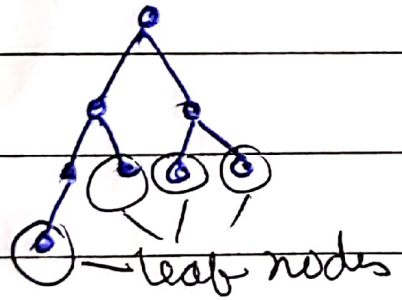
* Binary Tree:-

Imp Properties:-

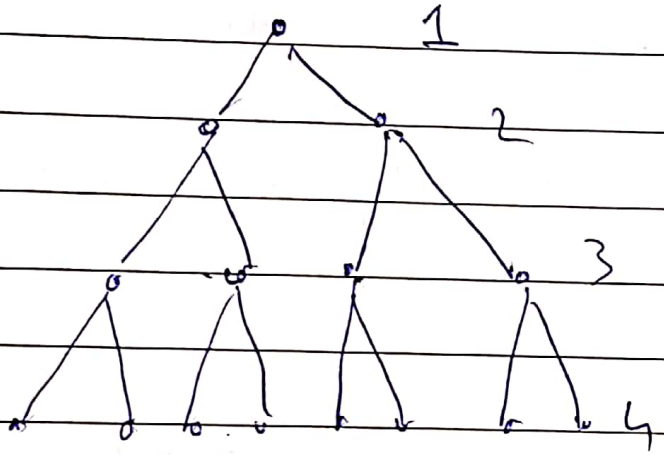
- nos. of leaf nodes = no. of internal nodes + 1



For a given level L :

Total nos. of nodes = $2^L - 1$

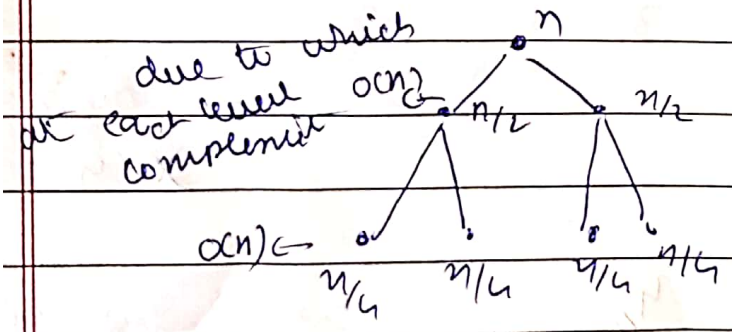
example :



$2^0 + 2^1 + 2^2 + 2^3 = 2^4 - 1$

$= 15$

height of Tree is $(\log_2 n + 1)$:



due to which at each level complexity

so basically at every level is division and multiplication by a factor 2

now this will terminate when $\frac{n}{2^i} = 1$

since we start from 0,

$\Rightarrow i = \log_2 n$

$\Rightarrow$ height = $\log_2 n + 1$

DS

Group Theory :-

(P_1) - Closure Property :-

Set A

$\forall a, b \in A$

$a * b \in A$

(P_5) - Commutative property

$\forall a, b \in A$

$\boxed{a * b = b * a}$

defⁿ of Algebric ~~Struct~~ struct

(P_2) - Associative property :-

Set A

$\forall a, b, c \in A$

$(a * b) * c = a * (b * c)$

if a AS satisfies A, P then it known as semi g.ng

(P_3) - identity Property :-

for Set A

$\forall a \in A$

i.e an ex identity element e,

such that $a * e$

(P_4) - Inverse Property :-

$\forall a \in A$ (Set)

$\exists a^{-1} \in A$

S.T $\boxed{a * a^{-1} = e}$

def ~~of~~ group :-

classmate
Date
Page

set	operation	Arithmetic type group	semi group	Monoid (e, *)
N_1	+	✓	✓	✗
N_1	−	✗	✗	✗
N_1	×	✓	✓	✓
N_1	÷	✗	✗	
$\mathbb{Z}$	+			
$\mathbb{Z}$	−			
R	+			
R	−			
M	+			
M	−			
M	×			
÷				

* Abelian Group :-

$(N, *)$ where

$a * b = a^b$

consider following sets :-

1 → $\{0, \pm 2, \pm 4, \pm 6, \cdots \pm\infty\}$, + ← this is a group

2 → $\{2^n \mid n \text{ is integer}\}$, × ← this is also group

ans 1 → given set of all even nos ;

when we add any 2 even nos we get an even nos

so this is arithmatic group.

always check if there is 0 for +, if it then then →

ans 2 → for × operation always check whether no 0 is present in grp if there is 0 it means -

classmate
Date
Page

Finite Groups

↳ a group finite nos of elements

O(g) (order of g)

↳ will be no. of elements in g

$\{0,1,2,3\}, +$

For it to be A.S, it must satisfy closure property

+	0	1	2	3
0	0	1	2	3
1	1	2	3	4

⇒ For this set since $0+1+3=4 \notin$ set, it is not a A.S

$\{1,-1\}*$

x	1	-1
1	1	-1
-1	-1	1

found

with root of unity $\{1, \omega, \omega^2\}, \times$

x	1	ω	ω^2
1	1	ω	ω^2
ω	ω		
ω^2	ω^2		

with root of unity $\{1,-1,i,-i\}, \times$

x	1	-1	i	-i
1				
-1				
i				
-i				

two operation

Addition modulo in $+_m$ — multiplication modulo in $\times_m$

- $a +_m b = a+b$ if $(a*b) < m$
  $= (a+b) - m$ if $(a*b) \geq m$

- $a \times_m b = \begin{cases} a \times b & \text{if } (a*b) < m \\ (a \times b) \,\%\, m & \text{if } (a*b) \geq m \end{cases}$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

* Order of an element in a group

↳ Given $(G, *)$ order of an element $a \in G$ in n

$O(a) = n$ (least +ve integer $n$ps)

Such that

$a^n = e$

consider $\{0, 1, 2, 3\}, +_4$, ∴ we take modulo 4

$a^2 = a \times a$

$a^2 = a * a$

for any identity element order = 1

order of an element & its inverse order is same

0	1	2	3
$0^1 = 0$	$1^1 = 1$	$2^1 = 2$	$3^1 = 3$
$0^2 = 0$	$1^2 = 2$	$2^2 = 0$	$3^2 = 2$
	$1^3 = 3$	$2^3 = 2$	$3^3 = 1$
$O(0) = 1$	$1^4 = 0$	$O(2) = 2$	$3^4 = 0$
	$O(1) = 4$		$O(3) = 4$

