2020

DISCRETE

ASSIGNMENT

Problems

Roll No: 19k-1048
Amman Soomro
SE - A

Q.1

Sol: Reflexive

Q. 2:

Sol: Reflexive, Symmetric, Transitive.

Q.3

a) $a = b$

$R = \{(0,0), (1,1), (2,2), (3,3)\}$

b) $a + b = 4$

$R = \{(1,3), (2,2), (3,1), (4,0)\}$

c) $a > b$

$R = \{(1,0), (2,0), (3,0), (4,0), (2,1), (3,1), (4,1), (3,2), (4,2), (4,3)\}$

d) $a | b$

$R = \{(1,0), (2,0), (3,0), (4,0), (1,1), (1,2), (2,2), (1,3), (3,3)\}$

- All non-negative integars are divisor of 0

e) $\gcd(a,b) = 1$

$R = \{(1,0), (1,1), (0,1), (1,2), (1,3), (2,1), (3,1), (4,1), (2,3), (3,2), (4,3)\}$

f) $\text{lcm}(a,b) = 2$

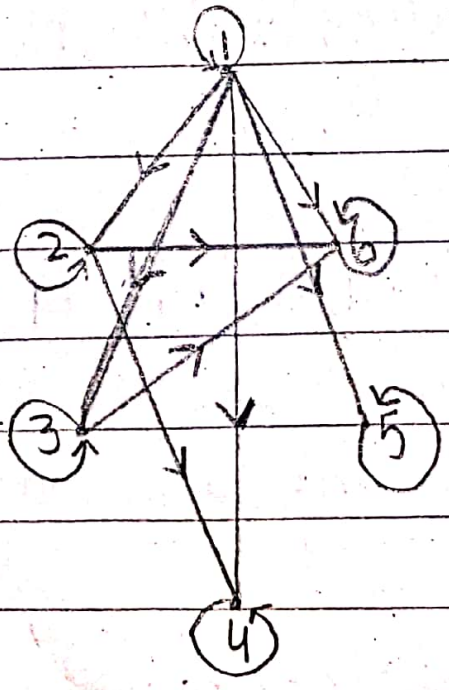
$R = \{(1,2), (2,1), (2,2)\}$

Q.4: a divides b

$A = \{1, 2, 3, 4, 5, 6\}$

Sol: $R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$

R	1	2	3	4	5	6
1	1	1	1	1	1	1
2	0	1	0	1	0	1
3	0	0	1	0	0	1
4	0	0	0	1	0	0
5	0	0	0	0	1	0
6	0	0	0	0	0	1



Q.5:

a) Transitive.

b) Reflexive, Symmetric, Transitive.

c) Symmetric

d) Anti-symmetric.

e) Reflexive, Symmetric, Anti-Symmetric, Transitive.

f) ~none.

Q.6

a) Anti-symmetric, Transitive.

b) Reflexive, Symmetric, Transitive

c) Reflexive, Symmetric, Transitive.

d) Reflexive, Symmetric.

Q.7

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

b) $R = \{(1,2), (2,3), (3,9)\}$

Q.8

a) $R_2 \cup R_4$

$= \{(a,b) \in R^2 \mid a \geq b \text{ or } a \leq b\}$

$= \{(a,b) \in R^2 \mid T\}$

$= \{(a,b) \in R^2\}$

$= R^2$

b) $R_3 \cup R_6$

$= \{(a,b) \in R^2 \mid a < b \text{ or } a \neq b\}$

$= \{a < b \text{ or } (a < b \text{ or } a > b)\}$

$= \{a < b \text{ or } a > b\}$ $\quad \because P \vee P \equiv P$

$= \{a \neq b\}$

$= R_6$

c) $R_3 \cap R_6$

$= \{a < b \text{ and } a \neq b\}$

$= \{(a < b \text{ and } a < b) \text{ or } (a < b \text{ and } a > b)\}$

$= \{a < b \text{ or } F\}$ $\quad p \vee F = p$

$= \{a < b\}$

$= R_3$

d) $R_4 \cap R_6$

$= \{a \leq b \text{ and } a \neq b\}$

$= \{a < b\}$

$= R_3$.

