CSE-1203 Date: 01.01.24

Chapter-4

Number theory and cryptography

Defn: If $a, b \in z$, $a \neq 0$ and there is an integer c, such that $b = ac$. then, "a divides b".

divisor (a) | dividend (b) | quotient (c)

remainder (r)

$b = ac + r$
$c = b/a$
$r = b \bmod a$

Defn: if $a, b \in Z$ and $m \in z^+$ then, $a \equiv b \pmod m$ iff $m | (a-b)$

$11 | (101 - 2) \Rightarrow 101 \equiv 2 \pmod{11}$
$11 \nmid 99$

#3

Theorem: If $a, b \in z$ and $m \in z^+$ then, $a \equiv b \pmod m$
iff $a \bmod m = b \bmod m$ → congruent modulo

Theorem: Let $m \in z^+$, then a, b, are congruent modulo of m if there exists an integer k such that $a = b + km$.

$a \equiv b \pmod m$
↳ $m | (a-b)$
$(a-b) = km$
$\Rightarrow a = b + km$

if $m \in z^+$, $a \equiv b \pmod m$ & $c \equiv d \pmod m$
$(a+c) = (b+d) \pmod m$
↳ $ac = bd \pmod m$

$a = b + km$
$c = d + k'm$

$(a+c) = b+km+d+k'm$

$\Rightarrow (a+c) = b+d+m(k+k')$

$(a+c) = (b+d) + mN$

$(a+c) = (b+d) \pmod m$

$ac = (b+km)(d+k'm)$

$= bd + bk'm + dkm + kk'm^2$

$= bd + m(bk' + dk + kk'm)$

$ac = bd + mN$

$ac = bd \pmod m$

Arithmatic modulo m:

$z_m \in$ set of non-negative integers less than m.

$z_m = \{0, 1, 2, \ldots, m-1\}$

Addition: $a +_m b = (a+b) \pmod m$

Multiplication: $a *_m b = ab \pmod m$

$7 +_{11} 9 = (7+9) \pmod{11} = 16 \pmod{11} = 5$

$7 *_{11} 9 = 63 \mod 11 = 8$

Self study:

- Binary expansion
- Octal expansion
- Hexadecimal expansion
- Base conversion.

Algorithm for Binary Addition:

$a = (1110)_2$
$b = (1011)_2$
$3 \leftarrow 0$

$a_n + b_n + c_{n-1} = c_n \cdot 2 + s_n$

$\rightarrow a_0 + b_0 = c_0 \cdot 2 + s_0$
$0 + 1 = 0 \cdot 2 + (1)$

$\rightarrow a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$
$1 \quad 1 \quad 0 = 1 \cdot 2 + (0)$

$\rightarrow a_2 + b_2 + c_1 = c_2 \cdot 2 + s_2$
$1 + 0 + 1 = 1 \cdot 2 + (0)$

$\rightarrow a_3 + b_3 + c_2 = c_3 \cdot 2 + s_3$
$1 + 1 + 1 = (1 \cdot 2) + (1)$

$(11001)_2$

Algorithm for Binary Multiplication:

$$ab = a(b_0 \cdot 2^0 + b_1 2^1 + b_2 2^2 + \cdots b_{n-1} \cdot 2^{n-1})$$
$$= ab_0 2^0 + ab_1 2^1 + ab_2 2^2 + \cdots ab_{n-1} 2^{n-1}$$

$a = (110)_2 \quad b = (101)_2$

$ab = (110)_2 \cdot 1 \cdot 2^0 + (110)_2 \cdot 0 \cdot 2^1 + (110)_2 \cdot 1 \cdot 2^2$

$= (110)_2 + (0000)_2 + (11000)_2$

$$\begin{array}{r} 110 \\ 0000 \\ 11000 \\ \hline (11110)_2 \end{array}$$

Algorithm for division and modulus.

$4 \mid 19 \mid 4$ (16, 3)

$3 \mid -16 \mid 6$ (-18, 2)

let, $a, d \in z$, $d > 0$

$q = a \text{ div } d$

$r = a \bmod d$.

