \ldots a_n\}$.

and $B = \{b_1, b_2, b_3, \ldots b_m\}$

$\therefore n(A) = n$ $\quad n(B) = m$.

i) Suppose f is one-one.
→ Each distinct elements of A must have distinct images in B.
⇒ B must have atleast n elements.
⇒ $a_1, a_2, \ldots a_n \in A$ must have images $f(a_1), f(a_2), \ldots f(a_n)$
⇒ $n(B) \geq n$.
⇒ $n(B) \geq n(A)$ $(\because n(A) = n)$
⇒ $\boxed{n(A) \leq n(B)}$ — (a).

ii) Suppose f is onto.
→ Each element of B is the image of atleast one element of A.
⇒ B A must have atleast m elements.
⇒ $n(A) \geq m$.
⇒ $n(A) \geq n(B)$ $(\because n(B) = m)$.
⇒ $\boxed{n(A) \geq n(B)}$ — (b)

iii) Suppose f is bijective.
From the result (i) & (ii), we get
$\boxed{n(A) = n(B)}$.

iv) Suppose $n(A) > n(B)$.
By the contrapositive of the result (i), we get
If $n(A) > n(B)$, then f is not one-one.
⇒ There are atleast 2 elements $x_1 \neq x_2 \in A$, have the same image y in B.
⇒ $y = f(x_1)$ & $y = f(x_2)$ for $x_1 \neq x_2 \in A$.
It means that atleast two elements of A have the same image under f.

Theorem-3:
Suppose A and B are finite sets having same number of elements and $f: A \to B$ is a function. Then f is one-one if and only if f is onto.

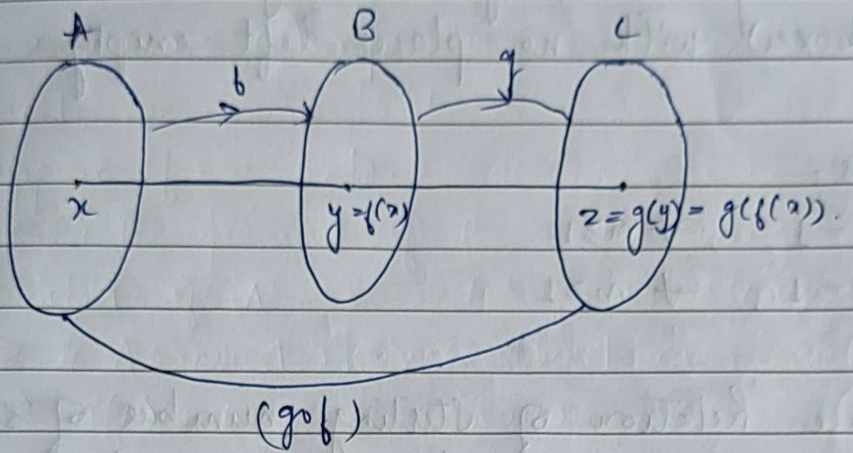
Proof:
Let $f: A \to B$
Given that, number of elements in A and B are same.
$\therefore \boxed{n(A) = n(B) = n}$.
Let $A = \{a_1, a_2, \cdots a_n\}$ & $n(A) = n$.
Suppose f is one-one,
$\Rightarrow$ Each element $a_1, a_2, \cdots a_n \in A$ must have distinct images $f(a_1), f(a_2), \cdots f(a_n)$.
$\Rightarrow$ The set of these images constitute a range of 'f' and it is denoted by $f(A)$.
$\Rightarrow f(A) = \{f(a_1), f(a_2), f(a_3), \cdots f(a_n)\}$.
$\Rightarrow n(f(A)) = n$.
$\Rightarrow \boxed{n(f(A)) = n(B)}$ $(\because n(B) = n)$
$\therefore$ f is onto.

Conversely,
Suppose f is onto,
$\Rightarrow$ co-domain (B) and range set ($f(A)$) have same number of elements.
$\Rightarrow B = f(A) = \{f(a_1), f(a_2), \cdots, f(a_n)\}$ & $n(B) = n$.
$\Rightarrow f(a_1), f(a_2) \cdots f(a_n)$ are distinct elements.
$\therefore$ f is one-one

★ Composition of Functions:

Let $f: A \to B$ and $g: B \to C$ be two functions. Then the compositions of two functions f and g is denoted by gof. is defined by the function $gof: A \to C$ such that, gof

$$gof(x) = g(f(x)), \quad \forall\ x \in A.$$



★ Invertible Function:

A function $f: A \to B$ is said to be invertible if there exists a function $g: B \to A$ such that $(gof)(x) = x$ & $(fog)(y) = y$. Then the function g is called inverse of function f and it is denoted by f^{-1}.

Unit-3:

ADVANCED COUNTING TECHNIQUE

13/07/22

* Sterling Number of Second Kind:
Sterling number of second kind is the number of partition of set of size 'n' into 'n' non-empty subsets.
(OR)
Sterling number of second kind is the number of possible ways to assign 'n' objects into 'n' identical places (boxes) with no place left empty.

* Properties:
1) $S(n,1) = 1$, $\forall\, n \geq 1$
2) $S(n,n) = 1$, $\forall\, n \geq 1$

* Recurrence Relation of Sterling number of second kind
If 'n' objects are kept in 'n' identical places with no place left empty and $n \geq n$, then Recurrence Relation of sterling number of second kind is:

$$\boxed{S(n,n) = S(n-1, n-1) + nS(n-1, n)}$$

Proof:
Let $a_1, a_2, a_3 \ldots a_n$ are n objects.
Then $S(n,n)$ is the count of number of ways of distributing n-objects in n-identical places.

$\Rightarrow$ There are $S(n-1, n-1)$ ways of distributing (assigning) $a_1, a_2, \ldots, a_{n-1}$ ($n-1$ objects) into $(n-1)$ places by keeping a_n^{th} object in n^{th} place.

Next, assigning $a_1, a_2, \ldots a_{n-1}$ objects in all n-places has $S(n-1, n)$ ways. and placing a_n^{th} object in n-places has n- no of ways.

$\therefore S(m-1, n)$ is total no of ways in which a_m^{th} object is kept in n-places.

$\therefore$ Total no of ways of assigning m-objects in n-places is,

$$\boxed{S(m,n) = S(m-1, n-1) + n\,S(m-1, n)}$$

★ Table consisting of possible Sterling Number of second kind:

$m=1$	1				
$m=2$	1	1			
$m=3$	1	3	1		
$m=4$	1	7	6	1	
$m=5$	1	15	25	10	1
⋮	⋮	⋮	⋮	⋮	⋮

★ General Formula to find Sterling No of second Kind:

If 'm' objects are kept in 'n' identical cases, then, we have the following formula to find Sterling no of second kind:

$$\boxed{S(m,n) = \frac{1}{n!}\sum_{K=0}^{n}(-1)^K\, {}^nC_K\,(n-K)^m}$$

★ General Formula to find no of onto functions:

Let A and B be two finite sets with $n(A) = m$ & $n(B) = n$, where $m \geq n$. Then number of onto functions from A to B is denoted by $P(m,n)$ and given by the formula

$$P(m,n) = n!\,S(m,n)$$

(OR)

$$P(m,n) = \sum_{K=0}^{n}(-1)^K\, {}^nC_K\,(n-K)^m$$

15/07/22

* Examples:

(1) Evaluate $S(8,5)$ and $S(7,4)$.

Sol:- Let $S(8,5)$

$\therefore n = 8 \;,\; r = 5$

$\therefore$ General formula Stirling number of second kind:

$$S(n,r) = \frac{1}{r!} \sum_{K=0}^{r} (-1)^K \, {}^{r}C_{K} \, (r-K)^n.$$

$$S(8,5) = \frac{1}{5!} \sum_{K=0}^{5} (-1)^K \, 5C_K \, (5-K)^8.$$

$$S(8,5) = 1050$$

$S(7,4)$; $n = 7$ & $r = 4$

$$S(7,4) = \frac{1}{4!} \sum_{K=0}^{4} (-1)^K \, 4C_K \, (4-K)^7.$$

$$S(7,4) = 350.$$

(2) A chemist who has 5 assistants is engaged in a research project that calls for 9 compounds must be synthesized. How many ways can the chemist assign these to the 5 assistants, so that each is working on atleast one synthesis.