* Generator element:-

Given a group $(G, *)$

if $\exists$ an element $a \in G$, it will be called generator of the group iff $\forall x \in G$ can be represented as $\{a, a^2, a^3, \ldots\}$

Consider the example:

$\{0, 1, 2, 3\}$ $+_4$

now $1^1 = 1 \pmod 4$ $\Rightarrow$ 1 is a generator

$1^2 = 2 \pmod 4$

$1^3 = 3 \pmod 4$

$1^4 = 0 \pmod 4$

however:

$2^1 = 2$ $\Rightarrow$ 2 is not generator

$2^2 = 0$

$2^3 = 2$

$2^4 = 0$

If $\exists$ Atleast 1 generator

$\Rightarrow$ grp is cyclic

Example:

Consider $\{1, 3, 5, 7\}$, $\times_8$

1	3	5	7	9
$1^1 = 1 \pmod 8$	$3^1 = 3 \pmod 8$	$7^1 = 7$	$9^1 = 1$
$1^2 = 1 \pmod 8$	$3^2 = 1$	$7^2 = 1$	$9^2 = 1$
$\vdots$	$3^3 = 3$	$7^3 = 7$	$9^3 = 1$
$1^8 = 1 \pmod 8$	3	$\vdots$	$\vdots$
			$9^8 = 1$

$\phi(1) = 1$

$\Rightarrow$ the given group is cyclic

Homomorphism of Groups

Given $(G,*)$ & $(G',\otimes)$ and there is a f^n mapping

$f: G \to G'$

Homomorphism iff $\boxed{f(a*b) = f(a) \otimes f(b)}$

$a,b \in G \quad f(a), f(b) \in G'$

ex:1 consider

$G \rightarrow$ group of integers with addition operation

$G' \rightarrow$ group of even integers with $+$ operation

$f(x) = 2x \;\forall x \in G$

consider $x_1, x_2 \in G$, Then

For $f(x_1+x_2) = 2(x_1+x_2)$

$= 2x_1 + 2x_2$

$= f(x_1) + f(x_2)$

$= f(x_1) \otimes f(x_2)$

$\Rightarrow$ the given two groups are Homomorphs

Properties

i) $f(e) = e'$ (this is e does not complement, identity doesn't) $\quad e \in G \quad e' \in G'$

ii) $f(a^{-1}) = (f(a))^{-1} \quad a, a^{-1} \in G$

Proof i)

$f(a) \otimes e' = f(a)$

$= f(a*e)$

$= f(a) \otimes f(e)$ by definition

$\Rightarrow f(a) \otimes e' = f(a) \otimes f(e)$

Proof ii)

$f(a) \alpha f(a^{-1}) = f(a * a^{-1})$

$f(a) \alpha f(a^{-1}) = f(e) = e'$ → by definition of homomorphism

$\Rightarrow f(a^{-1}) = (f(a))^{-1}$

Isomorphism of the group:

↳ $(G, *)$ & (G', α)

↳ if $f : G \to G'$ is

i) one to one

ii) onto

iii) hop should be homomorphism

Sub Group:-

Given $(G, *)$

Assume $H \subseteq G$ then H is called sub group with operation $*$ (binary operation) iff it satisfies all 4 properties:

i) identity property

ii) closure "

iii) inverse "

iv) associative "

Sub Group

- Normal subgroup
- Trivial subgroup $(G, *)$
  - i) $(G, *) \leq (G, *)$
  - ii) $\{e\} \leq (G, *)$

Normal Subgroup:

$(G, *)$ and $(H, *)$ where $H \subseteq G$ then H is called normal subgroup if for $a^{-1} \in H$ & $b \in H$

$Z_n \rightarrow$ set of integers modulo n

$\Rightarrow Z_5 (0,1,2,3,4)$ //

$\Rightarrow Z_n^* \rightarrow$ only those integers modulo n which are relatively prime

$\Rightarrow Z_8^* = \{1,3,5,7\}$

* Self Study:-

Group theory:

1. Group Axioms

Consider grp G, ST * is an operation performed on it we write that as:

$(G, *)$

there 3 imp. axioms:-

i) Identity: $\exists$ a unique $id \in G$ such that for some element $x \in G$

(or (e))

$id * x = x * id = x$

ii) inverse: for any element $x \in G$ there exists $x^{-1} \in G$, such that

$x * x^{-1} = x^{-1} * x = id$ (or e)

iii) closure:- Given any two elements x and y. If $x \in G$ and $y \in G$ then,

$x * y \in G$

Abelian Group:-

For any two elements $x, y \in G$, then

$\Rightarrow x * y = y * x$,

$\forall x, y \in G$,

For any two elements $x, y \in G$, then

if $x * y = y * x$ for all $x, y \in G$, then

$G \Rightarrow$ Abelian group

Example:

$(Z, +)$

here for any $a \in G$, $\exists\ a^{-1} \in G$

$a + a^{-1} = a + (-a) = 0$

Here identity here is called additive identity.

$(I + \{1\}, \times)$ set of +ve irrational nos along with 1

To here

identity axiom:

✓ there exist an $id \in G$, s.t $id * x = x * id = x$ for $x \in G$

inverse axiom:

✓ is satisfied

Basically check this first

closure axiom:

we have $\sqrt{2} \times \sqrt{2} = 2 \notin (I + \{1\})$

$\therefore$ the given set is not a group.

To see check dihedral grps

* Orders

The nos of elements of a group is called the orders. For a group, G, we use |G| to denote the order of G.

Consider following examples:

Ex 2.1

consider $Z_5 = \{0,1,2,3,4\}$

$\Rightarrow |Z_5| = 5$ //

EX 2.2

$D_4 = \{ id, r, r^2, r^3, V, H, D, D' \}$ we $|D_4| = 8$ //

for $|D_n| = 2n$

order of an element

order of an element in a group g, in a group G, is the smallest +ve integer n s.t $g^n = id$. If no such int exists we say that g has infinite order. The order of an element g is denoted using |g|.

Example 2.3

$(Z_{10}, +)$

$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$

consider the element 2 $\Rightarrow |2| = 5$

$2^1 = 2$ $2.1 = 2$

$2^2 = 4$ $2.2 = 4$

$2^3 = 6$ $2.3 = 6$

$2.4 = 8$

$2.5 = 10 \pmod{10}$

$= 0$

$0.1 = 1$

$\Rightarrow |0| = 1$

1.