$q = 0$

$r = |a|$

while $r \geq d$

$r := r - d$

$q = q + 1$

if $a < 0$, $r > 0$ then.

$r = d - r$

$q = -(q+1)$

example:

$a = -16$; $d = 3$

$q = 0$, $r = |-16| = 16$

$16 > 3$, $r = 16 - 3 = 13$, $q = 1$

$13 > 3$, $r = 13 - 3 = 10$, $q = 2$

$10 > 3$, $r = 7$, $q = 3$

$7 > 3$, $r = 4$, $q = 4$

$4 > 3$, $r = 1$, $q = 5$

$r \not> 3 \rightarrow$ break.

Section - 4.6 - Cryptography

1) Classical cryptography:

Ceaser's cipher.

A ..... Z

1 26

$E \rightarrow f(p) = (p+3) \bmod (26)$

$f(8) = f(8+3) \bmod (26) = 11$

Hello world.

↓

8

↓

11

↓

K ⟶ encrypted.

$D = f^{-1}(p) = (p-3) \bmod (26)$

$f(11) = (11-3) \bmod (26) = 8$

$x = a$

$y = b$

while $(y \neq 0)$

$r = x \bmod y$

$x = y$

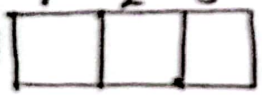
$y = r$

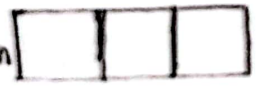
return x ;

(2) Block cipher:

Hello_World

1 2 3

Original 

Encryption 

transposition functions:

$\sigma(1) = 3$
$\sigma(2) = 1$
$\sigma(3) = 2$

Original: Hel lo_ Wor ldx # decryption:

Encryption: elH o-L orW dxL

$\sigma^{-1}(3) = 1$
$\sigma^{-1}(1) = 2$
$\sigma^{-1}(2) = 3$

(3) Public key Cryptography:

Discrete Math (CSE-4203)

Date: Online.

Sequence:

$a_n = \frac{1}{n}$

$n = z^{-1}$

But an can be fractional.

Recurrence relations

finding closed formula

type-1

example-6:

$2a_{n-1} - a_{n-2}$

$= 2[3(n-1)] - 3(n-2)$

$= 2[3n-3] - 3n+6$

$= 6n-6-3n+6$

$= 3n$

$= a_n$

example-7:

Recursive definitions:

Procedure fib(n: non-negative int)
if n==0, then return 0
else if n==1, then return 1
else return fib(n-1) + fib(n-2)

fib(5) → fib(4) + fib(3)

fib(3) + fib(2) fib(2) + fib(1)

3! ⇔ (1.2).3 → 3.2!
2! → 1.2 → n.fact(n-1)

procedure fact (n: non negative int)
if n==0, then return 1
else return n.fact(n-1)

(1) Your thoughts on problem
(2) Defn of procedure.
(3) Verification and validation

Discrete (CSE-4203) Date: April 22, 2024

Section 5.3
Mathematical Induction

$P(n) = 1+2+\cdots+n = \frac{n(n+1)}{2}$ Type-1

Step-1 : $P(1)$; $L \to 1$ $R \to 1$ ——(i)

$L = R$ ——(I)

Step-2: Let, $P(K)$ is true where $K \in Z^+$ such that,

$P(K) = 1+2+3+\cdots+K = \frac{K(K+1)}{2}$ ——(II)

Step-3: $P(K+1)$ will be true iff

$P(K+1) = 1+2+3+\cdots+K+(K+1) = \frac{(K+1)(K+2)}{2}$ ——(III)

Adding $(K+1)$ on both sides of (II)

$1+2+\cdots+(K+1)+K = \frac{K(K+1)}{2} + (K+1)$

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

$n < 2^n$; $n \in Z^+$

Type-2

S_1 : $1 < 1^1$

S_2 : $n = k \in Z^+$ $k < 2^k$ ⟶ assume true

S_3 : $n = (K+1) \in Z^+$ $(K+1) < 2^{k+1}$

Adding 1 on both sides of S_2.

