Sarita Sangvez
23i - 2088
CY - A

Discrete structures

Assignment 03

Q 9. $p = 919$

$g = 327$

Alice	Bob
$a = 400$	$b = 729$
Public key $A = g^a \bmod p$	$B = g^b \bmod p$.
$327^{400} \bmod 919$	$= 327^{729} \bmod 919$
$A = 128$	$B = 189$
$\xrightarrow{B}$	
$\xleftarrow{A}$	
Shared key K_{AB} ⇓	
$K_{AB} = B^a \bmod p$.	$K_{AB} = A^b \bmod p$
$= 189^{400} \bmod 919$	$= 128^{729} \bmod 919$
$= \underline{2}$ (Shared key)	$= \underline{2}$.

Q 10. $p = 11$

$q = 17$

$m = 45$

$n = p \times q = 187$

$\phi(n) = (p-1)(q-1) = 160$

$e = 7$ (gcd = 1)

$e \cdot d \bmod \phi(n) = 1$.

$d = 23$

gcd (160, 7)

~~160 = 7(22) + 6~~

gcd (7, 6)

7 = 6(1) + 1

gcd (6, 1)

6 = (1)(6) + 0

⇒ gcd = 1

public key : (e, n)

encryption : $y = m^e \bmod n$.

$y = 45^7 \bmod 187 =$

$(45^2 \times 45^4 \times 45^1) \bmod 187$

$45^2 \bmod 187 = 155$, $45^4 \bmod 187 = 89$, $45 \bmod 187 = 45$

$155 \times 89 \bmod 187 = 144$.

$144 \times 45 \bmod 187 = 122$.

Cipher text = 122.

private key : (d, n). $m = y^d \bmod n$.

$= 122^{23} \bmod 187$

$= 45$.

PAPERWORK

Q8. a) $\deg(v_1) + \dots + \deg(v_n) = 2n$.

$8x + 5 \times 4 + 6 \times 5 + 7 \times 6 = 2(58)$

$8x + 20 + 30 + 42 = 116$

$8x = 24$

$x = 3$.

b). $5 \times 4 + 7 + 7 \times 2 + 4x + 3y = 2(30)$

$41 + 4x + 3y = 60$

$4x + 3y = 19 \quad -①$

$7 + 7 + 5 + x + y = 24$.

$x + y = 5 \quad -②$.

$y = 5 - x$, put in eq ①

$4x + 3(5 - x) = 19$

$x = 4$.

Total no. of vertices with degree 4 = 9.

c) Hand shaking theorem is applied here.

Sum of odd numbers is even if and only if there is an even no. of odd no. So the no. of people who speak to odd no. of people (vertices) (degree) must always be even.

d) Total degrees $= 2 \times n$.

$= 2 \times 31 = 62$.

$3 \times 1 + 7 \times 4 + x = 62$

$x = 62 - 28 - 3 = 31$

Remaining 3 vertices must have degree that sums to 31.

$3 \times 1 + 7 \times 4 + 3d = 62$.

degree of 3 vertices $= d = 31/3 = 10.33$

not possible.

Distribution of degree is not possible as it violates rules of graph theory.

If one vertex has max degree (12), then other two would need degree summing to 19.

(distribution 9 and 10 possible)

e). Yes, a subgraph of a bipartite graph is bipartite

1. In a bipartite graph, $G = (V, E)$ is partitioned to U and V. $G = (V, U, E)$.

2. Any subset of vertices $V' \subseteq V$ and edges $E' \subseteq E$ in subgraph G' will maintain partitioning of U and V.

If bipartite graphs are required to have non empty edge sets, then

1. A subgraph with no edges can NOT be bipartite as it no longer meets the "non empty edge set condition"!

f). $n \times d = 15 \times 2$

$= 30.$

$30 = 1, 2, 3, 5, 6, 10, 15, 30.$

1. $n = 10$ and $d = 3$.
Regular graph. Could be cyclic with additional edges.