e) $R_3 - R_6$

$= \{ a < b \text{ and not } a \neq b \}$

$= \{ a < b \text{ and } a = b \}$

$= \emptyset$

f) $R_6 - R_3$

$= \{ a \neq b \text{ and not } a < b \}$

$= \{ a \neq b \text{ and } a \geq b \}$

$= \{ a > b \}$

$= R_5$.

g) $R_2 \oplus R_6$

$= [\{(a \geq b) \text{ or } (a \neq b)\} \text{ and not } \{(a \geq b) \text{ and } (a \neq b)\}]$

$= \{(a \geq b \text{ or } a \neq b) \text{ and not } (a > b)\}$

$= \{ T \text{ and } a \leq b \}$ $\quad \therefore P \wedge T = P$

$= \{a \leq b\}$

$= R_4$.

h) $R_3 \oplus R_5$

$= \{(a < b \text{ or } a = b) \text{ and not } (a < b \text{ and } a = b)\}$

$= \{ (a \leq b) \text{ and not } F \}$

$= \{ (a \leq b) \text{ and } T \}$

$= R_4$.

i) $R_2 \circ R_1$

$= \{ (a,b) \in R_1 \text{ and } (b,c) \in R_2 \}$

$= \{ a \succ b \text{ and } b \succeq c \}$

$= \{ a \succ c \}$

$= \{ a \succ b \}$

$= R_1$

j) $R_6 \circ R_6$

$= \{ (a,b) \in R_6 \text{ and } (b,c) \in R_6 \}$

$= \{ a \neq b \text{ and } b \neq c \}$

$= \{ (a,c) \in R^2 \mid T \}$

$= \{ a,c) \in R^2 \}$

$= R^2$

Q.9: (a)

a) {(1,1), (1,2), (1,3)}

b) {(1,2), (2,1), (2,2), (3,3)}

c) {(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)}

d) {(1,3), (3,1)}

a)

1	1	1
0	0	0
0	0	0

b)

0	1	0
1	1	0
0	0	1

1	1	1
0	1	1
0	0	1

0	0	1
0	0	0
1	0	0

Q.9 (b)

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

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

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

Q.10(a)

Reflexive: Because $l(a) = l(a)$ it follows that aRa for all strings a.

Symmetry: Suppose that aRb. Since $l(a) = l(b)$, $l(b) = l(a)$ also holds bRa.

Transitive: Suppose that aRb and bRc. Since $l(a) = l(b)$, and $l(b) = l(c)$, $l(a) = l(c)$, holds aRc.

(b) Reflexive: $a \equiv a \pmod m$ since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$.

Symmetry: $a \equiv b \pmod m$, then $a - b$ divisible by m, and so $a - b = km$, where k is an integer. It follows $b - a = (-k)m$, so $b \equiv a \pmod m$.

Transitive. $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Then m divides both $a - b$ and $b - c$. Hence, there are integers k and l with $a - b = km$ and $b - c = lm$. We obtain by adding the equations: $a - c = (a - b) + (b - c) = km + lm = (k + l)m$

Therefore, $a \equiv c \pmod m$.

Q.11	Quotient	Remainder.
a) 19/7	2	5
b) -111/11	-11	10
c) 789/83	34	7
d) 1001/13	77	0
e) 10/19	0	10
f) -1/3	-1	2
g) 3/5	0	3
h) 4/1	4	0

- Using $a = dq + r$

Q.12 Show that [illegible]

a) $19 = 7(2)+5$ $19 = 19$

b) $-111 = 11(-11)+10$ $-111 = -111$

c) $789 = 23(34)+7$ $789 = 789$

d) $1001 = 13 \times 77 + 0$ $1001 = 1001$

e) $10 = 19 \times 0 + 10$ $10 = 10$

f) $-1 = 3 \times (-1) + 2$ $-1 = -1$

g) $3 = 5(0)+3$ $3 = 3$

h) $4 = 1(4)+0$ $4 = 4$.