* Subgroup:-

If a subset H of a group G (which we write as $H \subseteq G$) is itself a group under the operation defined in G, we say that H is a subgrp of G

Notation:-

for any element g in a group, we $\langle g \rangle$ denote the set $\{g^n : n \in \mathbb{Z}\}$

this shows the n contains

as found out earlier we know that $|2| = 5$

we found $2 \cdot 1 = 2$ $\quad 2 \cdot 4 = 8$

$2 \cdot 2 = 4$ $\quad 2 \cdot 5 = 10 \pmod{10}$

$2 \cdot 3 = 6$ $\quad = 0$

$\Rightarrow \langle 2 \rangle = \{2, 4, 6, 8, 0\}$

* Cyclic groups:-

if there exists group element $g \in G$, such that $\langle g \rangle = G$, then we call the group G is a cyclic group.

the element that generates the who group is called generator of G.

Ex.4.1

$(\mathbb{Z}_{10}, +)$

$\langle 2 \rangle = \{2, 4, 6, 8, 0\}$

we consider 7:

$\langle 7 \rangle = \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} = \mathbb{Z}_{10}$

so 7 is the generator of the group

$\Rightarrow$ the group is cyclic

$7 \cdot 1 = 7$
$7 \cdot 2 = 4$
$7 \cdot 3 = 1$
$7 \cdot 4 = 8$
$7 \cdot 5 = 5$
$7 \cdot 6 = 2$
$7 \cdot 7 = 9$
$7 \cdot 8 = 6$
$7 \cdot 9 = 3$
$7 \cdot 10 = 0$

Ex 4.2

but $\langle 1 \rangle = \mathbb{Z}$

$a^1 = 1$

classmate
Date
Page

Example 4:)

U-Grp as the grp of units mod some nos. It is written as U(n) and means the five int relatively primes to n, under multiplication modulo n.

U(9) = {1, 2, 4, 5, 7, 8} is a cyclic & a quick computation

* ~~Homomorphism in group~~

* Finite Group :-

A Group with finite nos. of elements is called finite group order of a group.

$O(G)$ = no. of elements in G

consider the following set:

$\{0,1\}, *$ & $\{0,1\}, +$

*	0	1
0	0	0
1	0	1

Associative ✓
Commutative ✓

+	0	1
0	0	1
1	1	(2) ✗

fails closure property

Here identity = 1

now since 0 is present

→ inverse property fails

as $0 \times - \neq 1$

* Homomorphism in Groups :-

Let G and H be two groups, then a homomorphism from G to H is a function

$f: G \to H$ such that

$f(x \cdot y) = f(x) \circ f(y)$ for all $x, y \in G$

Grp homomorphism is basically group maps for short

it can be written as :

$$f(x \underset{\uparrow}{\cdot} y) = f(x) \underset{\uparrow}{\circ} f(y)$$

op of G grp.

op of H grp

Date
Page

Lemma:7

i) the identity map id: $id(x)=x$ is a

as consider $x,y \in G$, then

$$id(x\cdot y) = xy = id(x)\cdot id(y)$$

ii) similarly $f: H \to G$ defined by $f(x)=x$ is also grp with same proof

Rmk → constant map are not usually grp maps,

consider following example

for group $(\mathbb{Z},+)$

$f: \mathbb{Z} \to \mathbb{Z}$

$$f(n)=3 \quad \forall n \in \mathbb{Z}$$

consider $n=1$

$$f(1+1) = f(2) = 3$$

however $f(1)+f(1) = 3+3 = 6$

$\Rightarrow f(1+1) \neq f(1)+f(1)$

$\Rightarrow$ it's not homomorphic

Example (log and exponential):-

a) Prove that exponential func $\exp: (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$ given by $\exp(x) = e^x$ is a group map.

Sol) $f: (\mathbb{R}^+,+) \to (\mathbb{R}^+,\cdot)$

$= e$

for $x,y \in \mathbb{R}$,

$$\exp(x+y) = \exp(x)\cdot\exp(y)$$

$$e^{x+y} = e^x \cdot e^y$$

$\Rightarrow$ given is a group map ✓

Q⇒ Given $f: \mathbb{Z} \to \mathbb{Z}$ by

$f(x) = 5x$

Prove or disprove f is group map.

ans⇒ We $x, y \in \mathbb{Z}$, we

$f(x+y) = 5(x+y)$

$= 5x + 5y$

$= f(x) + f(y)$

$\therefore f$ is a group map

Q⇒ Prove given $g: \mathbb{Z} \to \mathbb{Z}$ by

$g(x) = x^2$

Prove or disprove g is a grp map.

ans⇒ Here consider ~~$x=5$, then~~ $x=2, y=3$ ~~(wrong)~~, it

$g(2+3) = g(5) = 5^2 = 25$

Here

$g(2) + g(3) \neq 25$

$\therefore$ Given is not a homomorphism.

consider a function:

$$tr\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a+d$$

Let for two matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \& \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

$$tr\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = tr\begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix} = a+a'+d+d'$$

$$b(x) \cdot b(x^{-1}) = b(x) \cdot (b(x))^{-1} = e$$

$$b(x \cdot x^{-1}) = b(e) = e$$

classmate

Date

Page

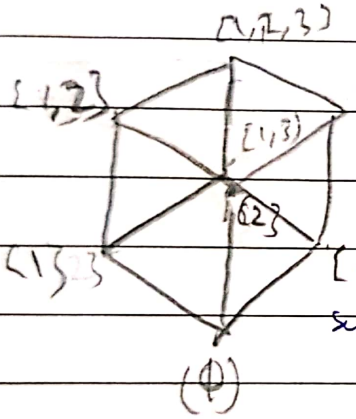
$$tr\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + tr\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = a+d+a'+d' \rightarrow (2)$$

$$(1) = (2)$$

$\therefore$ the given func is ~~for~~ homomorphism.

Ex = example $K_{3,3}$ & C_5.

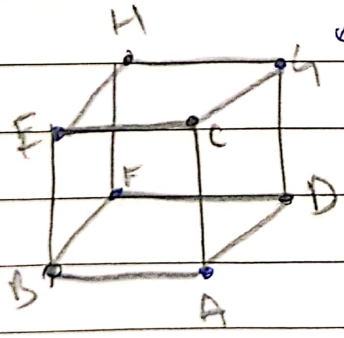
Q. Graph is



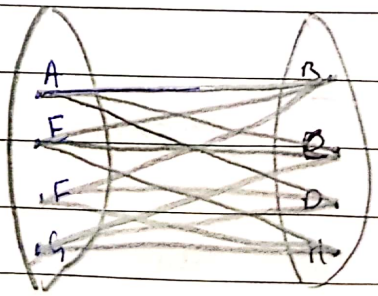
Since 3 is subset of {2,3} & so edge is connected

since ϕ is subset of {3}, {1,3}, {2}, thus all edges connected

similarly these are connected



this can be represented as a bipartite graph as:



$\Rightarrow \chi(G) = 2$,

* Hamilton Graphs

~~It is a graph in which every vertex can be visited~~ once. A graph is said to Hamilton if it has a Hamiltonian path / Hamiltonian cycle.