Sol:- Given that, there are 5 assistants,

$\therefore r = 5$

And 9 synthesis.

$n = 9$

$\therefore$ General Formula to find no. of onto functions,

$$P(n,r) = \sum_{K=0}^{r} (-1)^K \, {}^{r}C_{K} \, (r-K)^n$$

$$P(9,5) = \sum_{K=0}^{5} (-1)^K \, 5C_K \, (5-K)^9.$$

$$P(9,5) = 834120.$$

(3) There are 6 programmers who can assist 8 executives. In how many ways can the executives be assisted so that each programmer assists at least one executive.

Sol^n: Given that, there are 6 programmers,

$\therefore n = 6$.

And 8 executives

$\therefore m = 8$

$\therefore$ General formula to find no of onto function.

$$P(m,n) = \sum_{K=0}^{n} (-1)^K \, {}^nC_K \, (n-K)^m$$

$$P(8,6) = \sum_{K=0}^{6} (-1)^K \, {}^6C_K \, (6-K)^8$$

$$P(8,6) = 191520.$$

(4) If A & B are 2 finite sets with $n(A) = 5$ & $n(B) = 3$. Then find number of onto functions from set A to B.

Sol^n: Given that,

$n(A) = 5$

$n(B) = 3$.

General formula to find no of onto function.

$$P(m,n) = \sum_{K=0}^{n} (-1)^K \, {}^nC_K \, (n-K)^m$$

$$P(5,3) = \sum_{K=0}^{3} (-1)^K \, {}^3C_K \, (3-K)^5$$

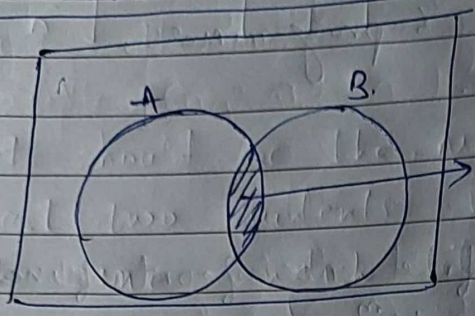
$\therefore P(5,3) =$

* ~~Pigeonhole~~ Principle of Inclusion and Exclusion:

Statement: Let A and B are any two sets. Then the number of elements in union of A and B is, the sum of the numbers of elements of A and B minus the number of elements in the intersection

of A and B.

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$



Similarly,

If A, B and C are any three sets, then the number of elements in union of A, B & C is,

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$$

★ Pigeonhole Principle:

Statement:

If n pigeons occupy n-pigeonholes and $m > n$, then two or more occupy pigeon same pigeonhole.

(OR)

If 'm' ~~pigeonhole~~ pigeon's occupy 'n' pigeonholes & $m > n$ Then atleast one pigeonhole must contain two or more - pigeons in it.

★ Generalized Pigeonhole Principle:

Statement:

If m- pigeons occupy n- pigeonholes then atleast one pigeonhole must contain $[(m-1)/n] + 1$ or more pigeons where [ ] stands for greatest integer function.

Proof:
We need to prove this theorem by method of contradiction.
Suppose every pigeonhole must contain $\left[\frac{m-1}{n}\right]$ or less no of pigeons in it.
∴ Total no of pigeons in 'n' pigeonholes is

$$n\left[\frac{m-1}{n}\right] \leq n\left(\frac{m-1}{n}\right) = (m-1).$$

∴ Total no of pigeons are less then $(m+1)$.
It contradicts the fact that there are 'm' pegions.
∴ At least one pigeonhole must contain $\left[\frac{m-1}{n}\right]+1$ or more pegions in it.

* Examples.

(1) Prove that in a set of 13 children atleast 2 have the birthday during same month.

Sol^n: Let us consider 13 children as pegions.

$$m = 13.$$

And 12 months as pgionholes.

$$n = 12.$$

∴ By Generalized pegionhole principle atleast one month, must be the birth month of $\left[\frac{m-1}{n}\right]+1$ or more children.

$$\therefore \left[\frac{m-1}{n}\right]+1 = \left[\frac{13-1}{12}\right]+1 = \left[\frac{12}{12}\right]+1 = [1]+1 = 1+1 = 2.$$

(2) If 7 cars carry 26 passengers prove that atleast one car must have 4 or more passengers.

Sol^n: Given that,

$$m = 26 \qquad n = 7 \text{ (cars)}$$

∴ By generalized pegion hole principle atleast one

car must contain $\left[\frac{n-1}{n}\right]+1$ or more passengers.

$\therefore \left[\frac{n-1}{n}\right]+1 = \left[\frac{26-1}{7}\right]+1 = \left[\frac{25}{7}\right]+1 = [3.57]+1 = 3+1 = \boxed{4}$

Imp.

(3) What should be the minimum number of students that atleast two students have their last name starts with same english letter.

Sol^n: Given that,

$n = 26$ (English alphabet)

$m = ?$

Also given that 2 or more students have their last name starts with same english letter.

$\therefore$ By generalized pigeonhole principle,

$\left[\frac{m-1}{n}\right]+1 \geq 2.$

$\left[\frac{m-1}{26}\right]+1 \geq 2.$

$\left[\frac{m-1}{26}\right] \geq 2-1$

$\left[\frac{m-1}{26}\right] \geq 1$

$\left(\frac{m-1}{26}\right) \geq \neq 1$ [If it is -26 then inequality change i.e. $\leq$.

$m-1 \geq 26.$

$\boxed{m \geq 27}$

$\therefore$ minimum 27 students should be there.

selection : ${}^nC_r$
combinations : ${}^nP_r$

8/07/22

4) Find least number of ways of choosing 3 different no's. from 1 to 10 so that all choices have have the same sum.

Sol^n: No. of ways of chosing 3-digits from 1 to 10 is ${}^{10}C_3$.

$= \frac{10!}{7!3!} = 120.$

$\therefore \boxed{n = 120.}$

The smallest sum of 3-digits by chosing 1, 2 and 3, i.e $1+2+3 = 6$.

The largest sum of 3-digits by chosing 8, 9 and 10, i.e $8+9+10 = 27$

$\therefore$ Sum of 3-digits lies b/w 6 and 27 is 22 in number

$\therefore \boxed{n = 22}$

$\therefore$ By generalized pigeonhole principle,

atleast $\left[\frac{n-1}{n}\right] + 1$ choices have the same sum.

$\therefore \left[\frac{n-1}{n}\right] + 1 = \left[\frac{120-1}{22}\right] + 1 = \left[\frac{119}{22}\right] + 1.$

$= [5.40] + 1$

$= 5 + 1$

$= 6.$

$\therefore$ 6 different choices have same least sum.

* Recurrence Relation:

A recurrence relation for the sequence $\{a_n\}$ (or) $(a_0, a_1, \ldots\ldots a_{n-1}, \ldots)$ is an equation that expresses a_n in terms of one or more of previous terms of the sequence, namely $a_1, a_2, a_3 \ldots a_n$ for all integers $n \geq 0$.

* Solution of Recurrence Relation:
A sequence $\{a_n\}$. $(a_1, a_2, a_3, \ldots a_n, \ldots)$ is called a solution of recurrence relation if its terms satisfy the recurrence relation.

Example:
The sequence 1, 3, 7, 15, 31, ... is the solution of recurrence relation $\boxed{a_n = 2a_{n-1} + 1}$

Note: The recurrence relation,
$$4a_{n+3} - a_{n+2} + 11a_{n+1} - 6a_n = 0.$$
can also be written as,
$$4Y_{n+3} - Y_{n+2} - 11Y_{n+1} - 6Y_n = 0.$$
or
$$4U_{n+3} - U_{n+2} - 11U_{n+1} - 6U_n = 0.$$
or
$$4f(x+3) - f(x+2) + 11f(x+1) - 6f(x) = 0.$$

* Order of a recurrence Relation:
It is the difference b/w the largest and smallest subscript appearing in its relation.

Example:
$$4a_{n+3} - a_{n+2} + 11a_{n+1} - 6a_n = 0.$$
order is $n+3 - n = 3$.

* Linear Recurrence Relation with constant co-efficient
The linear recurrence relation with constant co-efficients of order K is of the form

$$\boxed{C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_K a_{n-K} = 0 f(n).}$$

where $f(n)$ is the function of variable n only and

$c_0, c_1, c_2, \ldots c_k$ are constants.