Q.12

[redacted] $a \bmod m \equiv b \bmod m \Rightarrow a \equiv b \pmod m$

→ $a \equiv b \pmod m \Rightarrow m \mid a-b$

→ $a = m\left(\frac{a}{m}\right) + a \bmod m \quad ; b = m\left(\frac{b}{m}\right) + b \bmod m$

→ $a-b = m\left\{\left(\frac{a}{m}\right) - \left(\frac{b}{m}\right) + (a \bmod m - b \bmod m)\right\}$

→ $a \bmod m = b \bmod m \Rightarrow a-b = m\left(\left(\frac{a}{m}\right) - \left(\frac{b}{m}\right)\right)$

⇒ $m \mid a-b \Rightarrow a \equiv b \pmod m$

Q.13:	a div m	a mod m
1) a = -111 ; m = 99	$-2 \rightarrow (-111 = 99 \times (-2) + 87)$	87
2) a = -9999; m = 101	$-99 \rightarrow (-9999 = -99 \times 101 + 0)$	0
3) a = 10999; m = 999	$10 \rightarrow (a = 999 \times 10 + 0)$	309
4) a = 123456; m = 1001	$123 \rightarrow (a = 1001 \times 123 + 333)$	333

- Using $a = qd + r$.

Q.14: Congruent to 5 modulo 17.

a) 80 b) 103 c) -99 d) -122

- Keep adding 17 to 5. and minus.

5+17 mod 17	5-17 mod 17
17+99 mod 17	-17 " "
39+17 mod 17	-39 " "
56+17 mod 17	-46 " "
73+17 mod 17	-63 " "
90+17 mod 17	-80 " "
107 mod 17.	-97 " "
	-114 " "
	-131 " "

a) Not Congruent
b) Not Congruent
c) Congruent
d) Not Congruent

Q.15 Pairwise relatively prime.

a) 11, 15, 19

Sol: $11 = 11$; $15 = 3 \cdot 5$; $19 = 19$

$\gcd(11, 15) = 1$

$\gcd(11, 19) = 1$

$\gcd(15, 19) = 1$

• Relatively Prime. Ans.

b) 14, 15, 91

Sol: $14 = 2 \cdot 7$; $15 = 3 \cdot 5$; $91 = 3 \cdot 7$

$\gcd(14, 15) = 1$

$\gcd(14, 91) = 1$

$\gcd(15, 91) = 3$

• Not relatively prime.

c) 19, 17, 31, 37

Sol: $19 = 2 \cdot 2 \cdot 3$; $17 = 17$; $31 = 31$; $37 = 37$

$\gcd(19, 17) = 1$

$\gcd(19, 31) = 1$

$\gcd(19, 37) = 1$

$\gcd(17, 31) = 1$

$\gcd(17, 37) = 1$

$\gcd(31, 37) = 1$

• Relatively Prime.

d) 7, 8, 9, 11

Sol: $7 = 7$; $8 = 2 \cdot 2 \cdot 2$; $9 = 3 \cdot 3$; $11 = 11$

$\gcd(7,8) = 1$

$\gcd(7,9) = 1$

$\gcd(7,11) = 1$

$\gcd(8,9) = 1$

$\gcd(8,11) = 1$

$\gcd(9,11) = 1$

• Relatively Prime.

Q.16: Prime Factorization:

a) 88

Sol: $88 = 2 \cdot 2 \cdot 2 \boxed{11}$

b) 196

Sol: $196 = 2 \cdot 3 \cdot 3 \boxed{7}$

c) 729

Sol: $729 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \boxed{3}$

d) 1001

Sol: $1001 = 7 \cdot 11 \cdot \boxed{13}$

e) 1111

Sol: $1111 = 11 \cdot \boxed{101}$

f) 909

Sol: $909 = 3 \cdot 3 \boxed{101}$

Q.17 : Euclidean Algorithm.

a) (144, 89)

Sol: $144 = 1 \cdot 89 + 55$ $\quad 13 = 1 \cdot 8 + 5$

$89 = 1 \cdot 55 + 34$ $\quad 8 = 1 \cdot 5 + 3$

$55 = 1 \cdot 34 + 21$ $\quad 5 = 1 \cdot 3 + 2$

$34 = 1 \cdot 21 + 13$ $\quad 3 = 1 \cdot 2 + 1$

$21 = 1 \cdot 13 + 8$ $\quad 2 = 2 \cdot 1$

→ $q_1 - q_9 = 1$

→ $s_0 = 1 ; s_1 = 0 \quad ; t_0 = 0 ; t_1 = 1$

→ $s_2 = s_0 - q_1 s_1 = 1$ $\quad t_2 = t_0 - q_1 t_1 = -1$

$s_3 = s_1 - q_2 s_2 = -1$ $\quad t_3 = t_1 - q_2 t_2 = 2$

" " " $= 2$ $\quad$ " " " $= -3$

" " " $= -3$ $\quad$ " " " $= 5$

" " " $= 5$ $\quad$ " " " $= -8$

" " " $= -8$ $\quad$ " " " $= 13$

" " " $= 13$ $\quad$ " " " $= -21$

" " " $= -21$ $\quad$ " " " $= 34$

" " " $= 34$ $\quad$ " " " $= -55$

⇒ $\gcd(144, 89) = 34 \cdot 144 + (-55) \cdot 89$ Ans.

