Discrete mathematics

Introduction

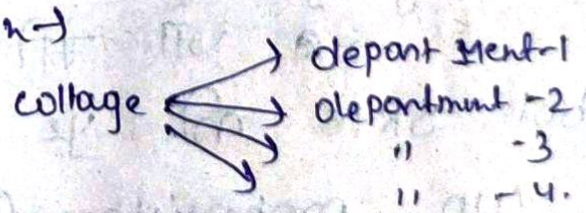
↳ Discrete mathematics is the branch of mathematics dealing with objects that can assumes only distinct & separated value.

In the other words.

The study of mathematical structure that are fundamentally discrete rather than continious.

Desi language → a. Discrete objects (गणना-अगणना) के study को EH Discrete mathematics कहते है।

Ex→



Ex- Google maps uses discreate mathematics to determine fastest driving routes and times.

Doing web search - in multiple languages at once, and returning a summary, uses linear algebra.

propositional logic → also known as sentential logic and statement logic, is the arm/limb of logic that studies ways of combining and/or developing entire propositions, statements or sentances to form more complicated propositions, statements or sentances, as well as the logical relationships and properties that are derived from these methods of combining or altering statements.

Ex→ Patna is a capital of Bihar.

→ 8 is odd number
5 is prime number.

Desi language.

→ जो भी sentence में हम ये bol skte की ye true or false hai wo propositional sentance hai

Ex- Happy Birthday! ⟶ exclamatory
She walk to School.

* they are not propositional sentance because we don't have know the value of "She" or "x" or "y". hence, we are unable to determine the truth value for the sentance.

Propopositional Equivalences

↳ Two logical expressions are said to be equivalent if they have the same truth value in all cases. sometimes this fact helps in proving a mathematical result by replacing one expression with another equivalent expression, without changing the truth value of the original compound proposition.

Types

1. tautology → A proposition which is always true, is called a tautology.
2. contradiction → A proposition which is always false, is called a contradiction
3. contingency → A proposition that is neither a tautology nor a contradiction is called a contingency.

Example
1. $p \vee \neg p$ is a tautology
2. $p \wedge \neg p$ is a contradiction.
3. $p \vee q$ is a contingency.

Desi language $p \leftrightarrow q$ logically p and q equal hoo. tae hai

Example -1.

Show that $(p \Leftrightarrow q) \Rightarrow (\bar{q} = \bar{p})$ is a tautology.

We can use a truth table to verify the claim

p	q	$p \Leftrightarrow q$	$\bar{p} \Rightarrow \bar{q}$	$\bar{q}$	$\bar{p}$	$(\bar{q} \Rightarrow \bar{p}) \equiv (\bar{p} \Rightarrow \bar{q})$ required
T	T	T	T	T	T	T
T	F	F	T	T	F	T
F	T	F	T	F	T	T
F	F	T	T	T	T	T

I am not saying that p is equal to q since p and q represent two different statements. they cannot be the same. what I am telling - they always produce the same truth value, regardless of truth values of the underlying propositional variables. that is why we write $p \equiv q$ instead of $p = q$

Some properties

1. commutative properties $p \vee q \equiv q \vee p$
$p \wedge q \equiv q \wedge p$.

2. Associative properties: $(p \vee q) \vee r \equiv p \vee (q \vee r)$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

3. Distributive laws: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

4. idempotent laws: $p \vee p \equiv p$,
$p \wedge p \equiv p$.

5. De morgan's law $\overline{p \vee q} \equiv \bar{p} \wedge \bar{q}$,
$\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$.

6. Law of the excluded middle, or inverse laws
$p \vee \bar{p} \equiv T$.
$p \wedge \bar{p} \equiv F$.

7. Identity laws: $p \vee F \equiv p$,
$p \wedge T \equiv p$.

8. Domination laws: $p \vee T \equiv T$,
$p \wedge F \equiv F$.

9. Equivalence of an implication and its contrapositive : $p \Rightarrow q \equiv \bar{q} \Rightarrow \bar{p}$.

10. writing an implication as a disjunction
$p \Rightarrow q \equiv \bar{p} \vee q$.

11. The negation of an implication
$\overline{p \Rightarrow q} \equiv p \wedge \bar{q}$

Ex→1 what is the negation of $2 \leq x \leq 3$?

→ The inequality $2 \leq x \leq 3$ means

$$(x \geq 2) \wedge (x \leq 3)$$

its negation, according to Demorgan's laws is

$$(x < 2) \vee (x > 3)$$

The inequality $2 \leq x \leq 3$ yields a closed interval. its negation yields two open intervals.

Key points.

1) Two logical statements are logically equivalent if they always produce the same truth value

- consequently, $p \equiv q$ is same as saying $p \Leftrightarrow q$ is a tautology.

- Besides distributive and Demorgan's laws, remember these two equivalences as well; they are very helpful when dealing with implications.

$$p \Rightarrow q \equiv \bar{p} \Rightarrow \bar{q}$$

$$p \Rightarrow q \equiv \bar{p} \vee q.$$

Quantifiers

→ In Discrete mathematics, as they help in translation of a

given logical statements.

* Quantifiers are words that refers to quantities such as "some" or "all". It tells for how many elements a given predicate is true.

Types
- Universal Quant... (∀) (for all)
- Existential Quan... (∃) (there exist / कोई)

Desi language → exact number बताए बताए / Quantity बताए जैसे – सब, कम, ज्यादा,

Ex→ all, some, many

"Can I have some water?"

Ex 1. Universal
1 real
2
↳ (for every) x (there is a y) such y≤x

सारे real no सब के लिए कम से कम एक y तो होगा या दो जो x से छोटा या equal हो गया.

Here for every → ∀ means All सब के लिए

~~for~~ there is a → एक या एक तो होगा या दो।

Ex-1. • ∀x (x² ≥ 0)

Explain → the square of any no is +ve

Universal

* The Ex- $\forall x$ (x is a square) predict it is $\forall$ or $\exists$ comparing with (x is rectangle)

Soln :: Since All squares are rectangles.

Ex-9 • $(x \geq x^2)$ is it is universal or existential.

Ans — :: Since $x=0$ is a solution there are many others.

so it is E

since if we take $x=-1$ then not satisfy so not $\forall$

Introduction to proff

→ mathematical proof is an argument we give logically to validate a mathematical Statement In order to validate a Statement we consider two things A Statement and logical operators.

Types of mathemical proofs:

1. proof by cases — In this method, we evalute every case of the statement to conclude its truethiness.

for example : for every integer n, the integer $n(n+1)$ is even

proff — if n is even, hence $n = 2k$ for some number k. now the statement becomes $2k(k+1)$ which divisible by 2, hence it is even

if n is odd hence $n = 2k+1$ for some number k, now the statement becomes: $(2k+1)(2k+1+1) = (2k+1)2(k+1)$ which is again divisible by 2 and hence in both cases we proved that $n(n+1)$ is even.

2. proff by contradiction → their we assume opposite of required statement and then we get wrong statement which assume.

ex — prove $\sqrt{2}$ is irrational let $\sqrt{2} = p/q \rightarrow$

Ans. →

$\sqrt{2} = p/q$

where p and q do not have factor.

on squaring both side

$2q^2 = p^2$

$p^2/2 = q^2$

so 2 divides p & q is a multiple

mathemical induction

The proff of mathematical induction consists of 3 parts.

let P(n) denote a statement (a formula/theorem) associated with n = 1, 2, 3. - - - - any natural number

Step 1 · verification.