$(K+1) < \underbrace{2^k+1 < 2^k+2^k}_{1 < 2^k}$

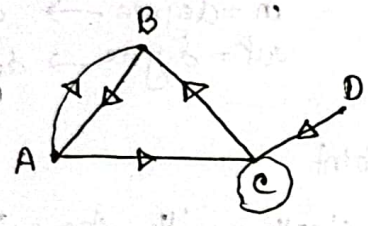
$(K+1) < 2.2^k$

$(K+1) < 2^{K+1}$

Graphs:

 # Defn: 1

G(V, E)



two types
- ↳ directed
- ↳ undirected

- finite → contains finite no. of vertices.
- infinte

- multi graphs and/or (self loops + multipledges)
- simple graph

Adjacency:

↳ direction doesn't matter

A → B, C
B → A, C
C → A, B, C, D
D → C

C ↺ back वालिएज

Degree: of Vertex

↳ represents no. of edges connected

deg(A) = 3
deg(B) = 3
deg(C) = 5
deg(D) = 1

6 edges

self loop - 2

Theorem (I) – hand-shaking theorem

G(V, E)

|E| = m

$2m = \sum_{v \in V} deg(v)$

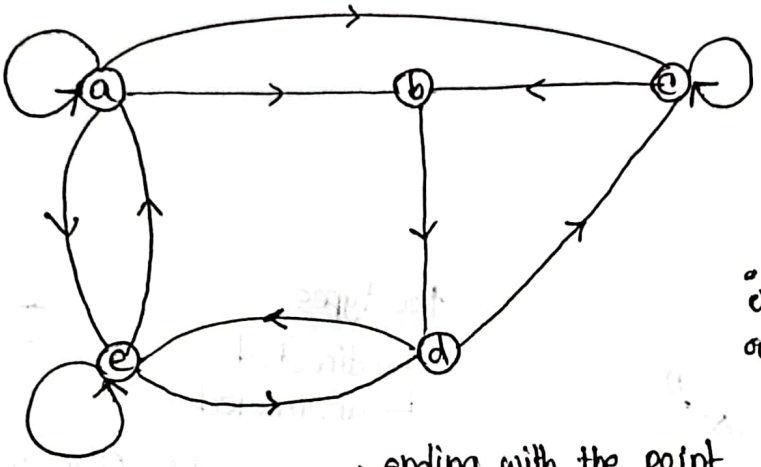
6 edges → 12 = 12

Theorem (II) – Any undirected graph has even number of odd-degree vertices.

$2m = \sum_{v \in V} deg(v)$

$= \sum deg(V_o) + \sum deg(V_e)$

V_o → odd
V_e → even



in = degree → $\deg^-(v)$
out = degree → $\deg^+(v)$

ending with the point ↗

v	$\deg^-(v)$	$\deg^+(v)$ → starting with the point
a	2	4
b	2	1
c	3	2
d	2	2
e	3	3
Σ	12	12

for any directed graph, $\Sigma \deg^-(v) = \Sigma \deg^+(v)$

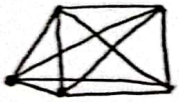
CSE-4203 - Discrete Mathematics Date: 25.01.2021

Types of graphs:

(1) complete graphs (K_n) (n) → no. of vertices of graph

$K_1 \rightarrow$ · $K_2 \rightarrow$ —

$K_5 \rightarrow$



complete graph: there is an edge between every possible combinations of vertices.