b) (1001, 100001)

Sol: $100001 = 99 \cdot 1001 + 902$

$1001 = 1 \cdot 902 + 99$

$902 = 9 \cdot 99 + 11$

$99 = 9 \cdot 11$

→ $q_1 = 9$; $q_2 = 1$; $q_3 = 99$.

→ $s_0 = 1$; $s_1 = 0$; $t_0 = 0$; $t_1 = 1$

$s_2 = 1$ $t_2 = -99$

$s_3 = -1$ $t_3 = 100$

$s_4 = 10$ $t_4 = -999$

$\gcd(a, b) = s_n a + t_n b$

$\gcd(1001, 100001) = 10 \cdot (10001) + (-999) \cdot 1001$ Ans.

Q. 18) (a)

a) $55x \equiv 34 \pmod{89}$

Sol:

$89 = 55 \cdot 1 + 34$

$55 = 34 \cdot 1 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2 \cdot 1$

$2 = 5 - 3 \cdot 1$

$3 = 8 - 5 \cdot 1$

$5 = 13 - 8 \cdot 1$

$8 = 21 - 13 \cdot 1$

$13 = 34 - 21 \cdot 1$

$21 = 55 - 34 \cdot 1$

$34 = 89 - 55 \cdot 1$

$\Rightarrow 1 = 34 \cdot 55 + (-21) \cdot 89$ | Inverse

$\Rightarrow 34 \cdot 55 \equiv 34 \pmod{89}$ | $55 \Rightarrow 34$

• Multiply both sides by 34

$x \equiv 34 \times 34 \pmod{89}$

$x = 1156 \mod 89$

$x = 88.$

Q.18 (b):

$232 = 89(2) + 54$

$89 = 54(1) + 35$

$54 = 35(1) + 19$

$35 = 19(1) + 16$

$19 = 16(1) + 3$

$16 = 3(5) + 1$

$1 = 16 - 3 \cdot 5$

$3 = 19 - 16 \cdot 1$

$16 = 35 - 19 \cdot 1$

$19 = 54 - 35 \cdot 1$

$35 = 89 - 54 \cdot 1$

$54 = 232 - 89 \cdot 2$

$1 = 73 \cdot 89 - 28 \cdot 232$

$\rightarrow 73 \cdot 89 \pmod{232}$

inverse

$89 = 73$

- Multiply both sides by 73

$x = 73 \times 2 \pmod{232}$

$x = 146 \bmod 232$

$x = 146$ Ans.

Q.19(a) (ii)

$a=1 \; ; \; a_2=2 \; ; \; a_3=3 \; ; \; a_4=4$

$m_1=2 \; ; \; m_2=3 \; ; \; m_3=5 \; ; \; m_4=11$

$M = 2 \cdot 3 \cdot 5 \cdot 11 = 330.$

$Z_1 = 330/2 = 165 \qquad Z_3 = 330/5 = 66$

$Z_2 = 330/3 = 110 \qquad Z_4 = 330/11 = 30$

$Y_1 = 165^{-1} \pmod 2 = 1^{-1} \pmod 2 = 1 \pmod 2 = 1$

$Y_2 = 110^{-1} \pmod 3 = 2^{-1} \pmod 3 = 2 \pmod 3 = 2$

$Y_3 = 66^{-1} \pmod 5 = 1^{-1} \pmod 5 = 1 \pmod 5 = 1$

$Y_4 = 30^{-1} \pmod{11} = 8^{-1} \pmod{11} = 7 \pmod{11} = 7$

$W_1 = 165 \pmod{330} = 165$

$W_2 = 220 \pmod{330} = 220$

$W_3 = 66 \pmod{330} = 66$

$W_4 = 210 \pmod{330} = 210$

$X = 1 \cdot 165 + 2 \cdot 220 + 3 \cdot 66 + 4 \cdot 210 \pmod{330}$

$X = 1643 \pmod{330} \rightarrow \boxed{X = 323}$

$\Rightarrow 323 + 330k$ Ans.