P(n) should be true for n = 1, 2

Step-2 Inductive property

Step-3 Assume P(n) to be true for n = k, the we prove. P(n) to be true for n = K+1

Step-4 – (conclusion)

we conclude that results is true for for n ∈ N

Ex-1 prove by mathematical induction for all tve integers

$P(n) = n < 2^n$

Step 1 putting n = 1, 2 we see that

$1 < 2^1 = 2$

$2 < 2^2 = 4$

∴ The result is true for n = 1, 2

∴ P(1), P(2) one true.

Step-2 Assume result to be true for n = K

assume P(K) is true therefor $K < 2K$

Now multiply both side by 2

$\therefore 2K < 2^{K+1}$

But $K+1 \leq 2K$ → equal hoo taa hai 1 se pr फर्क नहीं करता तो बड़ी होगा

$K+1 < 2^{K+1}$ ∴ The result is true for n ∈ K+1

Direct proof

→ when we want to prove a conditional statement p implies q. we assumes that p is true, and follow implication to get to show that q is then true.

Ex→ If m is even and n is odd, then their sum is odd

val.

Soln proff since m is even and n is odd then their s is odd

Since m is even, there is an integer j such that $m = 2j$

Since n is odd, there is an integer k such that $n = 2k+1$ then,

$m+n = (2j)+(2k+1) = 2(j+k)+1$

Since $j+k$ is an integer, we see that $m+n$ is odd.

contraposition proff.

↳ proff by contraposition is a rule, of interference used in proffs where one infers a conditional statement from its contraposition. In other words, the conclusions "if A, then B" is inferred by constructing a proff of claim "if not B, then not A" instead.

Ex-1 $p = x+y \geq 2$ then $x \leq 1$ or $y \leq 1$

$\therefore p = x+y \geq 2$

$q \equiv x \leq 1$ or $y \leq 1$

$\sim p \equiv x+y < 2$ $\sim q \equiv x > 1$ & $y > 1$

So $x+y < 2 \equiv \sim p$ $\boxed{\sim q \to \sim p}$

Vacuous proff method?

↳ of an implication happens when the hypothesis of the implication is always false.

- A conditional statement $p \to q$ is true if p is false
- A conditional statement $p \to q$ is true if hypothesis is false.

if we can show p is false, then we have a proff, called vacuous proff, of the conditional statement $p \to q$.

Ex- prove that if $n^2 < 0$ then $1 = 2$ when n is a real number

→ since $n^2 \geq 0$ for every real number then the implication is vacuously true.

Trivial proff

A conditional statatement $p \to q$ is true if q is TRue.

→ Trivial proff of an implications happens when the hypothesis of the implication is always true.

Ex-1 use a trivial proff to show that if $n>1$ then $n^2 \geq n$ for all integer.

proff: Since $n^2 \geq n$ is always true As on LHS its n times n and on RHS it's on n, So by trival proff method is true.

Mistakes in proffs

(1) State something is true without adequate supports.

Ex By definition of even $A = 2k$ & $B = 2l$ for some integer k and l

Note $A+B = 2k+2l$

So $A+B$ is even

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

$= 2k^2 - 1 = k^2$

$k^2 - 1 = 0$

$k = +1, -1$

it is not give that.

$2k^2+1 \geq 0$

$2k^2+1 \geq 1$

$-\frac{1}{\sqrt{2}} \leq k \leq \frac{1}{\sqrt{2}}$

Chapter – 2

Recurrence Relation

A recurrence relation is an equation that defines a sequence based on a rule that gives the next term as a function of the previous terms

Ex- $x_{n+1} = 2 - x_n/2$

A recurrance relation is an equations that uses recursion to relate terms in a sequence or elements in an array.
It is a way to define a sequence or array in terms of itself.

Ex→ problem in which Recurrence Relation is use is tower of Hanoi puzzle.

Ex→ $T(n-1) + n$ for $n>0$ and $T(0) = 1$

Given $T(n) = T(n-1) + n$

$= T(n-2) + (n-1) + n$

$= T(n-k) + (n-(k-1)) \cdots (n-1) + n$

Substituting $k = n$ we get

$T(n) = T(0) + 1 + 2 + \cdots n = \frac{n(n+1)}{2} = 0$

Ex-2 what is the time complexity of tower of Hanoi problem

Soln For tower of Hanoi $T(n) = 2T(n-1) + c$ for $n>1$ and $T(1) = 1$

Solving this.

$$T(n) = 2T(n-1) + c$$
$$= 2(2T(n-2)+c) + c$$
$$= 2^2 T(n-2) + (c + 2c)$$
$$= 2^k T(n-k) + (c + 2c + \cdots + kc)$$

Substituting $k = (n-1)$, we get

$$T(n) = 2^{(n-1)} \times T(1) + (c + 2c + (n-1)c) = O(2^n)$$

Types of recurrence relation

1. Linear, 2. Non-linear 3. Homogeneous 4. Non-Hom-
5. constant coefficients vii) Variable coefficient:

Order of recurrence relation is the difference between the highest and the lowest subscript of a in a eqn

Ex- $2a_n = \frac{3}{2} a_{n-1} + n a_{n-2}$

order $= n - (n-2)$

$= n - n + 2$

$= 2$

} soln of Recurrence relat

$a_n = a_n^h + a_n^p$

↳ Homogeneous. ↳ Part, Particu

modeling using Recurrence Relation

Someone deposite 100 in a saving account at a bank yielding 5% per year with interest compounded annually. How much money will be in the account after 30 years?

Soln let P_n denote the amount in the account after n years

How can we determine P_n on the basis of P_{n-1}?

we can derive the following recurrence relation

$$P_n = P_{n-1} + 0.05 P_{n-1} = 1.05 P_{n-1}$$

The initial condition is $P_0 = 10,000$

then we have

$$P_1 = 1.05 P_0$$
$$P_2 = 1.05 P_1 = (1.05)^2 P_0$$
$$P_3 = 1.05 P_2 = (1.05)^3 P_0$$
$$\vdots$$
$$P_n = 1.05 P_{n-1} = (1.05)^n P_0$$

∴ use this formular to calulate

$$P_{30} = (1.05)^{30} \times 100 = 432.19$$

homogeneous linear equation

Recurrence relations with constant coefficients.

↳ follow the same proces which we followed in the differential equation while find the C.F.