Hamiltonian Path:
A path that covers all vertices exactly once.

Hamiltonian cycle:
A cycle in which each vertex covered only once and each path is only covered once and all vertex are completed.

For a Hamiltonian graph:
components of $(G-S) \leq |S|$ $\quad S \subseteq V$(vertex)

So if
components of $(G-S) > |S|$ ← G is not Hamiltonian

(A) 

has 2 components

$S = \{$ $\}$

(B) 

has 3 components

$S = \{3,4\}$

So $(G_A - S) = 2 \leq |S|$ ✓

⇒ the given graph is Hamiltonian

So $(G_B - S) = 3 > |S|$ ✓

⇒ the given graph is not Hamiltonian

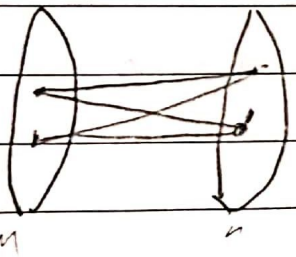
For a bipartite graph:-

$K_{m,n}$ (i.e why we write K for complete) $= K_{m,n}$

provided the given bipartite graph is complete,

if $m = n$

we say that the graph will be Hamiltonian



$d(u) + d(v) \geq n$

$d(v) \geq \frac{n}{2}$, then graph can be said to be Hamiltonian.

for all $n \geq 3$

For any graph G, 4 possibilities:

	EG	HG
G is	✓	✓
G is	✓	✗
G is	✗	✓
G is	✗	✗

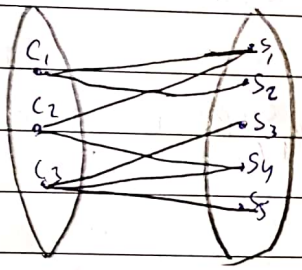
DS

Matching

1. Complete matching of $V_1 m$ to $V_2 m$ in a bipartite graph iff every subset of r vertices in V_1 is collectively adj to r or more V in V_2 for all r values.

2. $C_i M$ exist if (not only if) there is a $m > 0$ for all which degree of every V

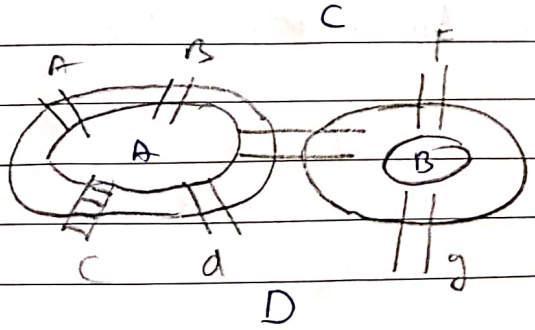
$$V_i m \geq m$$
$$\geq \text{degree of every } V \text{ in } V_2$$



For $r=1$ $\{C_1\} \to \{S_1, S_2\}$
r $\{C_2\} \to \{S_1, S_4\}$
$\{C_3\} \to \{S_3, S_4, S_5\}$

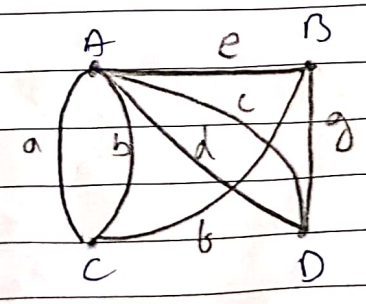
Konesberg 7 bridges Problem :- (Eulerian graph and Eulerian cycle)

Given 7 bridge as shown :-



such that starting from C, we have to cover all bridges and return to C.
all the bridges are to be traveled only once.

So the graph would drawn as follows :-

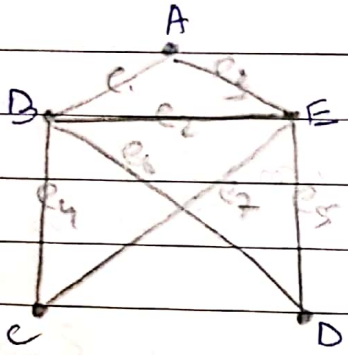


P ⇒ Q Eulerian cycle → degree(v) = 2e
Q ⇒ P

let $m' = m-1$ (we know there are cycles that cover all edges) Eulerian cycles

ignore]

example:- consider the following graph:-



AeiB _____ A

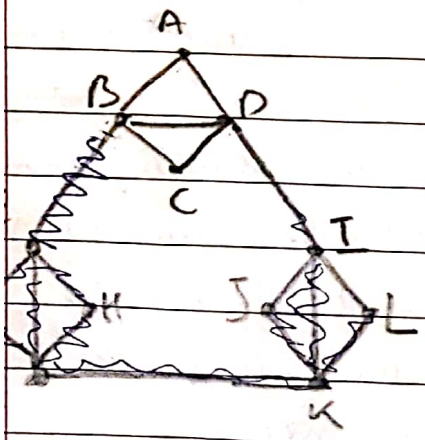
cycles of edges from A, such that all edges are covered.

cycles:- 1. $e_1, e_4, e_7, e_2, e_6, e_5$

2. $e_6, e_6, e_5, e_7, e_4, e_2, e_3$

$A \xrightarrow{e_1} B e_6 D e_5 E e_7 C e_4 B e_2 E e_3 A$

here all edges have even degree, This is possible for only such graphs (when all edges are even, we can get one edge that covers all edges) provided we visit each edge once.



Here A–D is a Bridge as if we consider it before all the other edges

new problem

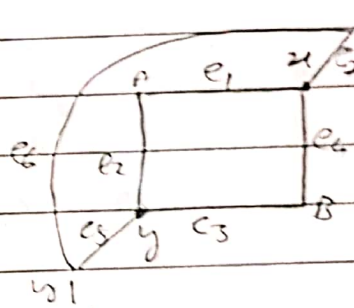
TSP:- Given n cities, distance between any two cities, a TS starts from one of these cities, & visit each city exactly once and comes back to the starting point. Design an algo to find such route?

* G_1 exactly two vertex edges (say x,y) with odd degree and other even degree.