* Homogeneous and Non-homogeneous linear recurrence relation:

The linear recurrence relation.

$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = f(n)$

is said to be homogeneous linear recurrence relation if $f(n) = 0$. otherwise it is called non-homogeneous linear recurrence relation.

* Generating function:

Let $\{a_n\}$ or $(a_0, a_1, a_2, \ldots)$ be a sequence of real no's then the generating function of $\{a_n\}$ is denoted by $G(a, z)$ and defined by,

$$G(a,z) = a_0 + a_1 z^1 + a_2 z^2 + a_3 z^3 + \cdots = \sum_{n=0}^{\infty} a_n z^n$$

where z is a variable.

* Some Standard Generating function:

(1) If $\{a_n\}$ is a sequence and $a_n = c$, $\forall\, n \geq 0$. where c is constant, then find generating function of $\{a_n\}$.

Sol^n: Let $\{a_n\}$ be a sequence when $a_n = c$, $\forall\, n \geq 0$.

By generating function:

$$G(a,z) = \sum_{n=0}^{\infty} a_n z^n.$$

$$G(a,z) = \sum_{n=0}^{\infty} c z^n.$$

$$G(a,z) = c + cz + cz^2 + cz^3 + \cdots$$

$$\therefore G(a,z) = c(1 + z + z^2 + z^3 + \cdots).$$

$$G(a,z) = c\left(\frac{1}{1-z}\right)$$

$$\therefore \boxed{G(a,z) = \frac{c}{1-z}}$$

$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}$.

② If $\{a_n\}$ is a sequence and $a_n = b^n$, $\forall n \geq 0$, then find generating function of $\{a_n\}$.

Sol^n: Let $\{a_n\}$ be a sequence when $a_n = b^n$, $\forall n \geq 0$.

By generating function,

$$G(a,z) = \sum_{n=0}^{\infty} a_n z^n.$$

$$= \sum_{n=0}^{\infty} b^n z^n.$$

$$= 1 + bz + b^2z^2 + b^3z^3 + \cdots$$

$$= 1 + (bz) + (bz)^2 + (bz)^3 + \cdots$$

$$\boxed{G(a,z) = \frac{1}{1-bz}}$$

Note: If $\{a_n\}$ is a sequence & $a_n = c.b^n$, $\forall n \geq 0$ then

$$\boxed{G(a,z) = \frac{c}{1-bz}}$$

③ If $\{a_n\}$ is a sequence & $a_n = n$ $\forall n \geq 0$, then find generating function of $\{a_n\}$.

Sol^n: Let $\{a_n\}$ be sequence when $a_n = n$, $\forall n \geq 0$.

By generating function

$$G(a,z) = \sum_{n=0}^{\infty} a_n z^n$$

$$= \sum_{n=0}^{\infty} n z^n$$

$$= 0 + 1z + 2z^2 + 3z^3 + \cdots$$

$$= z(1 + 2z + 3z + \cdots)$$

$$G(a,z) = z\left(\frac{1}{(1-z)^2}\right)$$

$$\boxed{G(a,z) = \frac{z}{(1-z)^2}}$$

Note: If $\{a_n\}$ is sequence & $a_n = (n+1)$, $\forall n \geq 0$ then $G(a,z) = \frac{1}{(1-z)^2}$

Sl. No	Sequence $\{a_n\}$	Generating Function $G(a,z)$
1.	$a_n = c$, $\forall n \geq 0$	$\frac{c}{1-z}$
2.	$a_n = b^n$, $\forall n \geq 0$	$\frac{1}{1-bz}$
3.	$a_n = n$, $\forall n \geq 0$	$\frac{z}{(1-z)^2}$
4.	$a_n = (n+1)$, $\forall n \geq 0$	$\frac{1}{(1-z)^2}$
5.	$a_n = c \cdot b^n$, $\forall n \geq 0$.	$\frac{c}{1-bz}$

* Solution of Homogeneous linear Recurrence Relation By Generating Function:

Consider a homogeneous linear recurrence relation $c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0$ — (1), $\forall n \geq k$.

Then following steps to be followed to solve (1) are:

Step 1:
Multiply z^n on both sides of eq^n (1) & take summation from $n = k$ to ∞.

Step 2:
Write each term in the form of $G(a,z)$.

Step 3:
Solve $G(a,z)$ by using standard generating function for the sequence $\{a_n\}$.

Examples:

(1) Solve homogeneous linear recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$, $\forall n \geq 2$ given initial condition $a_1 = 5$ and $a_2 = 3$ by using generating function.

Sol:- Let,

$$a_n = 3a_{n-1} - 2a_{n-2} \quad \forall n \geq 2.$$

$$a_n - 3a_{n-1} + 2a_{n-2} = 0 \quad \text{---(1)}$$

Put $n = 2$ in (1), we get

$$a_2 - 3a_1 + 2a_0 = 0$$

$$3 - 3(5) + 2a_0 = 0$$

$$3 - 15 + 2a_0 = 0$$

$$-12 + 2a_0 = 0$$

$$2a_0 = 12$$

$$\boxed{a_0 = 6}$$

Multiply z^n on both sides of eq(1) & take summation from $n = 2$ to ∞

$$\sum_{n=2}^{\infty} (a_n - 3a_{n-1} + 2a_{n-2}) z^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n - 3\sum_{n=2}^{\infty} a_{n-1} z^n + 2\sum_{n=2}^{\infty} a_{n-2} z^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n + a_0 + a_1 z - a_0 - a_1 z - 3\sum_{n=2}^{\infty} a_{n-1} z^{n-1} \cdot z^1 +$$

$$2\sum_{n=2}^{\infty} a_{n-2} z^{n-2} \cdot z^2 = 0.$$

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n - 6 - 5z - 3z\left(\sum_{n=2}^{\infty} a_{n-1} z^{n-1} + a_0 - a_0\right)$$

$$+ 2z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} = 0.$$

By step

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n - 6 - 5z - 3z\left(\sum_{n=0}^{\infty} a_n z^n - 6\right) + 2z^2\left(\sum_{n=0}^{\infty} a_n z^n\right) =$$

$$\Rightarrow G(a,z) - 6 - 5z - 3z(G(a,z) - 6) + 2z^2 G(a,z) = 0$$

Examples:

(1) Solve homogeneous linear recurrence relation $a_n = 3a_{n-1} - 2a_{n-2}$, $\forall n \geq 2$ given initial condition $a_1 = 5$ and $a_2 = 3$ by using generating function.

Sol:- Let,

$$a_n = 3a_{n-1} - 2a_{n-2} \quad \forall n \geq 2.$$

$$a_n - 3a_{n-1} + 2a_{n-2} = 0 \quad \text{---(1)}$$

Put $n = 2$ in (1), we get

$$a_2 - 3a_1 + 2a_0 = 0$$

$$3 - 3(5) + 2a_0 = 0$$

$$3 - 15 + 2a_0 = 0$$

$$-12 + 2a_0 = 0$$

$$2a_0 = 12$$

$$\boxed{a_0 = 6}$$

Multiply z^n on both sides of eq(1) & take summation from $n = 2$ to ∞

$$\sum_{n=2}^{\infty} (a_n - 3a_{n-1} + 2a_{n-2}) z^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n - 3\sum_{n=2}^{\infty} a_{n-1} z^n + 2\sum_{n=2}^{\infty} a_{n-2} z^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n + a_0 + a_1 z - a_0 - a_1 z - 3\sum_{n=2}^{\infty} a_{n-1} z^{n-1} \cdot z^1 +$$

$$2\sum_{n=2}^{\infty} a_{n-2} z^{n-2} \cdot z^2 = 0.$$

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n - 6 - 5z - 3z\left(\sum_{n=2}^{\infty} a_{n-1} z^{n-1} + a_0 - a_0\right)$$

$$+ 2z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} = 0$$

By step

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n - 6 - 5z - 3z\left(\sum_{n=0}^{\infty} a_n z^n - 6\right) + 2z^2\left(\sum_{n=0}^{\infty} a_n z^n\right) =$$

$$\Rightarrow G(a,z) - 6 - 5z - 3z(G(a,z) - 6) + 2z^2 G(a,z) = 0$$

$G(a,z) - 3zG(a,z) + 18z^2 G(a,z) = 6+5z.$

$G(a,z)[1-3z+2z^2] + 18z^2 = 6+5z.$

$G(a,z)[1-3z+2z^2] = 6+5z-18z^2.$

$G(a,z)[2z^2-3z+1] = 6-13z.$

$G(a,z)[2z^2-2z-z+1] = 6-13z.$

$G(a,z)[2z(z-1)-1(z-1)] = 6-13z.$

$G(a,z)[(2z-1)(z-1)] = 6-13z.$

$$G(a,z) = \frac{6-13z}{(2z-1)(z-1)} \quad \text{---} \quad (2).$$

By partial function.