$2m = \sum deg(v)$ (m: no. of edges)

$2.10 = 5.4$ (degree of each vertices ⇒ 4)

$\Rightarrow 20 = 20$ (1st theorem)

$\sum deg(v) = \sum deg(v_o) + \sum deg(v_e)$ (2nd theorem)

$\downarrow$ ⓪ $\downarrow$ ⑤

② cycles (C_n) $\underbrace{n \geq 3}$ (only these graphs will have cycles)

$C_3 =$  $C_5 =$

③ Wheels (W_n)

condition: $W_n = C_n + 1$

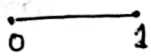
$W_3 = C_3 + 1$

④ n-cubes (Q_n) → n dimensional cube

$Q_1 \rightarrow 2^1 \rightarrow$ vertices — 0, 1

$Q_2 \rightarrow 2^2 \rightarrow$ vertices — 00, 01, 11, 10 (gray code)

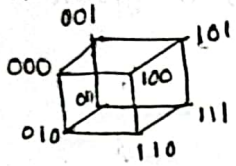
$Q_3 \rightarrow 2^3 \rightarrow$ " — 000, ..., 111 (adjacent vertices should have bit difference of 1)

Q_1 

($Q_1 \rightarrow$ 1D fig)

Q_2 

($Q_2 \rightarrow$ 2D fig)

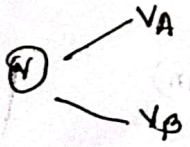
Q_3 

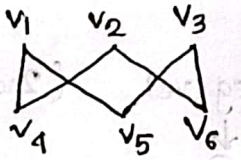
($Q_3 \rightarrow$ 3D fig)

(Q_4 is not possible to represent on paper)

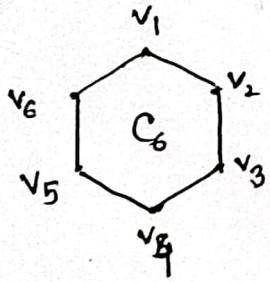
⑤ Bipartite graphs

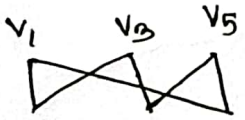
We can divide the set of vertices into two groups such that no edges between vertices of same group and





(non-adjacent vertices in same group)





→ blue

→ green

* graph coloring: minimum no. of colors required so that no two adjacent vertices have same color (known as chromatic number of a graph)

For any bipartite graph,

chromatic number is 2

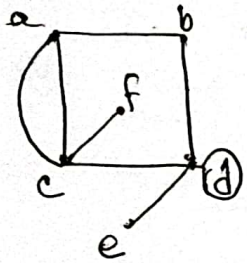
x_2

converting a bipartite graph into a complete bipartite graph:
each vertices of a group must have connection with all vertices of the other group.

$K_{3,3}$

3 ways to represent graphs in code:

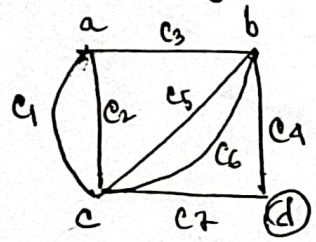
Adjacency list



V	N(V)
a	b, e
b	a, d
c	a, d, f, a
d	b, d, e, c
e	d
f	e

{ If there are more than one edges beth two vertices, address that}

Adjacency Matrix: Square matrix $|V| \times |V|$



(undirected graph)

	a	b	c	d
a	0	1	2	0
b	1	0	2	1
c	2	2	0	1
d	0	1	1	1

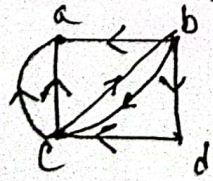
no. of edges between vertices of row and col^n

Incidency Matrix: vertices $|V| \times$ edge $|E|$

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
a	1	1	1	0	0	0	0	0
b	0	0	1	1	1	1	0	0
c	1	1	0	0	1	1	1	0
d	0	0	0	1	0	0	1	1

{ which vertices connected in that edge}

Efficient way sequence: Adjacency list > Adjacency Matrix > Incidence Ma
directed graph:



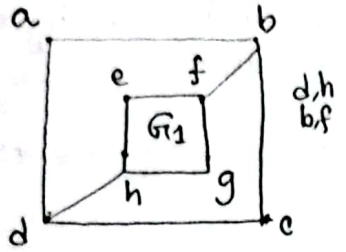
no sense of direction in adjacency list or incidence Matrix