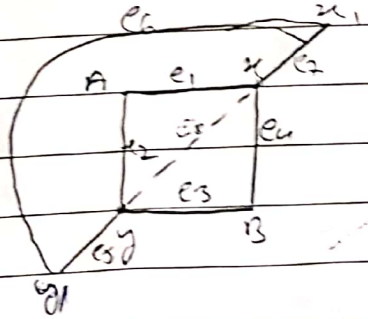
* $G_2 \rightarrow G_1$ + edge (x,y)
* ES list down
* ES remove edge (x,y) → FP for G_1

in order to find Eulerian path

Consider following example:



1st → make the graph such that its Eulerian graph is



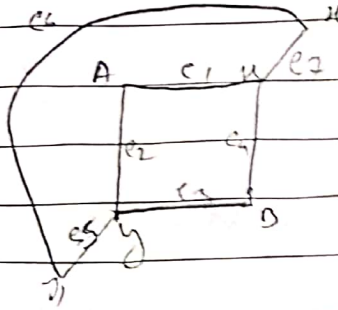
we get Eulerian cycle, as

A e2 y e5 y e6 x1 e7 x e4 B e3 y e5 x e1 A.
1 2 3 4 5 6 7 8

remove this edge

Then

2nd → remove edge and start with node of odd incoming degree



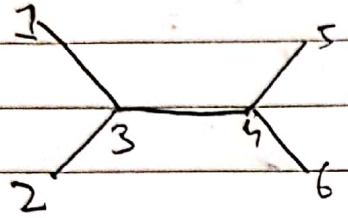
Starting from x1

x e6 A e2 y x e7 x1 e6 y1 e5 y e3 B e4 x e1 A

diff b/w

Path	Trail
can't repeat edges as well as vertices.	can't repeat edges can repeat vertices

consider the following example:



for I =
i) {1, 4, 5, 6}
ii) {3, 5, 6}
iii) {4, 1, 2}
} here all 3 are maximal set

- maximal ∈ can't add any more elements with it, then it's called a maximal set

- Out of the maximal the one with highest cardinality = maximum
  so here
  ⇒ Maximum = {1, 2, 5, 6} = α_0

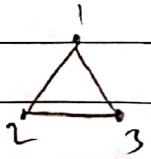
not every maximal is maximum and every maximum is a maximal.

Types of Graphs:-

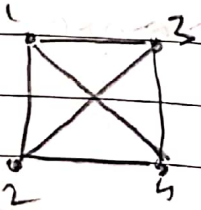
i) K_n ∈ complete graph of n vertices (no self loops allowed).

K_1

K_3



K_4



for K_n

no. of edges can be dealt with say :⇒ i) $^nC_2$ (every edge has 2 node, so no. of ways to select 2 node)

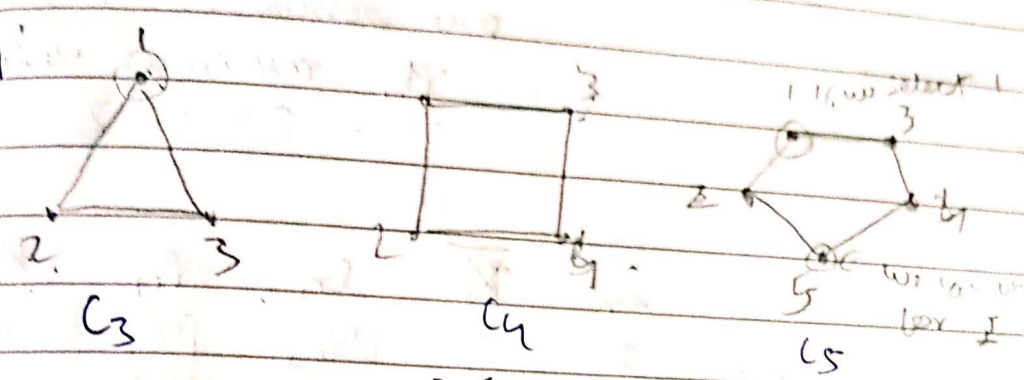
ii) by 1st rule of graph theory:
Total no. of degree of edge for each node = 2 × no. of edges

i.e $n(n-1) = 2 \times |E|$

$\Rightarrow |E| = \frac{n(n-1)}{2}$ //

* Cycle graphs:-

C_n



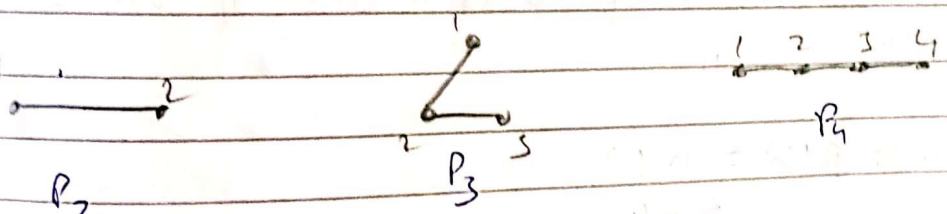
C_3 C_4 C_5

$\Rightarrow \alpha_0 = 1$ $\Rightarrow \alpha_0 = 2$ $\Rightarrow \alpha_0 = ?$

$\Rightarrow \alpha_n = \left[n/2 \right]$

* Path graph:-

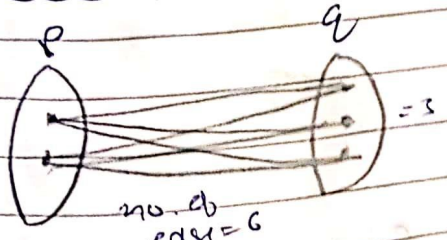
Remove 1 edge from $C_n \Rightarrow$ get P_n unique path blw 2 vertices



P_2 P_3 P_4

hen $\alpha_n = \left[n/2 \right]$

* Dispaatita Graph:-

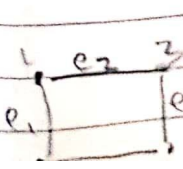


represented as $K_{2,3}$ max Possible no. of edges $= p \cdot q$

$\alpha_0 = \max(p, q)$

Vertex cover:-

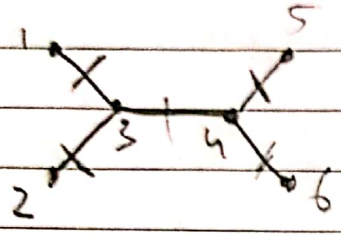
Covering of all the edges of graph using vertices



hen Vertex cover = {1, 2, 4, 3}

minimal = {1, 2, 3}

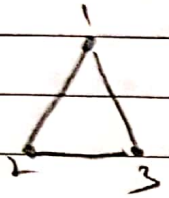
maximal = {1, 2, 3}



Here the vertex cover = {3,4}

Other possibilities → {1,2,4}, {3,5,6}
{1,2,3}, {4,5,6}

$\Rightarrow \beta_0$ = minimum vertex cover
= {3,4} = 2



	K_n	$\overline{K_n}$	C_n	P_n	$K_{p,q}$
α_0	1	n	$\lfloor n/2 \rfloor$	$\lceil n/2 \rceil$	max(p,q)
β_0	n-1	0	$\lceil n/2 \rceil$	$\lfloor n/2 \rfloor$	min(p,q)

$\Rightarrow \boxed{\alpha_0 + \beta_0 = n}$

IMP.