→ for homogenous

→ First find the character eqn

→ The eqn is converted in polynomial

eqn

→ find the roots of the eqn.

case-1. Roots are real unequal :-

let root are r_1 & r_2

So soln will be :-

$$a_n = c_1 (r_1)^n + c_2 (r_2)^n, \quad c_1, c_2 \rightarrow \text{const}$$

case II Roots are real and equal :-

let root be r_1 & r_2

and $r_1 = r_2 = r$

So soln $= a_n = (c_1 + n c_2)(r)^n$

if soln are $r_1, r_2, r_3, r_4, \ldots$

and $r_1 = r_2 = r_3 = r_4 = \ldots = r$.

then

$$\text{soln} = a_n = (c_1 + n c_2 + n^2 c_3 + n^3 c_4 + \ldots) r^n$$

case -III roots are complex / Imaginary

$\alpha \pm i\beta$

then soln $= a_n = \rho^n [c_1 \cos n\theta + c_2 \sin \theta]$

where $\rho = \sqrt{\alpha^2 + \beta^2}$

$\theta = \tan^{-1}(\beta/\alpha)$

Ex-1 $a_n = 6a_{n-1} - 9a_{n-2}$

put $a_n = r^n$

$r^n = 6r^{n-1} - 9r^{n-2}$

divide by r^{n-2}

$r^2 = 6r - 9$

$r^2 - 6r + 9 = 0$

$(r-3)^2 = 0$

$r = 3, 3$

$r_1 = 3$ & $r_2 = 3$ & $r_1 = r_2 = r = 3$

So soln = $a_n = (c_1 + nc_2)3^n$

Q find the soln of $a_n = a_{n-1} + 2a_{n-2}$ $\{a_0 = 2, a_1 = 7\}$

Step-1 put $a_n = r^n$

So, $r^n = r^{n-1} + 2r^{n-2}$

Step-2 Divide the eqn with lowest power term Here (r^{n-2})

So, $= \frac{r^n}{r^{n-2}} = \frac{r^{n-1}}{r^{n-2}} + \frac{2r^{n-2}}{r^{n-2}}$

$= r^2 = r + 2$

Step-III find the roots

$r^2 - r - 2 = 0$

$r^2 - 2r + r - 2 = 0$

$r(r-2) + 1(r-2) = 0$

$= (r+1)(r-2) \Rightarrow r = 2, -1$

$\therefore \quad C_1(2)^n + C_2(-1)^n = a_n$

Given that at $n=0 \quad a=2$

So, $\quad 2 = C_1(2)^0 + C_2(-1)^0$

$C_1 + C_2 = 2 \quad \text{---} (1)$

at $n=1 \quad a=7$

$7 = C_1(2)^1 + C_2(-1)^1$

$7 = 2C_1 - C_2 \quad \text{---} (2)$

Eq (1) + Eq (2)

$(2 - C_1 - C_2) + (7 + C_2 - 2C_1)$

$9 - 3C_1 = 0$

$C_1 = 3$

put in 1st $\quad 3 + C_2 = 2 \quad C_2 = -1$

So, $\quad a_n = 3(2)^n + (-1)^{n+1}$

Generating function

→ In mathematics a generating function is a way of encoding an infinite sequence of number (a_n) by treating

them as the coefficient of a formal power series. This series are called generating function of the sequence

formal power series → records sequence of coefficients.

Ex-1 what is the sequence represented by the generating series $3+8x^2+x^3+\frac{x^5}{7}+100x^6+\cdots$?

we just read off the coefficients of each x^n term so $a_0=3$ since the coefficient of x^0 is 3 ($x^0=1$ so this is the constant term.) when is a_1? it is Not 8, since 8 is the coefficient of x^2 so 8 is the term a_2 of sequence. To find a_1 we need to look for the coefficient of x^1 which in this case is 0. So $a_1=0$. continuing, we have $a_2=8$, $a_3=1$, $a_4=0$, and $a_5=1/7$ so we have the sequence

$3, 0, 8, 1, 1/7, 100, \ldots$

Always start our sequence with a_0

Counting principal and relation

① principal of inclusion & exclusion

inclusion → Let A & B be any finite sets then

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

for any finite sets A, B, C.

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

Q1 In a survey of group of 50 people, it is found that 60 like egg and 30 like fish find pertage of people like both egg & fish.

$n(E) = 60$
$n(F) = 30$
$n(E \cap F) = ?$
$n(E \cup F) = 80$

$\therefore n(E \cup F) = n(E) + n(F) - n(E \cap F)$

$80 = 60 + 30 - n(E \cap F)$

$n(E \cap F) = 10$

Ex-2 In a survey of the usage of three toothpaste A, B, C. It is found that 60 people like A-55, likeB-40, like C-20, like A & B-35, $B \cap C = 15$ $A \cap C = 10$ $A \cap B \cap C = 10$

Ans

$n(A) = 55$ $n(B) = 40$, $n(C) = 20$ $n(A \cap B) = 35$
$n(B \cap C) = 15$ $n(A \cap C) = 10$ $n(A \cap B \cap C) = 10$

$\therefore n(A \cup B \cup C)$

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

$= 55 + 40 + 20 - 35 - 15 - 10 + 10$

$= 5 + 40 + 20$

$= 65$

*** Pigeonhole ***

If n pigeons are assigned to m pigeonholes and $m < n$ then at least one pigeonhole contains two or more pigeons.

Proof → Suppose each pigeonhole contains atmost one pigeon. Then m pigeons will be accomodated in m pigeonhole, one pigeon in each pigeonhole. But $m < n$, not all pegeons have been assigned pigeon holes

This is contradiction.

Hence there is atleast one pigeonhole which contains two or more pigeons.

Eg- If 4 colours are used to paint 50 bicycles show that atleast 8 of them will be of same colour.

→ Let colour denote pigeonholes (m) and bycycle denote pigeons (n) and $m < n$

$\frac{50}{7} = 7$ ∴ 7 bicycles each of 7 colours remainder 1 will be a colour from the 7

∴ 8 bicycles may have a same colour.

- The extended pigeonhole principal

Eg→ Show that in a group of 50 students atleast 5 are born in same month.

→ There are $n=12$ (months) pigeonhole and $Kn+1=50$ pigeons.

∴ $K \times 12 + 1 = 50$

$12K = 49$

$K = 49/12 = 4$ } remainder = 1

∴ Atleast 4+3 = 7 students are born in same month.

Relation

Any subset of certain product A×B will be a relation from set A to set B

Domain → collection of first elements of ordered pair in a Relation.

Range - collection of second elements of ordered pair in a Relation.

$n(A) = m$ $n(B) = n$

∴ Total Relation = 2^{mn}

properties of Relation

- = is Reflexive (2=2
- = is Symmetric (x=2 implies 2=x)
- = is transitive (2<3 and 3<5 implies 2<5)
- < irreflexive (2<3 implies 2≠3)
- ≤ is antisymmetric (x≤y and y≤x implies x=y).

Equivalent Relation

A Relation which is reflexive, symmetry and transitive all.

Ex-1

$R : R \to R$ $\quad aRb$ $(a-b)$ is div by 5.

∴ soln

① Reflexive $\quad aRa \Rightarrow a-a$ div by 5

② Symmetric $\quad aRb = (a-b)$ div by 5

$\frac{b-a}{5}$ = divisible 5 then

$\frac{a-b}{5}$ is div to $\quad bRa$
$\quad aRb$

both so symmetric.

Transitive $\quad aRb \longrightarrow a-b = 5I_1 \quad a-c = 5(I_1+I_2)$

$bRc \longrightarrow b-c = 5I_2 \quad a-c = 5I_3$

$\therefore aRc$

Hence it is equivalance.

Combing Relation

Relation from A to B are subsets of $A \times B$ two relation from A to B can be combined in any way two sets can be combined. The composite of R and S is the relation consisting of ordered pairs (a,c) where $a \in A$, $c \in C$, and for which there exist

an element B such that (a,b) R and (b,c) S.