a) (i) $a_1 = 1$; $a_2 = 9$; $a_3 = 3$

$m_1 = 5$; $m_2 = 6$; $m_3 = 7$

$M = 910$

$Z_1 = 210/5 = 42$ $\qquad$ $Z_3 = 210/7 = 30$

$Z_2 = 210/6 = 35$

$Y_1 = 42^{-1} \pmod 5 = 2^{-1} \pmod 5 = 3$

$Y_2 = 35^{-1} \pmod 6 = 5^{-1} \pmod 6 = 5$

$Y_3 = 30^{-1} \pmod 7 = 9^{-1} \pmod 7 = 4$

$W_1 = 196$

$W_2 = 175$

$W_3 = 120$.

$X = 1 \cdot 196 + 9 \cdot 175 + 3 \cdot 180 \pmod{910}$

$= 836 \pmod{910} \Rightarrow 906$

$\Rightarrow$ 906 + 910k Ans.

Q.19(b)

$a_1 = 3$; $a_2 = 3$; $a_3 = 1$; $a_4 = 0$

$m_1 = 5$; $m_2 = 6$; $m_3 = 7$; $m_4 = 11$

$m = 5 \cdot 6 \cdot 7 \cdot 11 \Rightarrow 2310$

$M_1 = 2310/5 = 462$ $M_2 = 2310/6 = 385$

$M_3 = 2310/7 = 330$ $M_4 = 2310/11 = 210$

$Y_1 = 462^{-1} \pmod 5 = 2^{-1} \pmod 5 = 3$

$Y_2 = 385^{-1} \pmod 6 = 1^{-1} \pmod 6 = 1$

$Y_3 = 330^{-1} \pmod 7 = 1^{-1} \pmod 7 = 1$

$Y_4 = 210^{-1} \pmod{11} = 1^{-1} \pmod 7 = 1$

$W_1 = 1386 \pmod{2310}$

$W_2 = 385 \pmod{2310}$

$W_3 = 330 \pmod{2310}$

$W_4 = 210 \pmod{2310}$

$X = 3 \cdot (1386) + 3(385) + 1(330) + 0(210) \pmod{2310}$

$X = 5643 \pmod{2310}$

$X = 1023$ Ans.

Q. 80:

a) $a = 2$; $m = 17$

$\gcd(2, 17) = 1$

$17 = 2 \cdot 8 + 1$

$1 = 1 \cdot 17 - 8 \cdot 8$

$1 = 1 \cdot 17 - 8 \cdot 2$

-8 is the inverse.

b) $a = 34$; $m = 89$

$89 = 34 \cdot 2 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 21 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 1 \cdot 2$

$1 = 1 \cdot 3 - 1 \cdot 2$

$1 = 1 \cdot 3 - 1(5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5$

" " " "

" " " " " "

$1 = 13(89 - 2 \cdot 34) - 8 \cdot 34 = 13 \cdot 89 - 34 \cdot 34$

$1 = 13 \cdot 89 - 34 \cdot 34.$

$\gcd(34, 89) = 1$ Hence, -34 is inverse

b) $a = 200$; $m = 1001$

$1001 = 5 \cdot 200 + 1$

$200 = 200 \cdot 1 + 0$

$\gcd(200, 1001) = 1$

$1 = 1001 - 5 \cdot 200$

$1 = 1 \cdot 1001 - 5 \cdot 200$

The inverse is -5. Ans.

c) $a = 144$, $m = 233$

$233 = 1 \cdot 144 + 89$

$144 = 1 \cdot 89 + 55$

$89 = 1 \cdot 55 + 34$

$55 = 1 \cdot 34 + 21$

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 2 \cdot 1$

$1 = 1 \cdot 3 - 1 \cdot 2$

$1 \cdot 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5$

" " " " " "

" " " " " "

$1 = 34 \cdot 144 - 55 \cdot (233 - 1 \cdot 144)$

$= 89 \cdot 144 - 55 \cdot 233$

$1 = 89 \cdot 144 - 55 \cdot 233$

Inverse = 89 Ans.