I is independent set of G if & only if $V(G) - I$ is vertex cover of G

$$\alpha_0(G) + \beta_0(G) = n(G)$$
$$\geq n(G)$$
$$\leq n(G)$$

Ques

* 1st Graph Theory :-

Summary of units done so far :-

i) 1st Theory of graph :-

Edge (v) = 2|E|

ii) # of entries being odd ⇒ even

iii) at least 1 degree repeated

iv) $\Delta(G) \leq n-1$

v) $S = (d_1, d_2, d_3, d_4 \ldots d_n)$

iff

$S = (x, d_2 - 1, d_3 - 1, \ldots d_n)$

α_0: maximum size of I

β_0: minimum size of vertex cover

we know that

$\alpha_0(G) + \beta_0(G) = n$

Proof

we know that

$V(G) - I$ is vertex cover $\rightarrow$ (1)

consider I is maximum I.S

$\Rightarrow$ $V(G) - I$ is vertex cover

basically $I = \alpha_0$

now let

K be minimum V.C. $\rightarrow$ (2)

$\therefore$ from (1)

β_0 (minimum size of vertex cover) $\leq |V(G) - \alpha_0|$ $\rightarrow$ (2)

$\Rightarrow$ $\beta_0(G) + \alpha_0(G) \leq V(G) = n$ $\rightarrow$ (3)

from (2), we can say that

$K = \beta_0(G)$

from 2, we can also say that

$\alpha_0(G) \geq |V(G) - K|$

$\alpha_0(G) \geq |V(G) - \beta_0(G)|$

$\alpha_0(G) + \beta(G) \geq V(G) = n$ $\rightarrow$ (4)

So from (3) & (4)

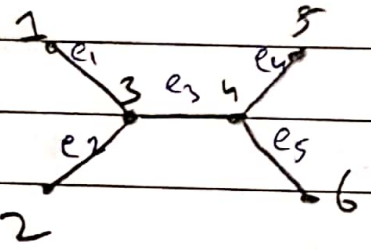
$\alpha_0(G) + \beta_0(G) = V(G) = n$ //

Hence the proof

M (Matching)

$M \subseteq E$

m ⊂ m — Parallel edges
— Independent edges
— non-adjacent

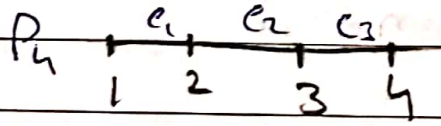


all matchings:

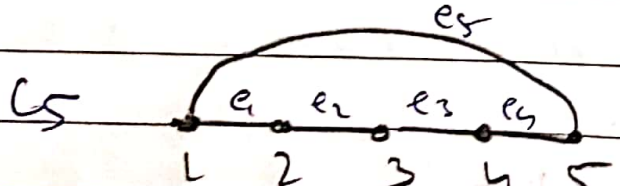
1 $\{e_1, e_4\}$
2 $\{e_2, e_5\}$
3 $\{e_3\}$

$\alpha_1(G) = 2$

consider Path graph of 4 vertices:

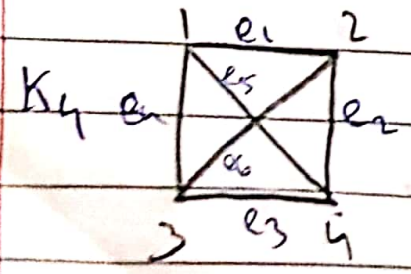


here all possible matchings
$\{e_1, e_3\}$
$\{e_2\}$



here, we have
$\{e_2, e_4\} = 2$
$\{e_1, e_3\} = 2$
$\{e_5, e_2\} = 2$
$\{e_5, e_3\} = 2$

max is is still 2

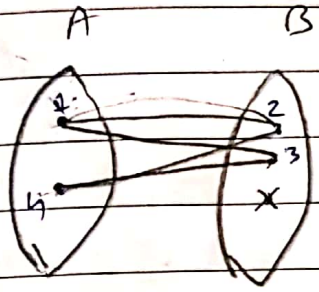


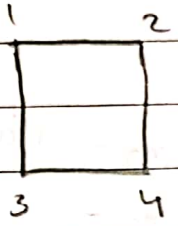
here
$\{e_1, e_3\}$
$\{e_4, e_2\}$

consider K_5

Sol:-

How to identify whether a graph is Bipaatite?

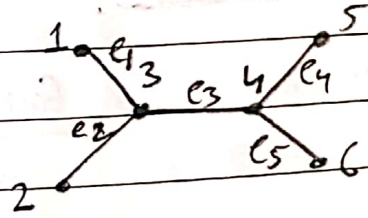




Tree is also bipaatite

β_1: minimum size of edge cover

↳ connected collection of edges covering all vertices.

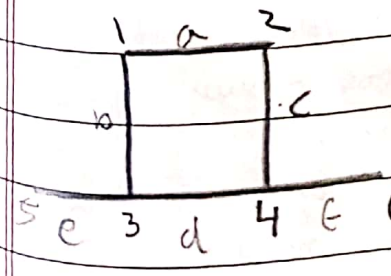


hw minimal an possible is?

$\{e_1, e_2, e_4, e_5\}$

$\Rightarrow \beta_1(G) = 4$

$\Rightarrow \boxed{\alpha_1(G) + \beta_1(G) = n}$



remember

maximal :- can't add any more

minimal :- can't remove any more

$\alpha_1 = \{c, a, f\} = 3$

$\beta_1 = \{c, a, f\} = 3$

$= \alpha_1 + \beta_1 = 6$ ✓ $= n$

User RSA and SHA256 (same as hashing algo)

15/03/18

DS

$a \equiv b \pmod m$

$\Rightarrow a \bmod m = b$

Facts:-

- $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $(a \cdot b) \bmod m =$

Co Prime

How many relatively prime no on the range 1–20

gcd(a, 20) = 1, 3, 7, 9, 11, 13, 17, 19

$\phi(n)$: (Euler totient function)

Fact 1:- If n is prime, then $\phi(n) = n-1$

Fact 2:- if c is composite & $c = n^k p^k$

Then, $\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \ldots$

n →	1	2	3	4	5	6	7	8	9	10
$\phi(n)$ →	1	1	2	2	4	2	6	4	6	4

→ the no. of numbers that are relatively prime to n.