2. $n = 15$, $d = 2$
Regular graph with smaller cycles (e.g one cycle of 10 vertices and another 5 vertices)

g). i. 1, 1, 1, 1, 1, 1

$1 + 1 + 1 + 1 + 1 + 1 = 2e$

$3 = e$

Ⓐ — Ⓑ

Ⓒ — Ⓓ

Ⓔ — Ⓕ

ii. $5 + 4 + 3 + 2 + 1 = 15$

$15 = 2e$

$7.5 = e$ (not possible)

iii. $6 + 6 + 4 + 2 + 2 + 2 + 2 + 1$

$= 25.$

not possible.

4). Total edges $= \frac{n(n-1)}{2} = \frac{10(9)}{2} = 45$;

The no. of simple graphs with exactly 10 vertices are 2^{45}.

i) $\sum \deg(v) = 2 \times 35$

$\sum \deg(v) = 70$

$70 \geq 3 \times n$.

$n \leq \frac{70}{3} = 23.3$.

If there are 23 vertices, then sum of degree must be atleast $3 \times 23 = 69$. Hence it is possible to have 23 vertices where each vertex has degree of atleast 3.

j) $\sum \deg(v) = 2\,|E(G)|$

$V(G)$ is set of vertices and $E(G)$ is set of edges

$\sum \deg(v) = n \cdot k$ $\quad k$ = degree (odd)

$n \cdot k = 2\,|E(G)|$ $\quad n$ = no. vertices

$|E(G)| = \frac{n \cdot k}{2}$

$\frac{n \cdot k}{2}$ must be an integer and this is always true as long as n is even.

So $|E(G)| = k \cdot \left(\frac{n}{2}\right)$ always an integer

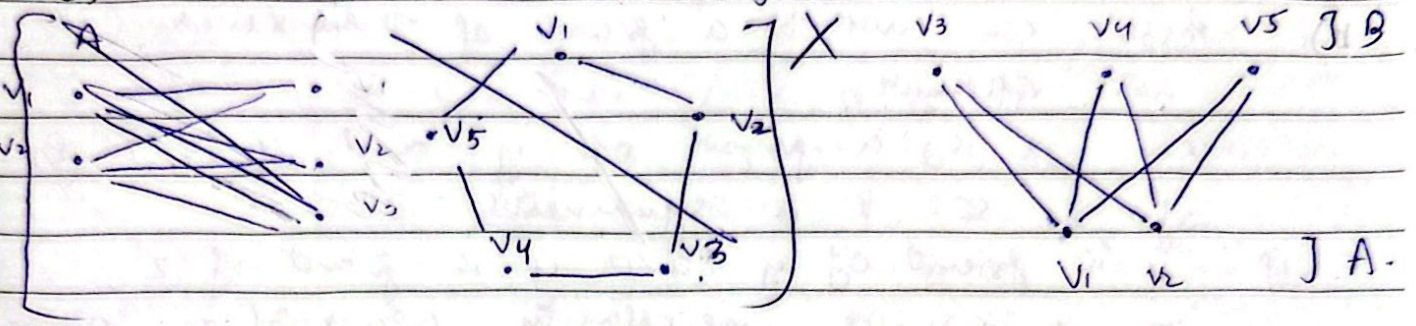
Hence qed.

k) $n-1$ vertices with odd degrees in G. and 1 even degree vertex

$\overline{G}$ has 1 odd degree vertex with $n-1$ vertices with odd degree.

So odd degree no. of vertices in G are $n-1$.

l). 5 vertices 6 edges. Bipartite graph.



m) Sum of degrees = $25 \times 3 = 75$.

$2E = 75$.

$E = 37.5$ (not possible)

so, 25 people can not have exactly 3 friends (vertices) (degree)

n). $\sum \deg(v) = 2E$.

$\sum \deg(v) = 2n$

where $\deg(v) \geq 2$. for all v.

so sum of degrees is atleast $2n (\sum \deg(v) \geq 2n)$.

If any vertex had degree greater than 2, sum of degrees would exceed $2n$.

Q7. a) A R B where A and B are disjoint sets.

R is not reflexive as $S = \{a, b, c, d, e\}$ so no element e.g (a, a) will exist.

e.g $A = \{a, b\}$, $B = \{c, d, e\}$.