$$\frac{6-13z}{(1-z)(1-2z)} = \frac{A}{(1-z)} + \frac{B}{(1-2z)} \quad \text{---} \quad (3).$$

$$6-13z = A(1-2z) + B(1-z) \quad \text{---} \quad (4).$$

put $z=1$ in (4), we get

$6-13(1) = A(1-2(1)) + B(1-1)$

$6-13 = -A$

$\boxed{A=7}$

put $z=1/2$ in (4), we get

$6-13(\frac{1}{2}) = A(1-2(1/2)) + B(1-1/2)$

$$6-\frac{13}{2} = \frac{B}{2}$$

$-1 = B$; $\boxed{B=-1}$

$\therefore$ eq: (3) becomes,

$$G(a,z) = \frac{7}{(1-z)} - \frac{1}{(1-2z)}$$

$\therefore$ By using standard generating function,

$\boxed{a_n = 7-2^n}$

$\because \frac{c}{1-z} \Rightarrow a_n = c : \frac{7}{1-z} ; a_n = 7$

$\frac{c}{1-bz} \Rightarrow a_n = c.b^n ; \frac{1}{1-2z} ; a_n = 2^n$

(2) Solve homogeneous linear recurrence relation $a_n = 2a_{n-1} - a_{n-2}$, $\forall n \geq 2$, given that $a_1 = 1$ and $a_2 = 4$ by generating function.

Sol: Let $a_n = 2a_{n-1} - a_{n-2}$ ——— (1)

put $n=2$ in (1).

$a_2 = 2a_1 - a_0$.

$a_0 = 4 - 2(2+1)$

$a_0 = 2 - 4$

$\boxed{a_0 = -2}$

Multiply z^n on both sides of equation (1) and take summation from $n=2$ to ∞

$$\Rightarrow \sum_{n=2}^{\infty} (a_n - 2a_{n-1} + a_{n-2}) z^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n - 2\sum_{n=2}^{\infty} a_{n-1} z^n + \sum_{n=2}^{\infty} a_{n-2} z^n = 0.$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n z^n + a_0 + a_1 z - a_0 - a_1 z - 2 \cdot \sum_{n=2}^{\infty} a_{n-1} z^{n-1} \cdot z + \sum_{n=2}^{\infty} a_{n-2} z^{n-2} \cdot z^2 = 0$$

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n - a_0 - a_1 z - 2z\left(\sum_{n=2}^{\infty} a_{n-1} z^{n-1} + a_0 - a_0\right) + z^2 \sum_{n=2}^{\infty} a_{n-2} z^{n-2} = 0$$

$$\Rightarrow \sum_{n=0}^{\infty} a_n z^n + 2 - z - 2z\left(\sum_{n=0}^{\infty} a_n z^n + 2\right) + z^2 \sum_{n=0}^{\infty} a_n z^n = 0$$

$$\Rightarrow G(a,z) + 2 - z - 2z(G(a,z) + 2) + z^2 G(a,z) = 0$$

$$G(a,z) + 2 - z - 2zG(a,z) - 4z + z^2 G(a,z) = 0.$$

$$G(a,z)(1 - 2z + z^2) = 5z - 2.$$

$$G(a,z)(1-z)^2 = 5z - 2.$$

$$G(a,z) = \frac{5z-2}{(1-5z)^2} \quad \text{---(2)}$$

∴ By partial function we have,

$$\frac{5z-2}{(1-z)^2} = \frac{A}{(1-z)} + \frac{B}{(1-z)^2} \quad \text{---(3)}$$

$$\frac{5z-2}{(1-z)^2} = \frac{A(1-z) + B}{(1-z)^2}$$

$$5z-2 = A(1-z) + B \quad \text{---(4)}$$

put $z=1$ in eq (4), we get

$$5(1) - 2 = A(1-1) + B$$

$$\boxed{B = 3}$$

put $z=0$ in eq (4), we get

$$5(0) - 2 = A(1-0) + B$$

$$-2 = A + 3$$

$$\boxed{A = -5}$$

∴ equation (2) becomes

$$G(a,z) = \frac{-5}{(1-z)} + \frac{3}{(1-z)^2}$$

∴ By standard generating function, of a_n,

$$a_n = -5 + 3(n+1)$$

$$a_n = -5 + 3n + 3$$

$$\therefore \boxed{a_n = 3n - 2}$$

* Solution of Non Homogeneous linear recurrence relations by using generating function.

Imp Example:

(1) Solve non-homogeneous linear recurrence relation $a_{n+2} - 2a_{n+1} + a_n = 2^n$, $\forall n \geq 0$ given that $a_0 = 2$ & $a_1 = 1$ by generating function.

Sol: Let $a_{n+2} - 2a_{n+1} + a_n = 2^n$, $\forall n \geq 0$ ——— (1).

Multiply z^n on both sides of eq (1) and take summation from $n = 0$ to ∞

$$\therefore \sum_{n=0}^{\infty} (a_{n+2} - 2a_{n+1} + a_n) z^n = \sum_{n=0}^{\infty} 2^n z^n.$$

$$\Rightarrow \sum_{n=0}^{\infty} a_{n+2} z^n - 2\sum_{n=0}^{\infty} a_{n+1} z^n + \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} (2z)^n$$

$a_n = b^n \Rightarrow \frac{1}{1-bz}$

$$\Rightarrow \sum_{n=0}^{\infty} a_{n+2} z^{n+2} z^{-2} - 2\sum_{n=0}^{\infty} a_{n+1} z^{n+1} z^{-1} + \sum_{n=0}^{\infty} a_n z^n = \frac{1}{1-2z}.$$

$$\Rightarrow \frac{1}{z^2}\left\{\sum_{n=0}^{\infty} a_{n+2} z^{n+2} + a_0 + a_1 z - a_0 - a_1 z\right\} - \frac{2}{z}\left\{\sum_{n=0}^{\infty} a_{n+1} z^{n+1} + a_0\right\} + \sum_{n=0}^{\infty} a_n z^n = \frac{1}{1-2z}.$$

$$\Rightarrow \frac{1}{z^2}\left\{\sum_{n=0}^{\infty} a_n z^n - 2 - 1z\right\} - \frac{2}{z}\left\{\sum_{n=0}^{\infty} a_n z^n - 2\right\} + \sum_{n=0}^{\infty} a_n z^n = \frac{1}{1-2z}.$$

Send z^2 to RHS, take LCM

$$\sum_{n=0}^{\infty} a_n z^n - 2 - z - 2z\left[\sum_{n=0}^{\infty} a_n z^n - 2\right] + z^2 \sum_{n=0}^{\infty} a_n z^n = \frac{1 \times z^2}{1-2z}$$

$$G(a,z) - 2 - z - 2z\,G(a,z) + 4z + z^2 G(a,z) = \frac{z^2}{1-2z}$$

$$G(a,z)[1 - 2z + z^2] = \frac{z^2}{1-2z} + (2 - 3z)$$

$$G(a,z)(1-z)^2 = \frac{z^2 + (2-3z)(1-2z)}{(1-2z)}$$

$$G(a,z)(1-z)^2 = \frac{z^2 + 2 - 4z - 3z + 6z^2}{(1-2z)}$$

$$G(a,z) = \frac{7z^2 - 7z + 2}{(1-2z)(1-z)^2} \quad \text{— (2)}$$

By partial fraction:

$$\frac{7z^2 - 7z + 2}{(1-2z)(1-z)^2} = \frac{A}{(1-2z)} + \frac{B}{(1-z)} + \frac{C}{(1-z)^2} \quad \text{: LCM is } (1-z)^2(1-2z). \quad \text{— (3)}$$

$$7z^2 - 7z + 2 = A(1-z)^2 + B(1-2z)(1-z) + C(1-2z) \quad \text{— (4)}$$

Put $z = 1/2$ in eq (4), we get

$$\frac{7}{4} - \frac{7}{2} + 2^{x1} = A(1-1/2)^2$$

$$\frac{7 - 14 + 8}{4} = A/4$$

$$\boxed{A = 1}$$

put $z = 1$ in eq (4)

$$7 - 7 + 2 = C(-1)$$

$$\boxed{C = -2}$$

put $z = 0$ in eq (4)

$$2 = A(1)^2 + B(1) + C(1)$$

$$B = 2 - A - C$$

$$B = 2 - 1 + 2$$

$$\boxed{B = 3}$$

∴ Equation (3) becomes,

$$G(a,z) = \frac{1}{1-2z} + \frac{3}{1-z} - \frac{2}{(1-z)^2}.$$

∴ By generating function

$$a_n = 2^n + 3 - 2(n+1)$$

$$a_n = 2^n + 3 - 2n - 2$$

$$\boxed{a_n = 2^n - 2n + 1}$$

Order = $n-(n-k)$
$= k$.