Ex→ Let A = {1,2,3} & B = {1,2,3,4}

$R_1 = \{(1,1), (2,2), (3,3)\}$

and $R_2 = \{(1,1), (1,2), (1,3), (1,4)\}$

combined them ⓐ $R_1 \cup R_2$ ⓑ $R_1 \cap R_2$

Ans. $R_1 \cup R_2 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (3,3)\}$

$R_1 \cap R_2 = \{(1,1)\}$.

Relation as a matrices:

A Relation R is defined as from set A to set B, then the matrix representation of Relation is $M_R = [m_{ij}]$ where

$M_{ij} = \{1, \text{if } (a,b) \in R$

$0, \text{if } (a,b) \in R\}$

properties

1. A Relation R is reflexive if the matrix digonal element are 1.

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

2. A Relation R is irreflexive if the matrix diagonal element are 0.

3. A Relation R is symmetric if transpose of Relation matrix is equal to its original Relation matrix i.e. $M_R = M_R(T)$

4. A Relation R is antisymmetric if their $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$

5. A Relation follows Join property the Join of Matrix M_1 & M_2 is $M_1 \vee M_2$ which is represented as $R_1 \cup R_2$ in terms of Relation.

6. A Relation follows meet property the meet ~~property~~ of matrix M_1 & M_2 is $M_1 \wedge M_2$ which represented as $R_1 \cap R_2$ in terms of Relation

Ex- 1. matrix Representation $A = \{a_1, a_2, \ldots a_m\}$
$B = \{b_1, b_2, \ldots b_n\}$

M_R = M×n matrix

$M_{ij} = 1$; if $(a_i, b_j) \in R$.

$M_{ij} = 0$; if $(a_i, b_j) \notin R$

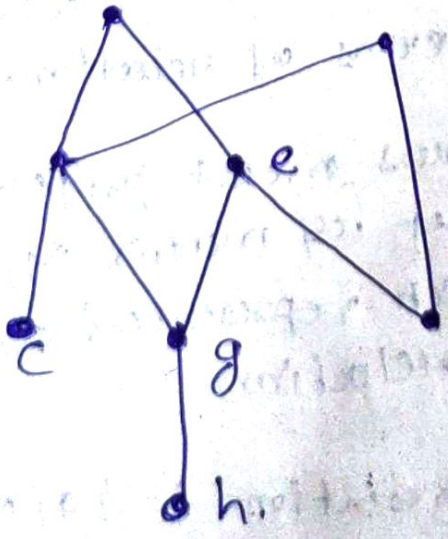
$A = \{1, 2, 3\}$

$R_1 = \{(1,2), (1,3), (2,3), (3,1)\}$

$$M_{R_1} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Hasse diagram

A Hasse diagram is a graphical representation of the relation of elements of a partially ordered set (Poset) with an implied upward orientation.



Ex-1

Ex-1 Draw Hasse diagram for (3, 4, 12, 24, 48, 72)

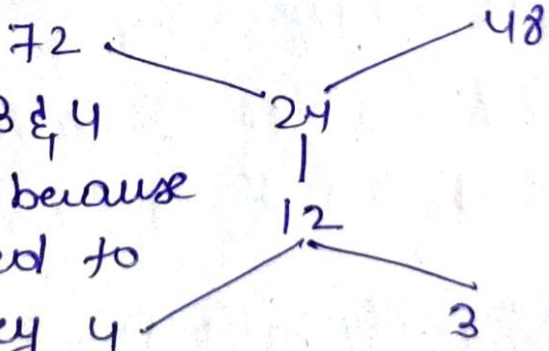
Explanation

According to above given question first, we have to find the poset for the divisibility.

let set is A.

A = {(3 < 12), (3 < 24), (3 < 48), (3 < 72), (4 < 12), (4 < 12), (4 < 48), (4 < 72), (12 < 24), (12 < 48), (12 < 72), (24 < 48), (24 < 72)}

So now the Hasse diagram will be



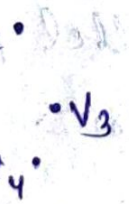
In this diagram 3 & 4 are at same level because they are not related to each other and they 4 are smaller than other elements in the set The next succeeding element for 3 and 4 then 24 is divisible by 3, 4 & 12 Hence, it is placed above 12. 24 divides both 48 and 72 but 48 does not divide 72. Hence 48 and 72 are not joined.

Use → communication — Ex- Google map.
→ computation → cloud computation.

Graph → It is collection of vertices and edges and denoted by: $G = (V, E)$ → set of edges.
↓
Set of vertices

Note: In a graph set of edges may be empty but set of vertices never by empty

- A graph in which set of edges ~~may be~~ is empty is known as Null graph



* Directed and indirected Graph:

Directed: A graph in which direction is given is said to be directed otherwise undirected

Simple graph → A graph is said to be simple if it do not have self loop as well as parallel edges.

Multi Graph - A graph is said to be multigraph in which it have left loop / parallel edge or both.

~~Pseudo Graph - A graph is said to be multigraph in which it have left loop / parallel edges or both.~~

Pseudo Graph → An undirected graph is said to be pseudo if it is having selfloop or parallel edge or both.

self loop - An edge whose starting and end vertices are same

parallel edges - Two or more edges are said to be parallel if their starting or end point is same.

Degree of edges:

No of edges associated to a vertex is known as its degree

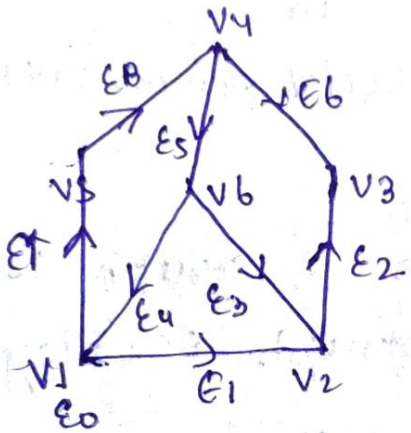
Indegree - (d-): No of edges coming in that vertex.

out degree : No of edges going out of vertex.

* Self loop is counted twice in the degree of vertex.

Adjacent – vertex
incident – edges.

Q Find Indegree outdegree, degree for each vertices in a given graph



Sum of degree of all vertices
$= \sum d(v_i) = 20$

No of Edges $|E| = 10$

Note– The sum of degree of all vertices of graph is twice the no of ~~total~~ edges in the graph this is known as Handshaking.

Q if the degree of vertices of graph is 17 then the no of edges in the graph?

$$\sum d(v_i) = 2|i|$$

$$17 = 2|E|$$

$|E| = 8.5$, Not possible such graph not exists.

Thorem

Note: The no of odd degree vertices in a graph is even.

Note: A vertex is said to be odd if its degree is ~~odd~~.

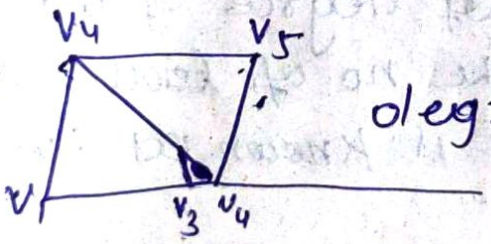
or

A vertex is said to be even if its degree is even

* Regular graph - A graph is said to be regular graph if degree of each vertices is equal

Ex→ 

$d(v_1) = 1 = d(v_2) = 1$



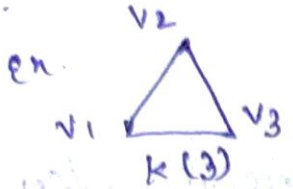
degree of each is 1.