Some example $\phi(20) = 8$

$\phi(19) = 18$

it is no. relative prime nos for a given nos, i.e. $\phi(n)$ = ans (nos of relative prime nos.) ↓ given nos

This is basically saying that, consider 4, the $4 = 2^2$ then we do $2^2 - 2^{2-1} = 4 - 2 \Rightarrow \phi(n)$

Linear congruence:-

$ax \equiv (b \bmod m)$ (division on mod m remains)

Soln = any value of x that satisfy this relation

multiplicative Inverse modulo m

↳ MI of a modulo m is any integer, $\bar{a}^1$ or $\bar{a}$, then

$$a\bar{a}^1 \equiv 1 \pmod m$$

3^{10} divides 11

$a = 3 \quad p = 11$

Little fermat theorem:-

↳ if m is Prime

$a^{-1} = a^{m-2} \bmod m$

$3 \to a^{20}$ divides 11

$11-1$

$a \equiv 1 \pmod p$

$3^{10} \equiv 1 \pmod{11}$

$= 1$

$3^{10 \times 2 + 1}$

$(3^{10})^2 \cdot 3^1$

* Application of Number Theory:-

- RSA algorithm

i) choose two distinct prime nos. (relatively large)

p, q

ii) $n = p \cdot q, \quad k = (p-1)(q-1)$

choose an integer e, such that

$1 < e < k$ and $\gcd(e, k) = 1$ [e must not be small]

↳ encryption

iii) let d be some multiplicative inverse of e mod k

i.e. $d \cdot e \equiv 1 \pmod k$

eg: MI of 8 modulo 15

sender side:

$c = m^e \bmod n$

(cipher text for encrypted message)

decrypting at receiver side:

$m = c^d \bmod n$

* order of an element:-

Let n be a +ve integer for an integer a:

Then the order of a modulo n is denoted by $\text{ord}_n(a)$: is a smallest +ve integers m such that $a^m \equiv 1 \pmod n$

$\gcd(a, n) = 1$

generator

If a $1 \le p \le m-1$, then

$a^p \equiv 1 \pmod m$

Ex:- calculating order of 7 say $\text{order}_7(2)$, then

Scanned by CamScanner

$\text{ord}_7(2) = ?$

$2^1 \equiv 2 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$\boxed{2^3 \equiv 8 \equiv 1 \pmod 7}$

$\text{ord}_7(2) = 3 \quad$ so $\rightarrow \{1, 2, 3\}$

$\text{ord}_7(3) = ?$

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 9 \pmod 7 \equiv 2 \pmod 7$

$3^3 \equiv 27 \pmod 7 \equiv 6 \pmod 7$

$3^4 \equiv 81 \pmod 7 \equiv 4 \pmod 7$

$3^5 \equiv 243 \pmod 7 \equiv 5 \pmod 7$

$3^6 \equiv 729 \pmod 7 \equiv 1 \pmod 7$

so it

$\text{ord}_7(3) = 6$

$\text{ord}_{13}(12) = 2$

because

$12^1 = 12 \pmod{13}$

$12^2 \equiv 144 \pmod{13} \equiv 1 \pmod{13}$

$12^3 \equiv 12 \pmod{13}$ repeatation

* Primitive root modulo n (PR)

n is a +ve integer (Prime), and a is any integer, such that

$\gcd(n, a) = 1$,

then a will be a P.R modulo n, IF and only if, (IFF)

$\text{ord}_n(a) = \phi(n)$

some imp symbols:

$\mathbb{Z} \in$ set of integers

$\forall \leftarrow$ for all

$\exists \leftarrow$ there exist/for some

$\forall a, b \in \mathbb{Z}$

means $\mathbb{Z}_n = \{1, 2, 3, \ldots, n-1\}$

$\exists$ unique $x, y \in \mathbb{Z}$, such that

$ax + by = \gcd(a, b)$

↳ called Bezout's identity.

eqns of form ax+by

$432 = 126 \times 3 + 54$

$126 = 2 \times 54 + 18$

18 as

$18 = 126 - 2 \times 54$

$= 126 - 2 \times [432 - 126 \times 3]$

$= 126 - 2 \times 432 + 6 \times 126$

$\boxed{18 = 7 \times 126 - 2 \times 432}$

you calculate the value x and y in this way

chinese remainder algorithm:-

- used for crypto analysis

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

there exist an unique soln such that

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$2 = a_1$

$3 \rightarrow a_2$

$2 \rightarrow a_3$

$3 \rightarrow m_1$

$5 \rightarrow m_2$

$2 \rightarrow m_3$

$M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 2 = 105$

$\Rightarrow M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$\Rightarrow M_1^{-1} = 35^{-1} \bmod 3$

$= 35^{3-2} \bmod 3$

$= 35 \bmod 3$

$= 2$

* Hand shaking theorem :-

it basically states that, for some v_i belonging to a graph G, then $d(v_i)$ = degree of vertex (in case of degree), then

$$\sum_{i=1}^{n} d(v_i) = 2|E|$$

and also

$$\sum_{i=1}^{n} d(v_i) = \underset{\text{(even)}}{\Sigma d(v_i)} + \underset{\text{(odd)}}{\Sigma d(v_i)}$$

* Min and max degree and degree sequence :-

Min degree
↳ represented by $\delta(G)$
↳ it is the min degree from the n vertices

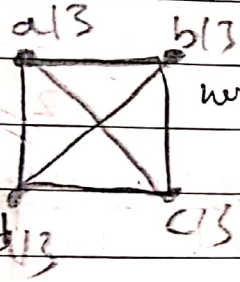
Max degree
↳ represented by $\Delta(G)$
↳ it the max degree from the n vertices of the graph