$R = \{(a, c), (a, d), (a, e), (b, c), (b, d), (b, e)\}$.

no element e.g (a, b) and (b, a) exists so anti / not symmetric.

e.g If (a, c) and (a, d), then (c, d) should exist but no such element like that exists in R so not transitive.

b) Person can not be a friend of themselves, so not reflexive.

since x is a friend of y and y is a friend of x, so R is symmetric.

If x is friend of y and y is friend of z, x is not necessarily friend of z. So not transitive.

c) e.g $S = \{(1,2), (1,3), (1,4), (2,2)\}$.

$(1,2) R (1,2)$. } all will be reflexive.
$(1,3) R (1,3)$ }

Symmetric if $(x_1, x_2) R (y_1, y_2)$, then $(y_1, y_2) R (x_1, x_2)$

$(1,2) R (1,3)$ is valid but

$(1,3) R (1,2)$ $3 \not\leq 2$ so false.

Hence not symmetric and antisymmetric

checking for $(1,2) R (1,3)$ and $(1,3) R (1,4)$

$1 = 1$ and $2 \leq 3$ so valid

$1 = 1$ and $3 \leq 4$ so valid.

now $(1,2) R (1,4)$. $1 = 1$ and $2 \leq 4$.

Hence it is transitive.

d). eg $Q = \{1, 2, 3\}$, $P = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}$
$\{2,3\}\ \{1, 2, 3\}\}$.

XRX is valid for $x \subseteq X$ so R is reflexive.

$x \subseteq y$ does not imply $y \subseteq x$ unless both x and y are equal. So R is not symmetric

If $x R y$ and $y R z$, then $x R z$.

If $x \subseteq y$ and $y \subseteq z$, then $x \subseteq z$. So it is transitive.

R is assymmetric as if $x \subseteq y$ and $y \subseteq x$ then $x = y$.

2.

a). e.g $S = \{2, 3, 4, 6, 9, 15\}$.

$2 = 2$, $3 = 3$, $4 = 2^2$, $6 = 3 \times 2$, $9 = 3^2$, $15 = 3 \times 5$

largest prime divisor 2 : $\{2, 4\}$

" " 3 : $\{6; 9\}$.

" " 5 : $\{15\}$.

The largest prime divsr of x is the same as itself.

$x R x$, so R is reflexive.

if $x R y$ then $y R x$ as they will have the same largest prime divsr. Hence R is symmetric.

If $x R y$ and $y R z$ e.g $2 R 4$ and $4 R 8$ then $2 R 8$. So R is transitive.

Hence R is an equivalence relation.

Equivalence class of $z = 11$: $[11]$ all numbers divisible by 11, so $[11] = \{11, 22, 33, 44 \ldots\}$.

b). we have $x_1^2 + x_2^2 = x_1^2 + x_2^2$ so $(x_1, x_2) R (x_1, x_2)$

Thus, R is reflexive.

If $x_1^2 + x_2^2 = y_1^2 + y_2^2$ and so $y_1^2 + y_2^2 = x_1^2 + x_2^2$

so R is symmetric.

If $(x_1, x_2) R (y_1, y_2)$ and $(y_1, y_2) R (z_1, z_2)$ then $x_1^2 + x_2^2 = y_1^2 + y_2^2$ and $y_1^2 + y_2^2 = z_1^2 + z_2^2$ then by equality $x_1^2 + x_2^2 = z_1^2 + z_2^2$. So R is transiti

Equivalence class of $z = (2, 5)$ denoted $[(2, 5)]$ is set of ordered pairs $(x_1, x_2) \in S$ such that

$x_1^2 + x_2^2 = 2^5 + 5^2$.

$x_1^2 + x_2^2 = 29$

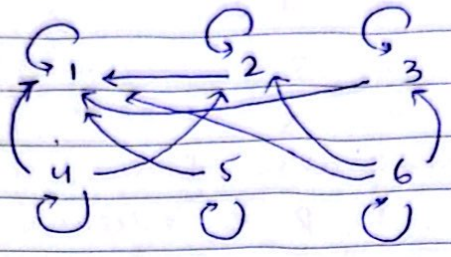
$x_1^2 + x_2^2 = \sqrt{29}$ (points on circle)

So points can have $(2, 5)$, $(-2, 5)$, $(\sqrt{29}, 0)$ ...