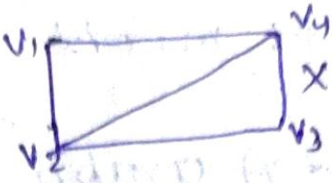
complete Graph: → ~~vertices~~ graph is said to be complete if for every pair of vertices there exist an edges between then is said to be complete

A complete graph with n vertices is denoted by K_n. → denotation of K graph with n vertices.

A complete graph with n vertices is denoted by K_n.

Ex.

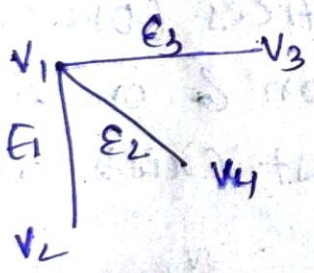




Ex.

Bipartite Graph:

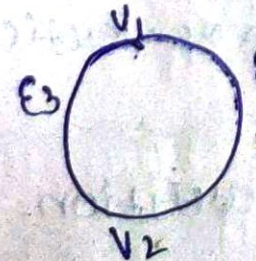
Let $G = (V, E)$ be a graph, the graph is said bipartide graph if the set of vertices can be partition into disjoint subset of V_1 such that for every edges one of the end point lies in one set another in the second set.

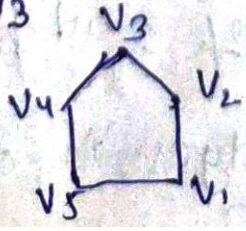


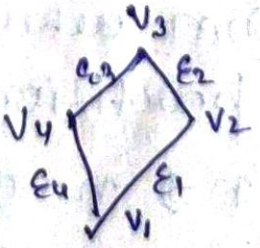
$V_1 = \{v_1\}$

and $\forall$ edge one of end point lies in V_1 and other in V_2.

Hence give graph is Bipartide graph.







$V_1 = \{v_1, v_3\}$

$V_2 = \{v_2, v_4\}$

Bipartite.

v_1, v_3, v_5 — odd path

v_2, v_4, v_5 — Take even path

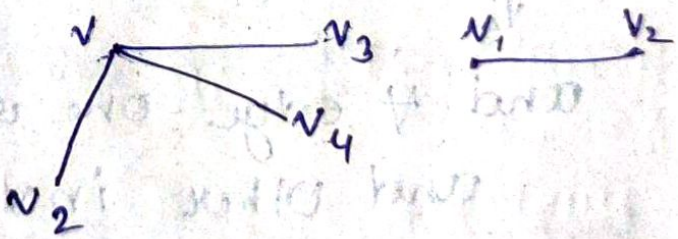
C_n = { Bip : n is even
Not Bip : n is odd

cycle Graph – A graph in which degree of all vertices is 2.

C_n → cycle graph n is no of vertices in the graph.

* complete Bipartite Graph

→ A Bipartite graph is said to be complete Bipartite graph if of every pair of vertices (one vertex is form one partition & one form another), there must exists an edge b/w them.



A complete Bipartite graph is denoted by $K_{m,n}$ where m ⇒ no of vertices in Ist partition

n ⇒ no of 2nd partition.

Note

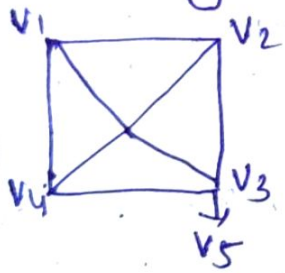
i) The no of edges in complete bipartite graph is mxn

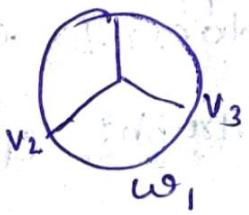
imp In a complete no of edges in complete bipartite graph is $m \times n$.

2) In a complete Bipartite graph m vertices having degree n & n vertices having degree m.

3) The "max m no of edges" in a complete bipartite graph is $\frac{n^2}{4}$

4) wheel Graph: A graph is said to be wheel graph if it is cycle graph & there exists on vertex which is connected to each and every vertices of graph





W_n = no of vertices

* theorem / Proff: the no of odd degree vertices in a graph is even.

$G = \{(V, E)\}$ Let V_e = even vertices

V_o = odd vertices

$V = V_e \cup V_o$

$V = V_e \cup V_o$

By hand Shaking thorem (i) $\sum d(V_i) = 2|E|$

$\therefore$ By $2|E| = \sum d(V_i)$

$= \sum d(V_i) + \sum d(V_o)$

$2|E| = 2K + \sum d(V_0)$

$\sum d(V_0) = 2(|E| - K)$ where K is an integer

= even no.

∵ The no of odd degree vertices will Always even no.

* Matrix representation of graph:-

i) incident matrix:

Note – if diagonal elements are zero then there doesn't exists a self loop.

For multi graph: $a_{ij} = \begin{cases} \gamma : \text{if} \longrightarrow \text{'}\gamma\text{'} \text{ edge} \\ 0 : \text{otherwise.} \end{cases}$

for directed graph $a_i = \begin{cases} 1 : \text{if for outward edge from } V_i \text{ to } V_i \\ 0 \text{ otherwise} \end{cases}$

2.) Adjoincy matrix:– $a_{ij} = \begin{cases} 1 \text{ if } V_i, V_j \text{ are complete connected by an edges} \\ 0 : \text{otherwise} \end{cases}$

ii)

Incident matrix :—

a_{ij} = { 1, if e_j is inward in v_i
-1, if " is outward in v_i
0 otherwise.

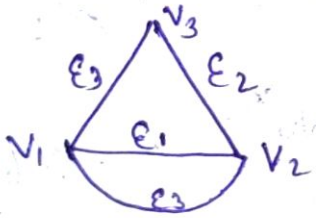
OR a_{ij} = { 1 ; for outward edge
0 otherwise.

i) Sum of rows of else matrix give degree of that vertices.

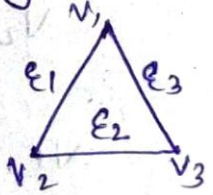
ii) If two columns are having same value then there exist a parallel edge b/w them.

Q Draw incident & Adjency matrix

(1)



(2)



I Adjency matrix :—

	V_1	V_2	V_3
V_1	0	2	1
V_2	2	0	1
V_3	1	1	0

Adjency matrix.

	V_1	V_2	V_3
V_1	0	1	1
V_2	1	0	1
V_3	1	1	0

II Incident matrix

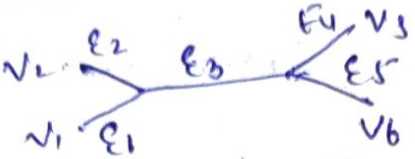
	e_1	e_2	e_3	e_4
V_1	1	0	1	1
V_2	1	1	0	1
V_3	0	1	1	0

Incident matrix.

	e_1	e_2	e_3
V_1	1	0	1
V_2	1	1	0
V_3	0	1	1

connectivity in graphs :-

1) paths : A sequence of edges started from vertex and travel to another vertex through edges is known as a path.