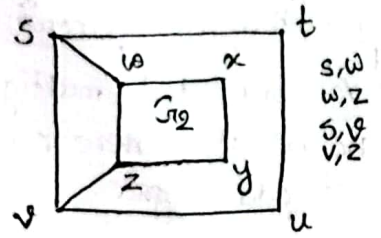
Adjacency Matrix:

	a	b	c	d
a	0	0	1	0
b	1	0	1	1
c	1	1	0	0
d	0	0	1	1

row to coloumn

Graph Isomorphism :





	G_1	G_2
(I) same # of vertices	8	8
(II) same # of edges	10	10
(III) same # of vertices of equal degrees	deg(2) → [4,4]	deg(3) → [4,4]

(IV) Find an isomorphism function

$f(x_1) = x_2$; where $x_1 \in G_1$, $x_2 \in G_2$

	a	b	c	d	e	f	g	h
a	0	1	0	1	0	0	0	0
b	1	0	1	0	0	1	0	0
c	0	1	0	1	0	0	0	0
d	1	0	1	0	0	0	0	1
e	0	0	0	0	0	1	0	1
f	0	1	0	0	1	0	1	0
g	0	0	0	0	0	1	0	1
h	0	0	0	1	1	0	1	0

= Adj (G_1)

consider vertices of same degrees:

G_1 → d, h ; b, f } only 2 pair

G_2 → s, w ; w, z ; s, v ; v, z } four pairs

	s	t	u	v	w	x	y	z
s	0	1	0	1	1	0	0	0
t	1	0	1	0	0	0	0	0
u	0	1	0	1	0	0	0	0
v	1	0	1	0	0	0	0	1
w	1	0	0	0	0	1	0	1
x	0	0	0	0	1	0	1	0
y	0	0	0	0	0	1	0	1
z	0	0	0	1	1	0	1	0

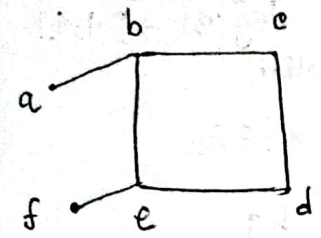
	u	v	s	t	w	x	y	z
u	0	1	0	1	0	0	0	0
v	1	0	1	0	0	~~0~~ 1	0	~~1~~ 0
s								
t								
w								
x								
y								
z								

f(a) = u
f(b) = v
f(c) ≠

↳ we can not map it, as we change, other two changes harper

Connectivity:

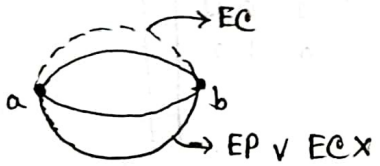
- path ⟶ abcbe
- simple path → abe
- circuits ⟶ bcde



including 5 vertices

abe

path length = n-1 (for n vertices)



(i) Euler and Hamilton paths

↳ visits every vertex exactly one.

(abcdef) ⟶ Hamilton

Euler path: visit every edge exactly once.

(ii) Euler and Hamilton circuit

Theorem-1: A connected multigraph ↳ EP and no EC. iff there one exactly two vertices of odd degree.

Theorem-2: A connected multigraph with at least 2 vertices has EC iff each vertex has even degree.

Diracs theorem

(G ⟶ simple graph)

n vertices, $n \geq 3$

$\deg(\forall v \in V) \geq \frac{n}{2}$

✗ has HC (then, a graph) might have.

$n = 5 > 3$

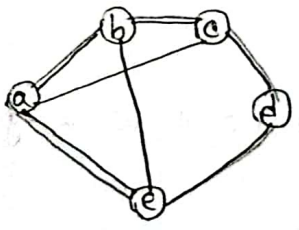
$d(a) = 3 > 2.5$

$d(b) \rightarrow 3$

$d(c) \rightarrow 3$

$d(d) \rightarrow 2$

$d(e) \rightarrow 3$



Ores theorem

(G ⟶ simple graph)

n vertices, $n \geq 3$

$\deg(u) + \deg(v) \geq n$ for every pair of vertices.

has HC.

$n = 5$

✓ b, d = 5, = 5

✓ c, e = 6 > 5

✓ a, d = 5 = 5