25/07/22.

* Solution of Homogeneous linear Recurrence Relation by Characteristic Root Method:

Consider homogeneous linear recurrence relation:

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0 \quad \text{---(1)}$$

Characteristic equation (or auxillary eq^n) of degree k.

$$c_0 r^n + c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k} = 0.$$

$$r^{n-k}[c_0 r^k + c_1 r^{k-1} + c_2 r^{k-2} + \cdots + c_k] = 0.$$

$$\boxed{c_0 r^k + c_1 r^{k-1} + c_2 r^{k-2} + \cdots + c_k = 0} \quad \text{---(2)}$$

Roots of (2) are $\alpha_1, \alpha_2, \cdots \alpha_k$.

Solution of (1) has following case.

Case 1: Roots are real and unequal than sol^n of (1) is,

$$\boxed{a_n = A_1\alpha_1^n + A_2\alpha_2^n + A_3\alpha_3^n + \cdots + A_k\alpha_k^n}$$

Case 2: Roots are equal, $\alpha_1 = \alpha_2$, than sol^n of (1) is,

$$\boxed{a_n = (A_1 + nA_2)\alpha_1^n + A_3\alpha_3^n + \cdots + A_k\alpha_k^n}$$

Case 3: Roots are complex.

$$\boxed{a_n = A_1(\alpha_1 + i\beta_1)^n + A_2(\alpha_1 - i\beta_1)^n + \cdots}$$

Case 4: Two complex roots are equal i.e $\alpha_1 \pm i\beta_1 = \alpha_2 \pm i\beta_2$.

$$\boxed{a_n = (A_1 + nA_2)(\alpha_1 + i\beta_1)^n + (A_3 + nA_4)(\alpha_1 - i\beta_1)^n + \cdots}$$

* Examples.

(1) Solve homogeneous linear recurrence relation $a_{n+2} - 3a_{n+1} + 2a_n = 0$, given that $a_0 = 1$, $a_1 = 3$ by characteristic root method.

Sol^n: Let, $a_{n+2} - 3a_{n+1} + 2a_n = 0$ ---(1).

Replace a_{n+2} by r^{n+2}, a_{n+1} by r^{n+1} & a_n by r^n.

$$r^{n+2} - 3r^{n+1} + 2r^n = 0$$

$$r^n(r^2 - 3r + 2) = 0.$$

$$\boxed{r^2 - 3r + 2 = 0} \quad \text{---(2)} \quad \text{(characteristic eq^n)}.$$

$\therefore$ Roots are $\alpha_1 = 1$ & $\alpha_2 = 2$.

$\therefore$ General solution of eq^n (1) is,

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n$$

$$a_n = A_1(1)^n + A_2(2^n).$$

$$\boxed{a_n = A_1 + A_2 2^n} \quad \text{---(3)}.$$

Put $n = 0$ in (3). and $a_0 = 1$

$$a_0 = A_1 + A_2 \cdot 2^0$$

$$1 = A_1 + A_2 \quad \text{---(4)}.$$

Put $n = 1$ in (3) and $a_1 = 3$.

$$a_1 = A_1 + A_2 2^1$$

$$3 = A_1 + A_2(2) \quad \text{---(5)}.$$

Solving (4) and (5).

$$1 = A_1 + A_2$$

$$3 = A_1 + 2A_2$$

$$-2 = -A_2$$

$$\boxed{A_2 = 2}$$

Put A_2 in eq^n (4)

$$\boxed{A_1 = -1}$$

$\therefore$ Particular solution of (1) is

$$a_n = (-1) + (2)2^n$$

$$\boxed{a_n = 2^{n+1} - 1}$$

(2) Solve homogeneous linear recurrence relation $a_n - 8a_{n-1} + 16a_{n-2} = 0$, given that $a_2 = 6$, and $a_3 = 80$ by characteristic root method.

Let $a_n - 8a_{n-1} + 16a_{n-2} = 0$. ---(1)

Replace a_n by r^n, a_{n-1} by r^{n-1} & a_{n-2} by r^{n-2}.

$$r^n - 8r^{n-1} + 16r^{n-2} = 0$$

$$r^{n-2}(r^2 - 8r + 16) = 0$$

$$\boxed{r^2 - 8r + 16 = 0} \quad \text{---} (2)$$

∴ Roots are $\alpha_1 = \alpha_2 = 4$.

∴ General solution of eq^n (1) is,

$$a_n = (A_1 + nA_2)\alpha_1^n$$

$$\boxed{a_n = (A_1 + nA_2)4^n} \quad \text{---} (3)$$

Put $n = 2$ in (3) and $a_2 = 6$.

$$a_2 = (A_1 + 2A_2)4^2$$

$$6 = (A_1 + 2A_2)16.$$

$$6 = 16A_1 + 32A_2 \quad \text{---} (4)$$

Put $n = 3$ in (3) and $a_3 = 80$.

$$a_3 = (A_1 + 3A_2)4^3$$

$$80 = 64A_1 + 192A_2. \quad \text{---} (5)$$

Solving (4) and (5). gives,

$$A_1 = \frac{-11}{8} \qquad A_2 = \frac{7}{8}$$

∴ Particular solution of (1) is,

$$a_n = \left(\frac{-11}{8} + \frac{7n}{8}\right)4^n$$

$$\boxed{a_n = (-11 + 7n)\frac{4^{n-1}}{2}}$$

27/07/22

★ Solution of Non-Homogeneous linear recurrence relation by characteristic root method:

Consider a non-homogeneous linear recurrence relation of order k.

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = f(n) \quad \text{---} (1).$$

General solution of recurrence relation (1) is,

$$\boxed{a_y = a_n^{(h)} + a_n^{(p)}} \quad \text{---} (2)$$

where $a_n^{(h)}$ is the general solution of the homogeneous part of the recurrence relation (1) and $a_n^{(p)}$ is particular solution of (1).

The following are the cases to find $a_n^{(p)}$.

Case1: If $f(n)$ is a polynomial of degree q and 1 is not a root of characteristic equation of homogeneous part of (1), then $a_n^{(p)}$ is as follows:

$$\boxed{a_n^{(p)} = B_0 + B_1 n + B_2 n^2 + \cdots + B_q n^q}$$

Case2: If $f(n)$ is a polynomial of degree q and 1 is a root of multiplicity m of characteristic equation of homogeneous part of (1), then $a_n^{(p)}$ is as follows:

$$\boxed{a_n^{(p)} = n^m (B_0 + B_1 n + B_2 n^2 + \cdots + B_q n^q)}$$

Case3: If $f(n) = \alpha b^n$, where 'α' and 'b' are constants and 'b' is not a root of characteristic equation of homogeneous part of (1), then $a_n^{(p)}$ is as follows:

$$\boxed{a_n^{(p)} = B_0 . b^n}$$

Case4: If $f(n) = \alpha b^n$, where α and b are constants and 'b' is a root of multiplicity m of characteristic equation of homogeneous part of (1), then $a_n^{(p)}$ is as follows:

$$\boxed{a_n^{(p)} = B_0 n^m b^n}$$

where $B_0, B_1, B_2, \ldots B_q$ are constants to be evalu by using the fact then $a_n = a_n^{(p)}$ satisfying the recurrence relation (1).