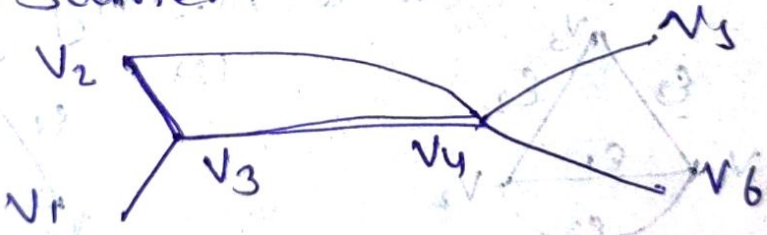
for multi-graph

from v_2 to v_5 ⇒ path ⇒ $v_2 \to e_2, v_3 - e_3\ v_4 - e_5$

$e_2\ e_3\ e_5$ → (for simple graph)

v_2, v_3, v_4, v_5 (non-unique)

2) circuit :- A closed path is said to be a circuit or a path in which initial and terminal vertices are same.



for circuit length > 1 Ex :- $v_2\ v_3\ v_4\ v_2$ a circuit of length (3) edges.

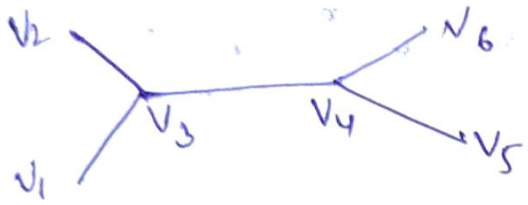
if length ≤ 1 } (Not a circuit)

3) cut-vertex :- The set of vertices whose removal from the graph leaves the graph disconnected.

If there is atleast one path b/w the two vertices then it is said to be

connected otherwise disconnected.

* cut vertices in a cycle graph is zero.



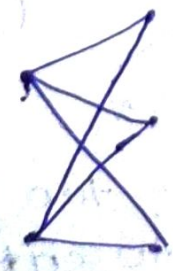
cut vertices v_3, v_4 and $v_3 - v_4$

4) Cut-Edges - The set of edges or edge whose removal from graph leaves the graph disconnected.

5) Vertex connectivity - The minimum no of vertices whose removal from the graph leaves the graph disconnected.

6) Edge connectivity - minimum no of edges whose removed from the graph leaves the graph disconnected.

$\underline{\Theta}$ K_{23} (complete Bipartite Graph)



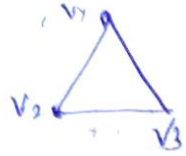
Edge connectivity = 2

vertex " = 2

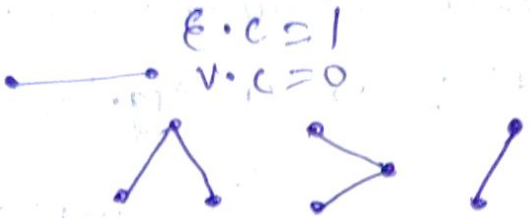
for $K_{m,n} = \{$ minm of $\{m,n\}$

then Edge con and vertex

complete graph



V·C = 0
E·C = 2



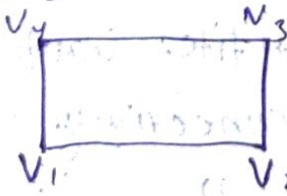
V. Imp

Graph Isomorphism

A pair of graph is said to be isomorphism to each other if they are same in each and every manner i.e. no of vertices, no of of edges, same no of same degree vertices, no of adjacent-vertex.

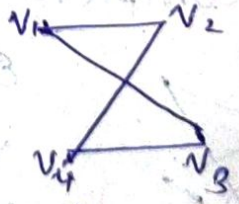
$C_1(a, E)$

Ex



=

$C_2 = (V, E)$



(isomorphic)

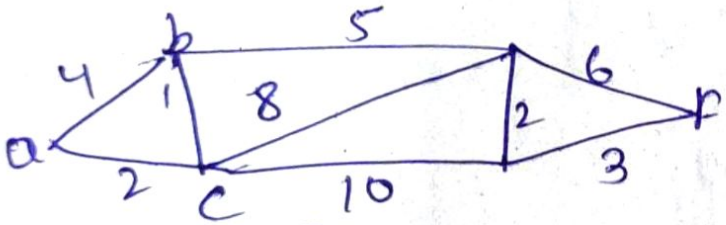
Let $G_1 = (V, E)$ $G_2 = (V, E)$ be two graph G_1 & G_2 are said to isomorphic to each other if there exists a one-one, onto function $f: V \to V$ which preserve adjency property.

if adjency matrix of 2 graph is same then ~~isomorphic~~ isomorphic.

1) Note if adjency matrix of two graph are same then the ~~matrix~~ graph is isomorphic graph.

2) if adjency matrix of two graph are not same then the graph may or may not be isomorphic.

Q Find the shortest path in the given weighted graph from A to F.



(1) (a) → (b) = 4 ✗
(a) → (c) = 2 ✓
(minimum one selected every ~~thing~~ time.

(2) (c) → (b) = 1+2 = 3 ✓
(c) → (d) = 2+8 = 10 ✗
(c) → (e) = 10+2 = 12 ✗

(3) (b) → (d) 3+5 = 8 (Not included because already selected path.

(4) (d) → (e) = 10 ✓
(d) → (f) = 14 ✗

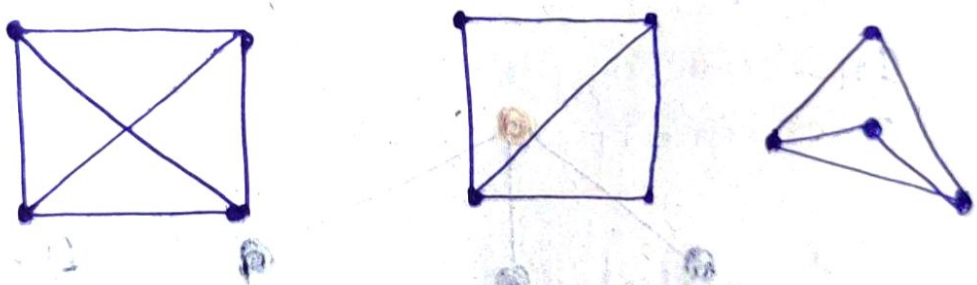
(5) (e) → (f) = 13

(a) — (c) — (b) — (d) — (e) — (f)

Graph - II

Planner graph → A planar graph is a graph that can be embedded in the plane i.e. it can be drawn on the plane in such a way that its edges ~~intersect~~ intersect only at their endpoints. In other words, It can be drawn in such a way that no edges cross each other

Eg.



Euler formula

Face + vertex = Edge + 2

Eg A cube, for example has 6 face 8 vertices and 12 edges and satisfies this formula.