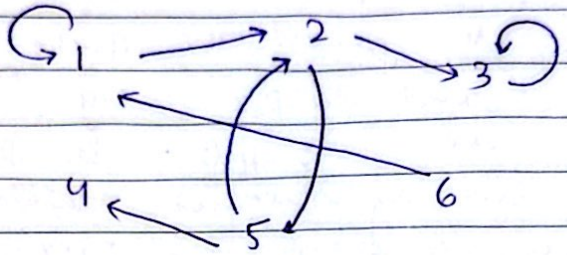
1 | 2 2 = 1.k

3) a). {1, 2, 3, 4, 5, 6}.

xRy : R = {(1,1) (2,1) (2,2) (3,1) (3,3) (4,1) (4,2) (4,4) (5,1) (5,5) (6,1) (6,2) (6,3) (6,6)}



b).



4:). xRy ⇒ x and y belong to same subset in partition.

eg For {1,3,6}: All pairs of elements from this are related. So (1,1) (1,3) (1,6) (3,1) (3,3) (3,6). (6,1) (6,3) (6,6)

So Final equivalence relation:

R = {(1,1) (1,3) (3,6) (3,1) (3,3) (3,6) (6,1) (6,3) (6,6) (2,2) (2,5) (5,2) (5,5) (4,4)}.

5) Partial order. Reflexivity, Antisymmetry, Transitivity.

$x \equiv y \pmod 5$

This means $5 \mid (x-y)$

xRx $\quad 5 \mid (x-x) = 5 \mid 0. \quad 0 = 5 \cdot k.$

So R is reflexive

xRy then yRx.

$x - y = 5k$ then $y - x = 5m$.

$(x-y) + (-x+y) = 0. \quad 0 = 5k + 5m.$

$k + m = 0.$

This does not show if $x = y$. So not antisymmetric.

xRy and yRz.

$x - y = 5k$ and $y - z = 5m$

$(x-y) + (y-z) = x - z = 5k + 5m$

$x - z = 5(k+m)$

$x - z = 5(v)$.

So xRz Hence R is transitive.

- R is NOT partial order as it is symmetric.

6. no. distinct elements = k.

a) $R = S \times S$.

no. elements $|S \times S| = k^2$

So total no. of relations on S are 2^{k^2}

Diagonal pairs: (a,a) pair must be symmetric.

Off-diagonal: (a,b) where $a \neq b$ both (a,b) and (b,a) should be included or both excluded.

k diagonal elements.

$\frac{k(k-1)}{2}$ unordered pairs

No. of symmetric relation:

$2^k \times 2^{\frac{k(k-1)}{2}} = 2^{\frac{k(k+1)}{2}}$

b). for antisymmetric relation.

Diagonal pairs we can either include (a,a) or not. So 2^k.

Off-diagonal pairs: we can have 3 choices.

1- exclude (a,b) and (b,a)

2- exclude (b,a) but not (a,b)

3- exclude (a,b) " " (b,a)

$2^k \times 3^{\frac{k(k-1)}{2}}$

7. aRb $\frac{b}{a}$ $a \mid b$. $b = a \cdot k$ //

Relation is antisymmetric if aRb and bRa. So it must mean $a = b$.
aRb means b is divisible by a.
bRa means a is divisible by b.
a divides b and b divides a. This implies $a = b$. So R is antisymmetric.

Q3. $A = \{ , 1, 2 \}$.
$B = \{ 1, 2, 3 \}$
$C = \{ 3, 4, 5, 6, 7, 8 \}$.

a) $A \cup B = \{ 1, 2, 3 \}$.
b) $A \cap B = \{1, 2\}$.
c) $A^c = \{ \ldots -1, 0, 3, 4, 5 \ldots \}$.
d) $A \cup C = \{ 1, 2, 3, 4, 5, 6, 7, 8 \}$.
e) $A \cap B = \{1, 2\}$
f) $B^c = \{ \ldots -1, 0, 4, 5, 6 \ldots \}$
g) $A^c \cup B = \{ \ldots -1, 0, 3, 4, 5, 6, 7 \ldots \}$
h) $A^c \cap B^c = \{ \ldots -1, 0, 4, 5, 6, 7 \ldots \}$
i) $(A \cup C)^c = \{ \ldots -1, 0, 9, 10, 11 \ldots \}$.
j) $(A \cap B)^c = \{ \ldots -1, 0, 3, 4, 5, 6 \ldots \}$
k. $A \oplus B = (A - B) \cup (B - A)$
$= \emptyset \cup 3$.
$= \{3\}$.