* Example:

(1) Solve the recurrence relation $a_n + 4a_{n-1} + 4a_{n-2} = 8$, $n \geq$ and given that $a_0 = 1$ & $a_1 = 2$.

Sol:- Let $a_n + 4a_{n-1} + 4a_{n-2} = 8$ — (1).

Characteristic equation of (1) is,

$$r^n + 4r^{n-1} + 4r^{n-2} = 0.$$

$$r^{n-2}[r^2 + 4r + 4] = 0$$

$$r^2 + 4r + 4 = 0. \quad \text{— (2).}$$

$$(r+2)^2 = 0.$$

$r = -2$ and $r = -2$.

$\therefore$ Roots are $\alpha_1 = \alpha_2 = -2$

$\therefore$ Solution of homogeneous part of (1) is,

$$a_n^{(h)} = (A_1 + nA_2)\alpha_1^n$$

$$\boxed{a_n^{(h)} = (A_1 + nA_2)(-2)^n} \quad \text{— (3).}$$

Particular solution $a_n^{(p)}$ of ~~eq (2).~~ $f(n) = 8$. ($f(n) = 8$ is a polyno of degree 0 and 1 is not a root of characteristic eq

$$\boxed{a_n^{(p)} = B_0} \quad \text{— (4).}$$

To find B_0, we use the fact that $a_n = a_n^{(p)} = B_0$. whi satisfies recurrence relation (1).

$$B_0 + 4B_0 + 4B_0 = 8. \quad (\because a_n \text{ is independent of } n \text{ . i.e } B_0)$$

$$9B_0 = 8$$

$$\boxed{B_0 = 8/9} \quad \text{— (5).}$$

$\therefore$ General solution of recurrence relation (1) is,

$$\boxed{a_n = (A_1 + nA_2)(-2)^n + 8/9} \quad \text{— (6).}$$

Put $n=0$ in (6) and use $a_0=1$.

$a_0 = (A_1)(-2)^0 + 8/9$

$1 = A_1 + 8/9$

$\boxed{A_1 = 1/9}$

Put $n=1$ in (6) and use $a_1=2$

$a_1 = (A_1+A_2)(-2)^1 + 8/9.$

$2 = -2A_1 - 2A_2 + 8/9.$

$2 = -\frac{2}{9} + \frac{8}{9} - 2A_2$

$2A_2 = \frac{6}{9} - 2$

$2A_2 = \frac{-12}{9}$

$\boxed{A_2 = -\frac{2}{3}}$

$\therefore$ Solution (4) becomes.

$\boxed{a_n = \left(\frac{1}{9} - \frac{2n}{3}\right)(-2)^n + \frac{8}{9}}$

(2) Solve the recurrence relation $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$, $n \geq 0$. and given that $a_0 = 0$ and $a_1 = 1$.

Sol:- Let $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$ ——— (1)

Characteristic eq:- of (1) is,

$r^{n+2} + 3r^{n+1} + 2r^n = 3^n$

$r^n(r^2 + 3r + 2) = 0$

$r^2 + 3r + 2 = 0$ ——— (2).

$r = -1$ and $r = -2$

$\therefore$ Roots are $\alpha_1 = -1$ and $\alpha_2 = -2$.

$\therefore$ Solution of homogeneous part of (1) is,

$a_n^{(h)} = A_1\alpha_1^n + A_2\alpha_2^n$

$\boxed{a_n^{(h)} = A_1(-1)^n + A_2(-2)^n}$ ——— (3)

Particular solution $a_n^{(p)}$ of eq^n (1) ($f(n) = 3^n$ is a polynomial degree 0 and 1 is not a root of characteristic equation (2)

$$\boxed{a_n^{(p)} = B_0 \cdot b^n} \quad \text{---(4)}$$

To find B_0, we use the fact that $a_n = a_n^{(p)} = B_0 \cdot b^n$ which satisfies recurrence relation (1).

~~$B_0 b^{(n+2)} + B_0 b^{(n+1)} + B_0 = 3^n$~~ $\quad B_0 \cdot 3^{n+2} + 3 B_0 3^{n+1} + 2 B_0 3^n = 3^n$

~~$B_0 (b^{n+2} + b^{(n+1)} + 1) = 3^n$~~ $\quad B_0 3^n (3^2 + 3 \cdot 3 + 2) = 3^n$

~~$B_0 \cdot b^n (b^2 + b + 1) = 3^n$~~ $\quad \boxed{B_0 = 1/20}$

$$\therefore \boxed{a_n^{(p)} = \frac{3^n}{20}}$$

∴ General solution of recurrence relation (1) is,

$$\boxed{a_n = A_1(-1)^n + A_2(-2)^n + \frac{3^n}{20}} \quad \text{---(5)}$$

Put $n = 0$ in (5) and use $a_0 = 0$.

$$a_0 = A_1(-1)^0 + A_2(-2)^0 + \frac{3^0}{20}$$

$$0 = A_1 + A_2 + \frac{1}{20}$$

$$\therefore A_1 + A_2 = -1/20 \quad \text{---(6)}$$

Put $n = 1$ in (5) and use $a_1 = 1$

$$a_1 = A_1(-1)^1 + A_2(-2)^1 + \frac{3^1}{20}$$

$$1 = -A_1 - 2A_2 + \frac{3}{20}$$

$$A_1 + 2A_2 = \frac{3}{20} - 1$$

$$A_1 + 2A_2 = -\frac{17}{20} \quad \text{---(7)}$$

$$\boxed{A_1 = 3/4} \qquad \boxed{A_2 = -4/5}$$

Solution (5) becomes,

$$\boxed{a_n = \left(\frac{3}{4}\right)(-1)^n + \left(\frac{-4}{5}\right)(-2)^n + \frac{3^n}{20}}$$

29/07/22

* Divide and Conquer Algorithm:

It works recursively. breaking down a given problem P. into two or more sub-problems (P1, P2 ... etc) of the same or related type, until these becomes simple enough to be solved directly. Then solutions to these sub-problems (S1, S2, ... etc) are combined to get a solution of original problem P.

A typical divide and conquer algorithm solves a given problem P using following steps.

Step 1: Divide:

- Breaks (or) divides the given problem P into sub problem $P_1, P_2, \ldots$ etc of same type.

Step 2: Conquer:

- Recursively solve the sub problem $P_1, P_2, \ldots$ etc

Step 3: Combine:

- Combines the solutions of sub-problems S1, S2.. etc to get solution of original problem P.

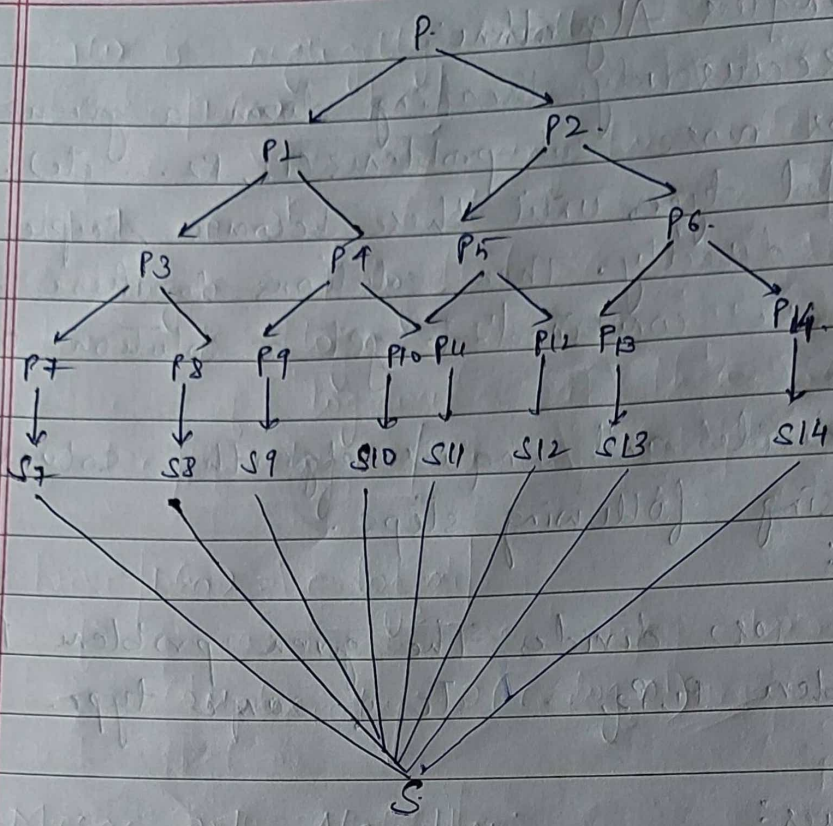
* Idea behind Divide and Conquer Algorithm:

Given a problem P of size $n = 2^k$.