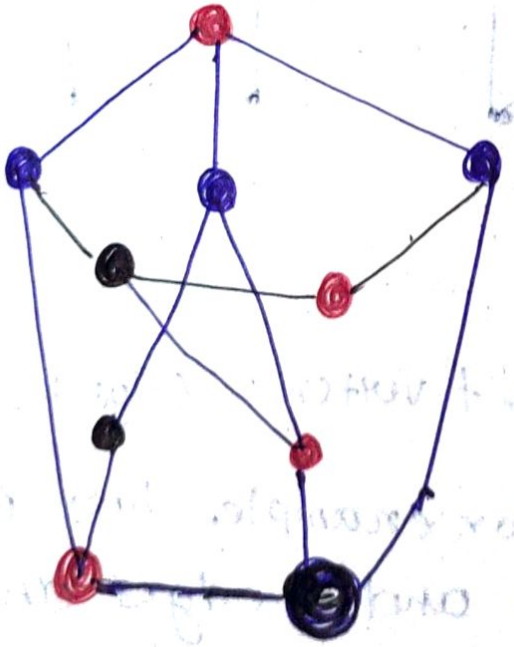
colouring of graph and chromatic number.

Colouring of graph and chromatic number

A graph colouring is an assignment of labels, called colours, to the vertices of a graph such that no two adjacent vertices share the same colour.

The chromatic number $\chi(G)$ of a graph G is the minimal number of colours for which such an assignment is possible.

Ex-



~~0 → red~~

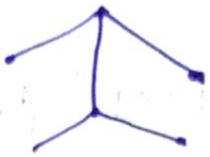
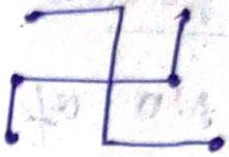
~~Adjacent vertex~~

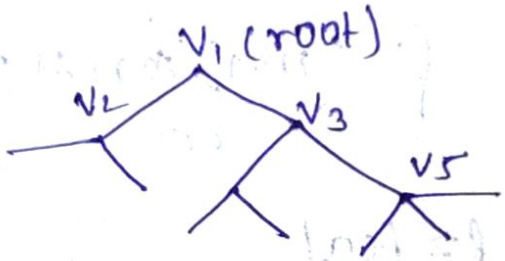
Aman

if you want to support Paytm - 9142513154.
9142513154

Tree graph and its properties.

A connected graph without any circuit is said to be a tree.

Ex-   

Rooted tree: 

leaf: The vertices which do not have any child.

Siblings - The vertices which have some parent then they are siblings.

* M-array - tree:
  A rooted tree in which each of the internal vertices is having atmost m- child.

* full m-ary tree:
  A rooted tree in which every internal vertices or node is having either zero or m child.

* complete m-ary tree: A complete m-ary tree is a rooted tree in which all the leafs lie on the same level.

* maximum level = height of trees.

Balanced tree → A tree is said to be balance if all the leaves of the tree lies on the level is either h or h-1

Properties

No of vertices ($n = m*i+1$)

$$l = \left[\frac{(m-1)*n+1}{m} \right]$$

where l = leaf

i = internal vertices

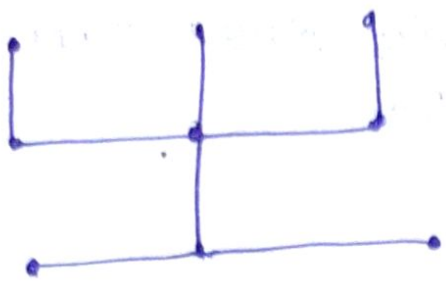
n = represent no of vertices in full m-ary tree

3) Spaning tree

Let G be a connected graph a Sub graph of G is said to be a Soapaning tree if :-

1) it will consist all the vertices of G
2) it do not have any circuit
3) it must have n-1 edge

if n vertices their should be n-1 edges



Minimum Spanning tree
→ spanning tree with max^m weight.

~~i) Prefix~~

infix and postfix notation.

→ In the infix expression, the operator appears between the operands and in infix notation if the operator appears before the operands in the expression. for the conversion b/w them two stacks are used efficiently.

In postfix expression, the operator appear after the operands.

1. Ex- Evaluate the expression a/b+c*d-e in postfix notation.

→ The expression = a/b+c*d-e

= {(ab/)+(cd*)}-e

= {(ab/)(cd*)+}-e

= {(ab/)(cd*)+}e-

So the output is: ab/cd*+e-

Note - postfix is also known as reverse polish notation

i/ abc++

Input

output (a+(b+c))

Eg ab*c+

((a*b)+c)

Eg which of the following is an infix expression?

a) (a+b)*(c+d)
b) ab+c*
c) +ab
d) abc+*

(a+b)*(c+d) is an infix expression
+ab is a prefix expression and
ab+c* postfix expression.

4. what is the time complexity of an infix to postfix conversion algorithm

Ans — O(N).

Number theory and its application in cryptography.

1. Divisibility and modular arithmetic

if $a|b$ then $b|a$ is an integer. if (a) does not divide b, we write $a|b$. Two integers are congruent mod m if and only if they have the same remainder when divided by m ....

if $a \equiv b \pmod m$, then $c+a \equiv c+b \pmod m$, where c is an integer.

we say that $a|b$ (a divides b) of $\exists$ an integer c such that $\frac{b}{a} = c$, $c \in \mathbb{Z}$

Eg: check 3 divides 7 and 12.

$7/3 = 2.33$ 3 does not divides 7.

$\frac{12}{3} = 4$ 3 divide 12

Properties of division

if a divide b and a divide c, then $a|b \pm c$

if a divide b, then a divide bc where $c \in \mathbb{Z}$

" a " " and $B|C$ then $a|c$

Division Algorithm

Let a be an integer and 'd' be a +ve integer then exists integer 'q', 'r' such that $\boxed{a = dq + r}$

Q what are quotient and remainder when 101 is divided by 11.

Soln: $101 = 11 \times 9 + 2$

$q = 9$ $r = 2$.

G.C.D of two Number a & b

Let 'a' and 'b' be two numbers then we say that a is the GCD if d/a & d/b it is the largest no which divides both the numbers.

* Ex- Find the GCD of 24 and 36?

$$24\overline{)36}\,(1$$
$$\underline{24}$$
$$12\overline{)24}\,(2$$
$$\underline{24}$$
$$\times\times$$

G.C.D.

* find the G.C.D (474, 662)

$$474\overline{)662}\,(1$$
$$\underline{414}$$
$$248\overline{)414}\,(1$$
$$\underline{248}$$
$$166\overline{)248}\,(1$$
$$\underline{166}$$
$$82\overline{)166}\,(2$$
$$\underline{164}$$
$$2$$

Benezout's theorem

If 'a' & 'b' are the integers then their exists integers s and t such that.

GCD $(a, b) = as + bt$

where

s and t are called Benzouts constants coefficient (may be +ve or -ve)

Ex- GCD (662, 414)

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$2 = 166 - 82 \cdot 2$$
$$= 166 - [248 - 166 \cdot 1]2 = 3 \cdot 166 - 248 \cdot 2$$

$= 3.414 - 5.662$

GCD $(414, 662) = s(414) + t(662)$

$\Rightarrow s = 8$ & $t = -5$

Inverse modulo m

$a \cdot \bar{a} = 1 \pmod m$

Q find the inverse of $3 \pmod 7$

Soln Let $\bar{a}$ be the inverse of 3

$3\bar{a} = 1 \pmod 7$

$7 \mid (3\bar{a} - 1)$

$\bar{a} = 1$ ✗ $\bar{a} = 4$ ✗

$\bar{a} = 2$ ✗ $\bar{a} = 5$ ✓

$\bar{a} = 3$ ✗ ∵ Inverse of 3 is 5 under $(\text{mod } 7)$

Q Inverse of $3 \pmod 4$.