Q6. Complete → vertex and degree is 7 of each.
So Total degree
$7n$
So total degree $7n = 7 \times 25 = 175$.
It is impossible to construct a graph where each vertex has degree 7 and 25 vertices present as total degree is odd.

Q4. Let A : set of multiples of 2
B : set of multiples of 3.
C : set of multiples of 5

Inclusion - exclusion principle

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

$|A \cap B| = 30$ (multiples of 2 and 3, so 6).
$|A \cap C| = 33$ (multiples of 10).
$|B \cap C| = 25$ (multiples of 15).
$|A \cap B \cap C| = 13$

So $|A \cup B \cup C| = 80 + 95 + 70 - 30 - 33 - 25 + 13$
$= 170.$

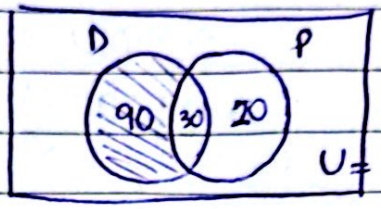
Q5. $R = \{(x,y) \mid D(x,y) = 50\}$.
$R = \{(a,b)\ (a,0)\ (b,a)\ (b,0)\ (0,a)\ (0,b)\}$.
a R a but the distance of a from itself is not 50 km but 0. So R is not reflexive.
If a R b then b R a as distance from both will be the same i-e 50 km.
So R is symmetric.
a R b and b R 0 then a R 0 because all have the same distance from eachother
So R is transitive.
Hence R is equivalence relation.

Q1. $|D| = 120$ $|P| = 50$ $|D \cap P| = 30$

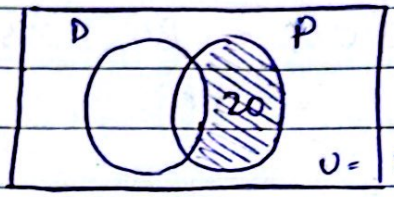
$|D \cap P| = |D| + |P| - |D \cap P| + |D \cap P|$

1. $|D - P| = |D| - |D \cap P| = 120 - 30 = 90$
2. $|P - D| = |P| - |D \cap P| = 50 - 30 = 20.$
3. $|D \cup P| = |D| + |P| - |D \cap P| = 120 + 50 - 30 = 140.$

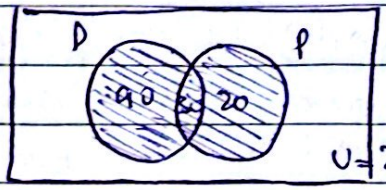
1.



2.

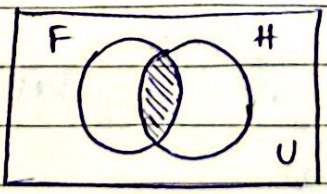


3.

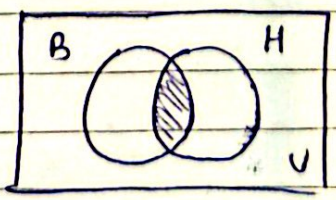


Q2.

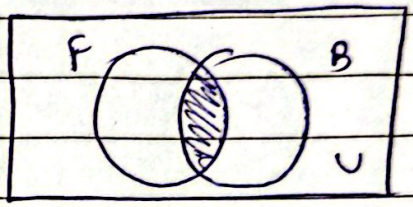
1. $|F| = 245$
2. $|H| = 265$
3. $|B| = 310$
4. $|F \cap H| = 135.$



5. $|B \cap H| = 145$



6. $|F \cap B| = 145$



7. $|\text{No game}| = 25$.