Algorithm DAC(P):

- If 'n' is small, solve it.
- else
  - divide P into 2 (or) more sub-problems $P_1, P_2, \ldots$ etc
  - DAC(P_1)
  - DAC(P_2).
  - :
- combine solutions of S_1, S_2.. etc of sub problems P_1, P_2.. etc

Problem



$n = 2^k$

$\frac{n}{2} = \frac{2^k}{2} = 2^{k-1}$

$\frac{n}{4} = \frac{2^k}{4} = 2^{k-2}$

$\frac{n}{8} = \frac{2^k}{8} = 2^{k-3}$

★ Time Required to Solve Problem P:

P P1 P2.

$T(n) = T(n/2) + T(n/2) + f(n)$

Where,

$f(n)$ = is the additional cost of combining solutions of sub-problems.

$T(n) = 2T(n/2) + f(n)$.

In general,

$$\boxed{T(n) = bT(n/2) + f(n)}$$

It is called recurrence relation of divide and conquer algorithm.

★ Examples:

(1) Solve $T(n) = 2T(n/2) + n$, using iteration (or) substitution method taking $n = 2^k$.

Sol: Let $T(n) = 2T(n/2) + n$ ——(1).

T(1) is negligibly small

$\therefore \boxed{T(n) = kc}$

Put $n = 3^k$.

$\log n = k \log 3$

$k = \frac{\log n}{\log 3}$

$\boxed{k = \log_3 n}$

$\therefore \boxed{T(n) = c \log_3 n}$

$\therefore$ Complexicity $O(c \log_3 n)$

* Merge sort Algorithm:

Merge sort keeps on dividing a given list of nu into equal halves if possible until it can no more be divided. Then mergesort combines the smalle sorted list keeping new list sorted.

Algorithm:

Step 1: If there is only one element in the list is sorted, return.

Step 2: Divide the list recursively into two halve until it can no more be divided.

Step 3: Merge the smaller lists into new list in a sorted order.

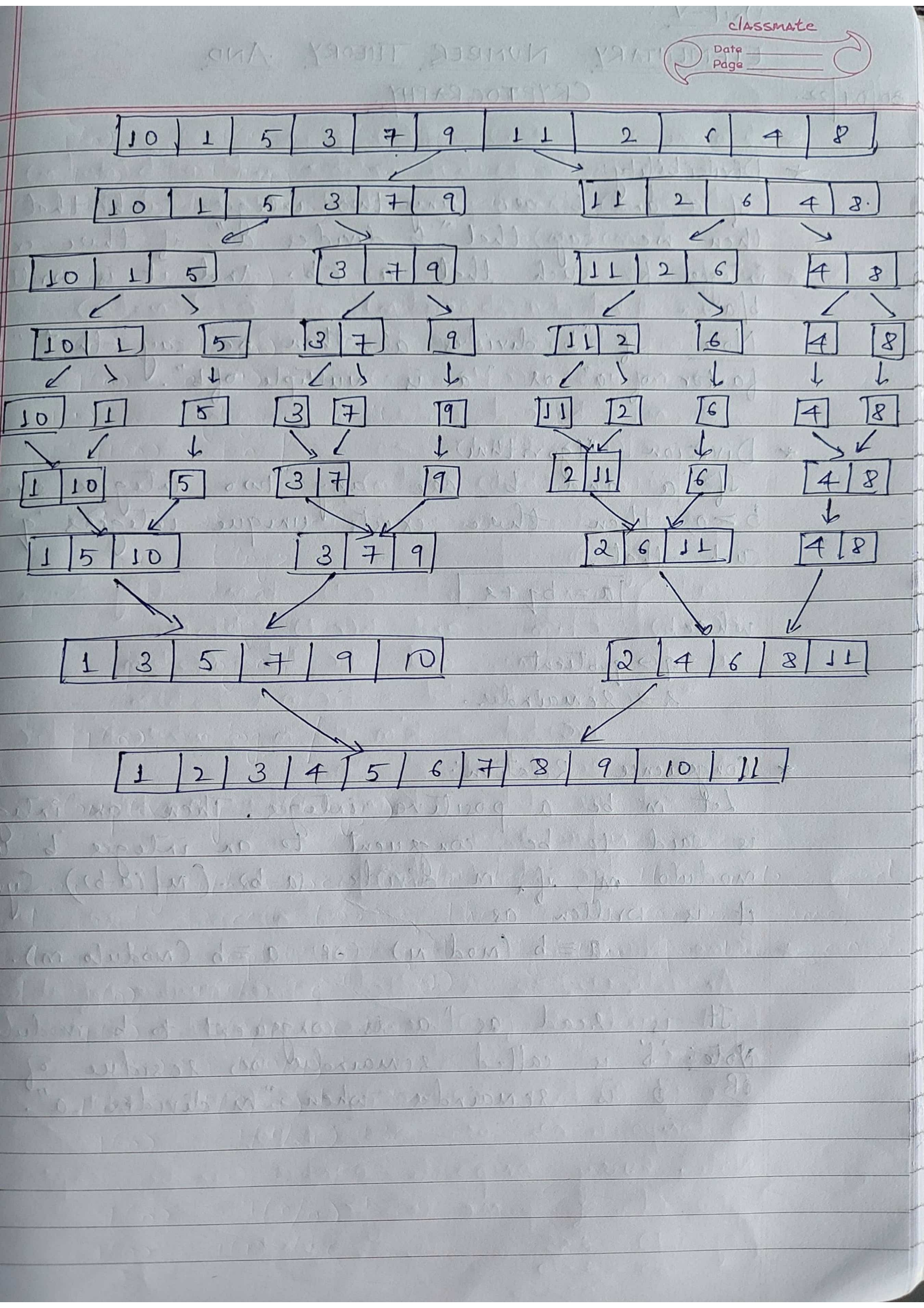
* Examples.

(1) Consider an unsorted list of numbers and sort it by merge sort algorithm.

10, 1, 5, 3, 7, 9, 11, 2, 6, 4, 8

Sol: Given nos;

10, 1, 5, 3, 7, 9, 11, 2, 6, 4, 8.


10 1 5 3 7 9 11 2 6 4 8
10 1 5 3 7 9
11 2 6 4 8
10 1 5
3 7 9
11 2 6
4 8
10 1
5
3 7
9
11 2
6
4 8
10
1
5
3
7
9
11
2
6
4
8
1 10
5
3 7
9
2 11
6
4 8
1 5 10
3 7 9
2 6 11
4 8
1 3 5 7 9 10
2 4 6 8 11
1 2 3 4 5 6 7 8 9 10 11

Unit-V:

ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY.

30/07/22.

★ Divisibility:

If 'a' and 'b' are any two integers such that $b \neq 0$, then we say that "b divides a", if there exists an integer 'k' such that $a = kb$, and it is written as $b|a$.

Note: If "b divides a", then we say that "b is a factor of a" or "a is multiple of b".

★ Division Algorithm:

If 'a' and 'b' are any two integers such that $b > 0$, then there exists unique integers 'q' and 'r' such that,

$$\boxed{a = bq + r}$$

where,

q → quotient

r → remainder.

★ Congruence Relation:

Let 'm' be a positive integer. Then an integer 'a' is said to be congruent to an integer 'b' under modulo m, if m divides $(a-b)$. $(m|(a-b))$. Symbolically it is written as

$$a \equiv b \pmod{m} \quad (\text{or}) \quad a \equiv b \ (\text{Modulo } m).$$

It is read as "a is congruent to b modulo m".

Note: 'b' is called remainder (or) residue of $a \pmod m$

OR 'b' is remainder when "m divides a".