Q.21: STOP POLLUTION

a) $F(P) = (P+4) \bmod 26$

A=0	B=1	C=2	D=3	E=4	F=5
G=6	H=7	I=8	J=9	K=10	L=11
M=12	N=13	O=14	P=15	Q=16	R=17
S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25.				

⇒ 18 19 14 15 15 14 11 11 20 19 8 14 13

⇒ 22 23 18 19 19 18 15 15 24 23 18 18 17

⇒ W X S T T S P P Y X M S R

b) $F(P) = (P+21) \bmod 26$

⇒ 18 19 14 15 15 14 11 11 20 19 8 14 13

⇒ 13 14 9 10 10 9 6 6 15 14 3 9 8

⇒ N O J K K J G G P O D J I

Q.91 (b)

a) C E B B O X N O B X Y G

→ 2 4 1 1 14 23 13 14 1 23 24 6

• decryption $f^{-1}(p) = (p-10) \bmod 26$

⇒ 18 20 17 17 4 13 4 17 13 14 22

• SURRENDER NOW.

b) L O W I P B S O X N.

⇒ 11 14 22 8 15 1 18 14 23 13

• decryption $f^{-1}(p) = (p-10) \bmod 26$

→ 1 4 13 24 5 17 8 4 13 3

BE MY FRIEND

Q.99

a) $5^{2003} \equiv (5^6)^{334} \cdot 5^{-1} \pmod 7$

$\equiv 1 \cdot 5^{-1} \pmod 7$

$\equiv 3 \pmod 7$

b) $5^{2003} \equiv (5^{10})^{200} \cdot 5^3 \pmod{11}$

$\equiv 1 \cdot 125 \pmod{11}$

$\equiv 4 \pmod{11}$

c) $5^{2003} \equiv (5^{12})^{167} \cdot 5^{-1} \pmod{13}$

$\equiv 1 \cdot 5^{-1} \pmod{13}$

$\equiv 8 \pmod{13}$.

Q.#3(a)

- I LOVE DISCRETE MATHEMATICS

8 11 14 9 1 4 3 8 18 9 17 4 19 4 19 20 19 7 4 19 20 19 8

11 14 17 9 4 7 6 11 21 5 20 7 9 9 7 15 3 22 10 7 15 2 3 5 18 22 11 21

- L OR VH GLVFUHWH PDWKHPDWLFV.

b)

i) MID TWO ASSIGNMENT.

ii) FAST NUCES UNIVERSITY.

Q. $g4(a) = h(k) = k \bmod 97$

i) 034567981

ii) 183911239

iii) 2201945744

iv) 9879955335

- $a = qd + r$

i) $k = 356370 \cdot 97 + 91$

$= 034567981 \bmod 97$

$= 91$ Ans.

ii) $k = 1888775 \cdot 97 + 57$

$= 183911939 \bmod 97$

$= 57$ Ans.

iii) $k = 9970059 \cdot 97 + 91$

$= 9901945744 \bmod 97$

$= 91$ Ans.

iv) $k = 10177890 \cdot 97 + 5$

$= 9879955335 \bmod 97$

$= 5$ Ans.

Q.34(b): $h(k) = k \bmod 101$

i) 104578690

ii) 432222187

iii) 379201919

iv) 501338753

i) $k = 1035439 \cdot 101 + 58$

$= 104578690 \bmod 101$

$= 58$ Ans

ii) $k = 4279427 \cdot 101 + 60$

$= 432222187 \bmod 101$

$= 60$

iii) $k = 3685167 \cdot 101 + 52$

$= 379201919 \bmod 101$

$= 59$

4963750

iv) $k = 3[redacted] \cdot 101 + 3$

$= 501338753 \bmod 101$

$= 3$

Q. 35: Pseudorandom Number:

- $x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$.

$\because (ax_n + c) \bmod m$

Sol: $4(3)+1 \bmod 7 = 6$

$4(6)+1 \bmod 7 = 4$

$4(4)+1 \bmod 7 = 3$

$4(3)+1 \bmod 7 = 6$

$\Rightarrow$ 6, 4, 3, 6, 4, 3, 6, 4.... Ans.