Let $\bar{a}$ be inverse of 3

$3\bar{a} \equiv 1 \pmod 4$

$4 \mid (3\bar{a} - 1)$ ∵ inverse of 3 is 3 under mod 4.

Linear congruence

A congruence of the form $ax \equiv b \pmod m$ where m is +ve integer and a & b are integers and x is a variable is linear congruence.

Q what is solution of $3x \equiv 4 \pmod 7$

$7 \mid 3x - 4$

$x = 1$ ✗ $x = 4$ ✗

$x = 2$ ✗ $x = 5$ ✗

$x = 3$ ✗ $x = 6$ ✓

GCD $(3, 7) = 1$ ∵ solution always exists

public

3 | 7 | 2
6
1 | 3 | 3
3
1

$1 = 3 \cdot 2 + 1$ — (1)

$1 = 7 + (3 \cdot -2)$

mod of 3 is -2

Now multiply above congruence with -2

$-6x \equiv 8 \pmod 7$

→ make it +ve by adding 7.

$x \equiv 6 \pmod 7$

$[6] = \{\ldots -8, -1, 6, 13, 20 \ldots\}$

Chinese Remainder theorem

In number theory, the chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by product of these integers, under the condition that the divisors are pairwise coprime.

Step-

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

Check $(m_1, m_2) = 1$ $(m_2, m_3) = 1$

$(m_3, m_1) = 1$

find $m = m_1, m_2, m_3$

find $m_1 = \frac{m}{m_1} = m_2 \cdot m_3$ $m_3 = \frac{m}{m_3} = m_1 \cdot m_2$ $m_2 = \frac{m}{m_2} = m_1 m_3$

Finding congruency $m_1y_1 \equiv 1 \pmod{m_1}$, $m_2y_2 \equiv 1 \pmod{m_2}$, $m_3y_3 \equiv 1 \pmod{m_3}$ find $\Rightarrow y_1\, y_2\, y_3$

* Now solve for

$$x \equiv M_1a_1y_1 + m_1a_2y_2 + \cdots + M_na_ny_n \pmod{m}$$

Q $x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$

$a_1 = 2 \quad a_2 = 1 \quad a_3 = 3$

$m_1 = 3 \quad m_2 = 4 \quad m_3 = 5$

* $(3,4) = 1$, $(4,5) = 1$ $(5,3) = 1$

m_1, m_2, m_3 are pair-wise co-prime

(*) $m = m_1 \cdot m_2 \cdot m_3 = 60$

$m_1 = 20 \quad m_2 = 15 \quad m_3 = 12$

$m_1y_1 \equiv 1 \pmod m$

$20y_1 \equiv 1 \pmod 3$

$y_1 = 2$

(*) $M_2y_2 \equiv 1 \pmod 4$

$15y_2 \equiv 1 \pmod 4$

$y_2 \equiv 3$

(*) $m_3y_3 \equiv 1 \pmod 5$

$12y_3 \equiv 1 \pmod 5$

$y_3 = 3$.

(*) $x \equiv 20 \cdot 2 \cdot 2 + 15 \cdot 2 \cdot 3 + 12 \cdot 3 \cdot 3 \pmod{60}$

$\equiv 233 \pmod{60}$

$x \equiv 53 \pmod{60}$ Ans 53

Cryptography

→ it is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

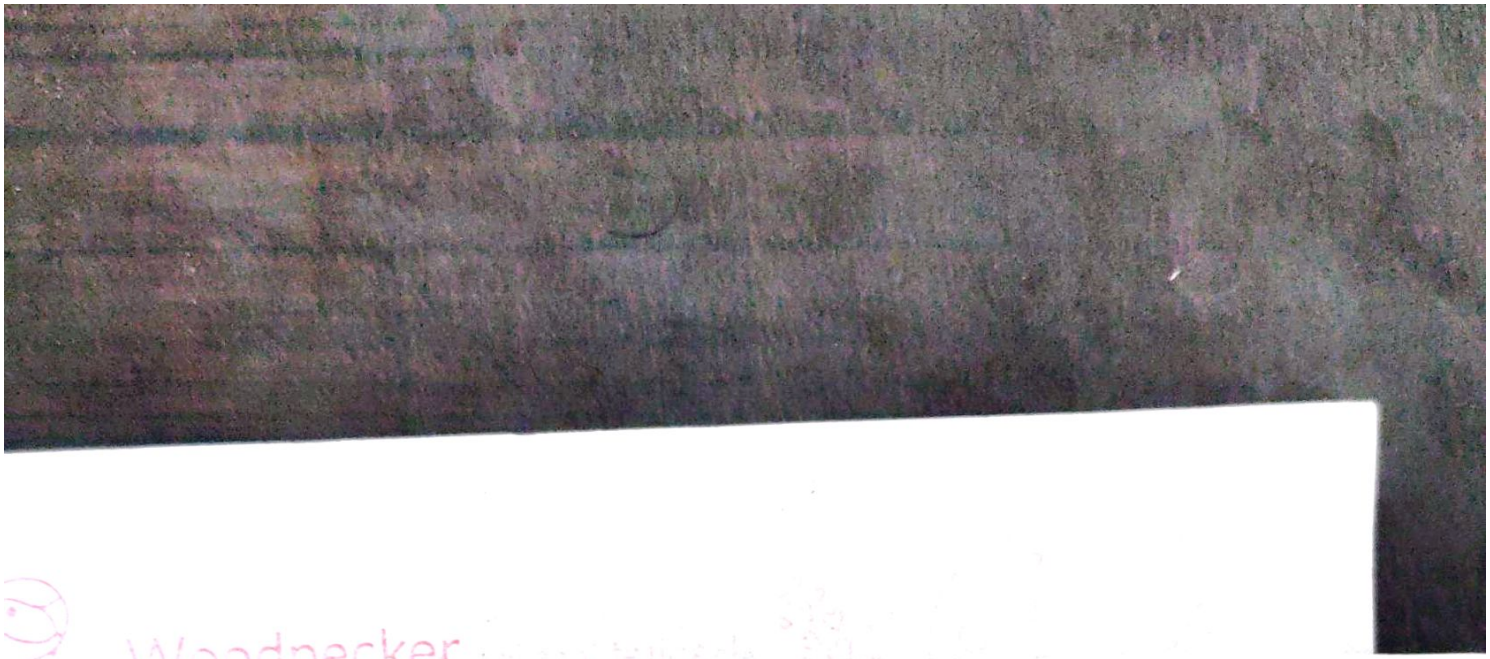
Cryptography not only protect data from theft and alterations, but can also be used for user authentication

Modern cryptography concerns with confidentiality - Information cannot be understood by anyone.

Eg- banking transaction cards, computer passwords, and e-commerce transactions.

There three types of cryptography

→ Symmetric-key Cryptography
→ Hash function
→ Public-key cryptography.



Woodpecker

(1) Both the sender and reciver share single key.

(2) Two related keys are used (Public or private)

(3) No key is used in Hash function