Imp inequalities
$\delta(G) \cdot |V| \leq 2|E|$

Imp inequalities
$\Delta(G) \cdot |V| \geq 2|E|$

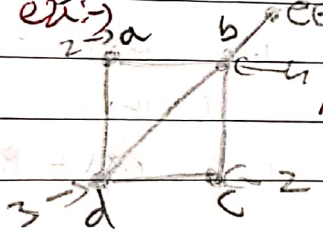
$\Delta(G) \cdot |V| \geq 2|E| \geq \delta(G) \cdot |V|$

ex:-



$\delta(G) = 3$

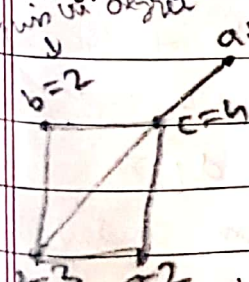
ex:-



here $\Delta(G) = 4$

Degree Sequence :- the arrangement of degree of all vertices of a graph in either in non-increasing or non decreasing order.

ex:- Consider the following the graph :-



its degree sequence → {4, 3, 2, 2, 1}

or degree we see → 1, 2, 4, 3, 2

say if we are given a degree sequence then can a simple graph be created, say :-

i) {2, 3, 3, 5, 4, 4}

we can use havel hakimi method,

here if we logically check, then on 3 oddnos → 3, 3, 5, so the sum of all degrees = 2 + 11 + 8 = 10 + 11 = odd ∴ not possible as $\Sigma d(v_i) = 2|E|$ even.

ii) {2, 5, 4, 3, 4} :- here we have 5 degree edge, which signifies 5 vertices, however one of the degree = 5, which is not possible, as in simple graph, no self loop or parallel edges allowed, i.e max degree can almost be n-1 = 4/1, hence no simple graph possible.

* Graph Theory :-

In started with Directed and undirected graphs

undirected graphs :-
unordered pair of vertices

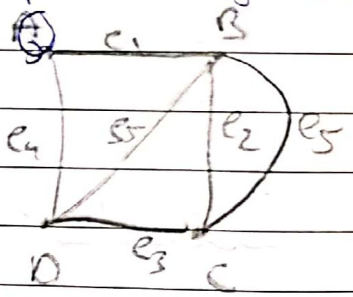
directed graphs :-
ordered pair of vertices

some imp terminology :-

* Self loop :- when starting and ending vertex of an edge is same (v_i, v_i) then it called self loop

* Parallel loop :- when more than one edge associated with a given pair of vertices, then such edges are called parallel edges.

	Self loop	Parallel loop
Graph	✓	✓
Multi-Graph	×	✓
Pseudo-Graph	✓	×
Simple Graph	×	×



here A-B ⟵ adj vertex
e_1-e_2 ⟵ adj edge
e_5 ⟵ Parallel loop

finite, Null, trivial and complete graph :-

Finite graph :- A graph with finite no. of vertices as well as finite nos. of edge. is called finite graph

NULL graph :- A graph where vertex set is non empty but edge set is empty.

Trivial graph :- A graph where vertex set contains only one vertex and edge set is empty is called Trivial graph.

complete graph :- a graph is said to complete if all vertex are connected with all possible edges.

* Division algorithm:

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then, there are unique integers q and r such that

$$a = dq + r$$

* Euclidean algorithm:

It states that

if $a = bq + r$, then

$$\gcd(a,b) = \gcd(b,r)$$

For example:

Consider gcd (2322, 634), using

$2322 = 634 \times 3 + 420$

gcd (634, 420)

$634 = 420 \times 1 + 214$

gcd (420, 214)

$420 = 214 \times 1 + 206$

gcd (214, 206)

$214 = 206 \times 1 + 8$

gcd (206, 8)

$206 = 8 \times 25 + 6$

gcd (8, 6)

$8 = 6 \times 1 + 2$

gcd (6, 2)

$= 2$

$\Rightarrow$ greatest common divisor of 2322 & 634 is 2 //

Proof of the algorithm:

The proof states that for any nos a and b, such that $a = bq + r$, the $\gcd(a,b) = \gcd(b,r)$, assuming it to be true, then,

d be nos such that,

$\gcd(a,b) = d$ iff $\gcd(b,r) = d$,

assuming, $\gcd(a,b) = d$, then

$\Rightarrow d|a$ and $d|b$, i.e. $a = dq_1$, $b = dq_2 + r$

for some constant Q,

$Qb = dq_2 Q$, then

consider,

$$a - Qb = dq_1 - dq_2 Q$$
$$= d(q_1 - q_2 Q)$$

so for $\frac{a - Qb}{d} = \frac{d(q_1 - q_2 Q)}{d} = (q_1 - q_2 Q)$

$\Rightarrow$ d divides a-Qb

d is common divisor

$\therefore$ the given assumption is true for b and r

So basically we can say that

since $d|a$ & $d|b \rightarrow (1)$

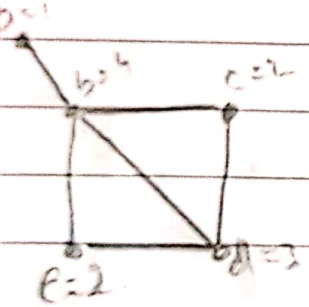
$\Rightarrow d|(a - bq)$

$\Rightarrow d|r \rightarrow (2)$

Hence the proof //

→ Havel Hakimi Theorem:-

consider the following graph:



its degree sequence is

4, 3, 2, 2, 1, so if I remove 4, the even vertex

X, 2, 1, 1, 0 will have one less edge, so 2

similarly if I remove 2, then

X, X, 0, 0, 0 ← this basically gives us a graph of 3 vertices with no edge, which is a null graph

Consider some more examples:

i) 7, 6, 5, 4, 4, 3, 2, 1,

X, 5, 4, 3, 3, 2, 1, 0

→ X, X, 3, 2, 2, 1, 0, 0

→ X, X, X, 1, 1, 0, 0, 0

→ X, X, X, 0, 0, 0, 0, 0

→ the given graph is valid

ii) 6, 6, 6, 6, 3, 3, 2, 2

X, 5, 5, 5, 2, 2, 1, 1 ← this won't be affected as it contains element and 0 value, so it will adjo 6 vertic

X, 5, 5, 5, 2, 2, 2, 1

X, X, 4, 4, 1, 1, 1, 1

X, X, X, 3, 0, 0, 0, 1

X, X, X, 3, 1, 0, 0, 0

X, X, X, X, 0, -1, -1, 0

→ the given graph is not valid

Divisibility :-

Q- Prove: if (a divides b) and (a divides c) then [a divides (b+c)] :

assume a|b and a|c

$\Rightarrow b = aq_1 \quad c = aq_2$

$\Rightarrow b+c = a(q_1+q_2)$

let $q_1+q_2 = M$, then

$\Rightarrow b+c = aM$

this of the form that shows if $\frac{b+c}{a}$ then $\frac{aM}{a}$ = some integer (true)

$\Rightarrow$ our assumption is True,

Hence. the proof.