Q. 36 (a):

i) 73939184434

Sol: $3(7)+3+3(2)+3+3(2)+1+3(8)+4+3(4)+3+3(4)+x_{12} \bmod$

$\Rightarrow 91+3+6+3+6+1+24+4+12+3+12+x_{12} \bmod 10$

$\Rightarrow 95 + x_{12} \bmod 10$

$\Rightarrow x_{12} = -95 \bmod 10$

$\Rightarrow x_{12} = 5$

$\Rightarrow$ Check digit = 5 Ans.

ii) 6368399 1346

Sol: $6(3)+3+6(3)+9+3(3)+9+9(3)+1+3(3)+4+6(3)+x_{12} \bmod 10$

$\Rightarrow 18+3+18+9+9+9+7+1+9+4+18+x_{12} \bmod 10.$

$\Rightarrow 118 + x_{12} \bmod 10$

$\Rightarrow x_{12} = -118 \bmod 10$

$\Rightarrow x_{12} = 9$

• Check digit = 2 Ans.

Q. 96(b)

a) 036000291459

⇒ 3(0)+3+3(6)+0+3(0)+0+3(9)+9+3(1)+4+3(5)+9 mod 10

⇒ 0+3+18+0+0+0+6+9+3+4+15+9 mod 10

⇒ 60 mod 10

→ 0 valid UPC code.

b) 019345678903

→ 3(0)+1+3(2)+3+3(4)+5+3(6)+7+3(8)+9+3(0)+3 mod 10

⇒ 0+1+6+3+19+5+18+7+24+9+0+3 mod 10

→ 88 mod 10

⇒ 8 not a valid UPC code.

Q.87(a)

i) 119881 (007)

Sol: $x_{10} = 1.0 + 2.0 + 3.7 + 4.1 + 5.1 + 6.9 + 7.8 + 8.9 + 9.1 \bmod 11$

$= 0 + 0 + 21 + 4 + 5 + 54 + 56 + 64 + 9 \bmod 11$

$= 213 \bmod 11$

$= 4$

- Check digit = 4

ii) 0381500018

Sol: $x_{10} = 1.0 + 2.3 + 3.8 + 4.1 + 5.5 + 6.0 + 7.0 + 8.0 + 9.1 \bmod 11$

$= 0 + 6 + 6 + 4 + 25 + 0 + 0 + 80 + 9 \bmod 11$

$= 50 + 80 \bmod 11$

- Check digit ⇒ 8

$\Rightarrow 80 + 50 \bmod 11 = 8$

$\Rightarrow \because 50 \bmod 11 = 6$

$\Rightarrow 80 + 6 \bmod 11 = 8$

$\Rightarrow 80 \bmod 11 = 9$

$\Rightarrow 80 \bmod 11 = 9 \bmod 11$

$\Rightarrow 560 \bmod 11 = 14 \bmod 11$

$\Rightarrow Q = 3$ Ans.

$\because 8^{-1} \bmod 11 = 7$

Q.38: ATTACK

A=00 ; B=01 ; C=02; D=03; E=04 ; F=05; G=06
H=07 ; I=08; J=09; K=10 ; L=11 ; M=12 ; N=13
O=14 ; P=15 ; Q=16 ; R=17; S=18; T=19 ; U=20
V=21 ; W=22; X=23; Y=24; Z=25.

• A T T A C K
00 19 19 00 02 10
0019 1900 0210

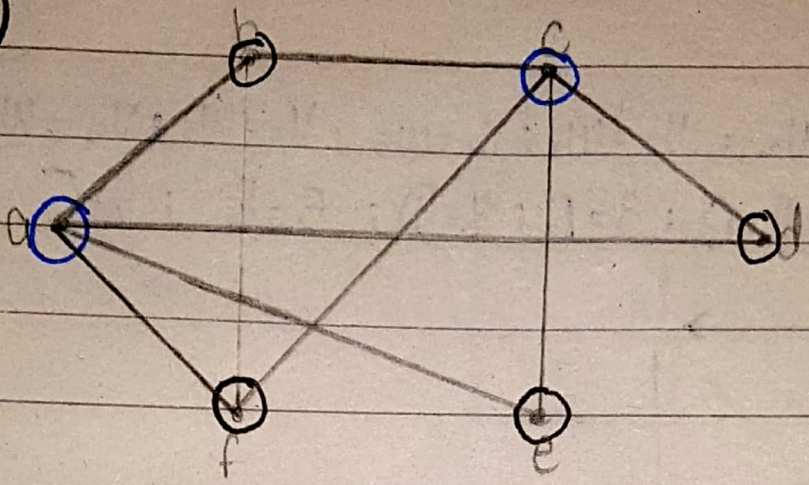
∵ $C = M^{13} \mod 2537$

$C_1 = 0019^{13} \mod 2537 = 2299$
$C_2 = 1900^{13} \mod 2537 = 1317$
$C_3 = 0210^{13} \mod 2537 = 2117$