* Properties of Congruence Relation:

1) If $a \equiv b \pmod m$, then $m \mid (b-a)$.
2) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.
3) If $a \equiv b \pmod m$ & $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

* Modular Arithmetic operation:

If $a \equiv b \pmod m$, then for $k \neq 0 \in Z$.

i) $a+k = b+k \pmod m$.
ii) $a-k = b-k \pmod m$.
iii) $ak = bk \pmod m$.
iv) $a^k = b^k \pmod m$.

* Properties of Modular Arithmetic Operation:

• Residue System Modulo m:

Define the set Z_m as a set of non-negative integers less than m,

$$Z_m = \{0, 1, 2, \ldots (m-1)\}.$$

It is called ~~modulo~~ residue system modulo.

• Residue Classes:

Each integer in Z_m represents a residue class. and it is denoted by $[a]$ and defined by

$$[r] = \{x : x \equiv r \pmod m\}.$$

eg: ① Residue system modulo 3 is,

$$Z_3 = \{0, 1, 2\}.$$

∴ Residue classes of elements of Z_3 are:

$[0] = \{x : x \equiv 0 \pmod 3\}$

$[0] = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$.

$[1] = \{x : x \equiv 1 \pmod 3\}$

$[1] = \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}$.

$[2] = \{x : x \equiv 2 \pmod 3\}$

$[2] = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$.

01/08/22.

★ Theorem:

Let n be a positive integer and $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then prove that $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Proof:

Given that, $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

$n \mid (a-b)$ & $n \mid (c-d)$ ——— (1);

$\Rightarrow n \mid (a-b)+(c-d)$.

$\Rightarrow n \mid a-b+c-d$.

$\Rightarrow n \mid (a+c)-(b+d)$.

$\Rightarrow \boxed{(a+c) \equiv (b+d) \pmod{n}}$.

By (1).

$(a-b) = k_1 n$ and $(c-d) = k_2 n$ (By division algorithm)

$c(a-b) = ck_1 n$ and $b(c-d) = bk_2 n$.

$ac - bc = (k_1 c)n$ and $bc - bd = (k_2 b)n$.

$ac - bc + bc - bd = (k_1 c)n + (k_2 b)n$

$ac - bd = k'n + k''n$, where $k' = k_1 c$ & $k'' = k_2$

$ac - bd = (k' + k'')n$.

$ac - bd = k_1 n$, where $k' = k' + k'' \in \mathbb{Z}$.

$\Rightarrow n \mid (ac - bd)$.

$\Rightarrow \boxed{ac \equiv bd \pmod{n}}$

★ Prime Numbers:

An integer $p \geq 2$ is called prime number, if it is divisible by 1 and itself. Otherwise a number is called composite number.

For eg: (1) Prime nos are 2, 3, 5, 7, 11, 13, 17, 19, 23 .....

(2) Composite nos are 4, 6, 8, 9, 10, ...

Note: Every composite number can be expressed as product of prime integers.

eg: i, $10 = 2 \times 5$.

ii, $20 = 2 \times 10$
$= 2 \times 2 \times 5$.

iii, $35 = 5 \times 7$.

* Relatively Prime Numbers / Co-Prime Numbers:
Two numbers 'a' and 'b' are said to be relatively prime if they have no common divisors other than 1 (GCD(a,b)=1)
eg: 10 and 21 are relatively prime as GCD(10,21)=1.

* ~~Euler's ϕ-Function / Euler's Totient Function~~:
* Reduced Residue-System modulo m:
The reduced residue system modulo m, is the set of all elements from residue system modulo m $Z_m = \{0, 1, 2, \ldots m-1\}$ which are relatively prime to m.
i.e $S = \{x : GCD(x, m) = 1\}$.

* Euler's ϕ-Function / Euler's Totient Function:
The Euler's (pi) ϕ function of an Integer $n \geq 1$, is denoted by $\phi(n)$ and defined by the number of non-zero positive integers less than 'n' that are relatively prime to n.

eg: 1. $\phi(1) = 0$.
$\phi(2) = n(\{1\}) = 1$.
$\phi(3) = n(\{1, 2\}) = 2$.
$\phi(4) = n(\{1, 3\}) = 2$
$\phi(5) = n(\{1, 2, 3, 4\}) = 4$
$\phi(6) = n(\{1, 2, 3, 4, 5\}) = 2$
$\phi(7) = n(\{1, 2, 3, 4, 5, 6\}) = 6$

* Note:
1) If $n = p$ is a prime no, then Euler's ϕ function of p is
$\boxed{\phi(p) = p-1}$

2) If n is a number that can be expressed as a product of two relatively prime nos a, b, then Euler's ϕ function of n is
$\boxed{\phi(n) = \phi(ab) = \phi(a) \cdot \phi(b)}$

relatively prime nos

eg: i) $\phi(20) = \phi(4 \times 5) = \phi(4) \cdot \phi(5) = 2 \times 4 = 8$

ii) $\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 4 \times 6 = 24$.

iii) $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \times 4 = 4$.

03/08/22

★ Euler's Theorem:

Statement: Let n and a be positive integer which are relatively prime ($GCD(n,a) = 1$). Then,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n) \rightarrow$ is Euler's ϕ-function.

Proof: Given that $n, a > 0 \in Z$.

$$\boxed{GCD(n,a) = 1.}$$

Let us take Eulu's ϕ function

$$\boxed{\phi(n) = k.}$$

∴ Reduced residue system modulo n is,

$$S = \{a_1, a_2, a_3, \ldots a_{\phi(n)}\}.$$

or

$$S = \{a_1, a_2, a_3, \ldots, a_k\}.$$

~~Next, we know that,~~

Let us take $a \neq 0 \in Z \ni GCD(a,n) = 1$.

$$aS = \{aa_1, aa_2, aa_3, \ldots aa_k\}.$$

Next, we know that,

$aa_1 \equiv a_1 \pmod{n}$, $aa_2 \equiv a_2 \pmod{n}$ .... $aa_3 \equiv a_3 \pmod{n}$.

Now, by multiplication congruence modulo n, we get.

$$aa_1 \cdot aa_2 \cdot aa_3 \cdots aa_k \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_k \pmod{n}$$

$$a^k(a_1 a_2 a_3 \cdots a_k) \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_k \pmod{n}$$

$$a^k \equiv 1 \pmod{n}$$

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

classmate
Date
Page

p & a are relatively prime. (p not divides a)

★ Fermat's Theorem / Fermat's Little Theorem:

Statement: Let p be a prime number such that p∤a. Then,

$a^{p-1} \equiv 1 \pmod{p}$

or $a^{K} = p \pmod{p}$

Proof: Given that p is a prime number and p∤a.

Let us take Euler's ϕ function of p

$\boxed{\phi(p) = p-1}$

∴ Reduced residue system modulo p is

$S = \{a_1, a_2, a_3, \ldots a_{p-1}\}$.

Let us take $a \neq 0 \in Z \ni p \nmid a$.

$aS = \{aa_1, aa_2, aa_3, \ldots aa_{p-1}\}$.

Next, we know that,

$aa_1 \equiv a_1 \pmod{p}$, $aa_2 \equiv a_2 \pmod{p}$. ... $aa_{p-1} \equiv a_{p-1} \pmod{p}$

Now by multiplication congruence modulo p, we get

$aa_1 \cdot aa_2 \, aa_3 \cdots aa_{p-1} \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_{p-1} \pmod{p}$

$a^{p-1}(a_1 a_2 a_3 \cdots a_{p-1}) \equiv a_1 a_2 a_3 \cdots a_{p-1} \pmod{p}$.

$\boxed{a^{p-1} \equiv 1 \pmod{p}}$

eg: i) $4^{\phi(9)} \equiv 1 \pmod{9}$

$\phi(9) = n(\{1, 2, 4, 5, 7, 8\}) = 6$.

$4^6 \equiv 1 \pmod{9}$.

$(4^3)^2 \equiv 1 \pmod{9}$.

$(1)^2 \equiv 1 \pmod{9}$

$\boxed{1 \equiv 1 \pmod{9}}$.

ii) $3^{\phi(5)} \equiv 1 \pmod{5}$

$\phi(5) \equiv 4$

$3^4 \equiv 1 \pmod{5}$

$81 \equiv 1 \pmod{5}$.