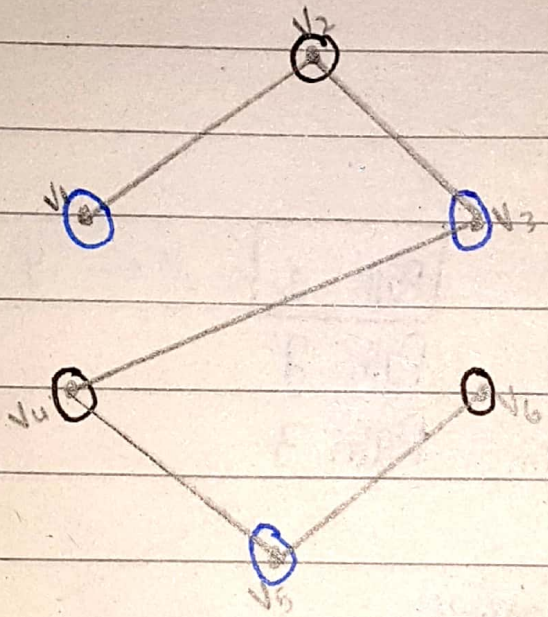
Encryption: 2299 1317 2117.

Q.39)

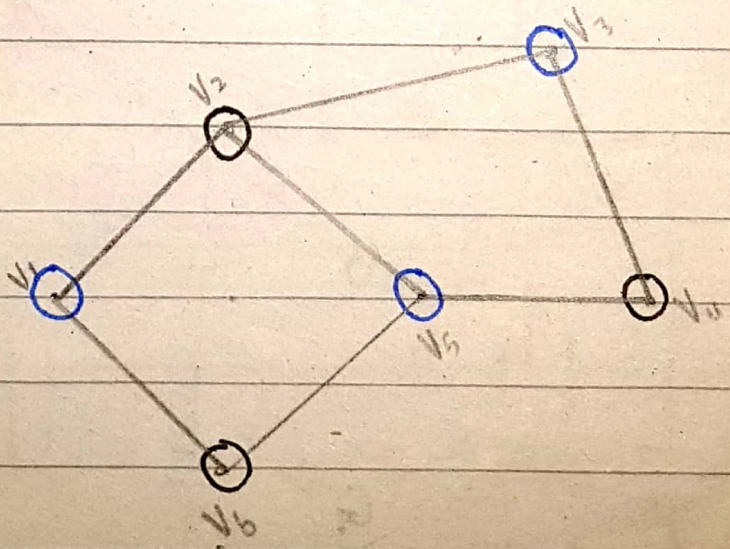
a)



b)



c)

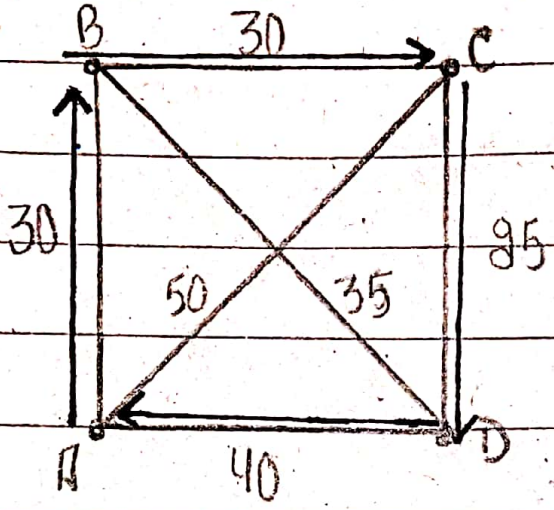


Q.30)

a) Isomorphic $V_1 = W_2$; $V_3 = W_1$; $V_4 = W_5$; $V_2 = W_3$; $V_5 = W_4$

b) Isomorphic 1 = B ; 2 = C ; 3 = A ; 4 = D ; 5 = E ; 6 = F

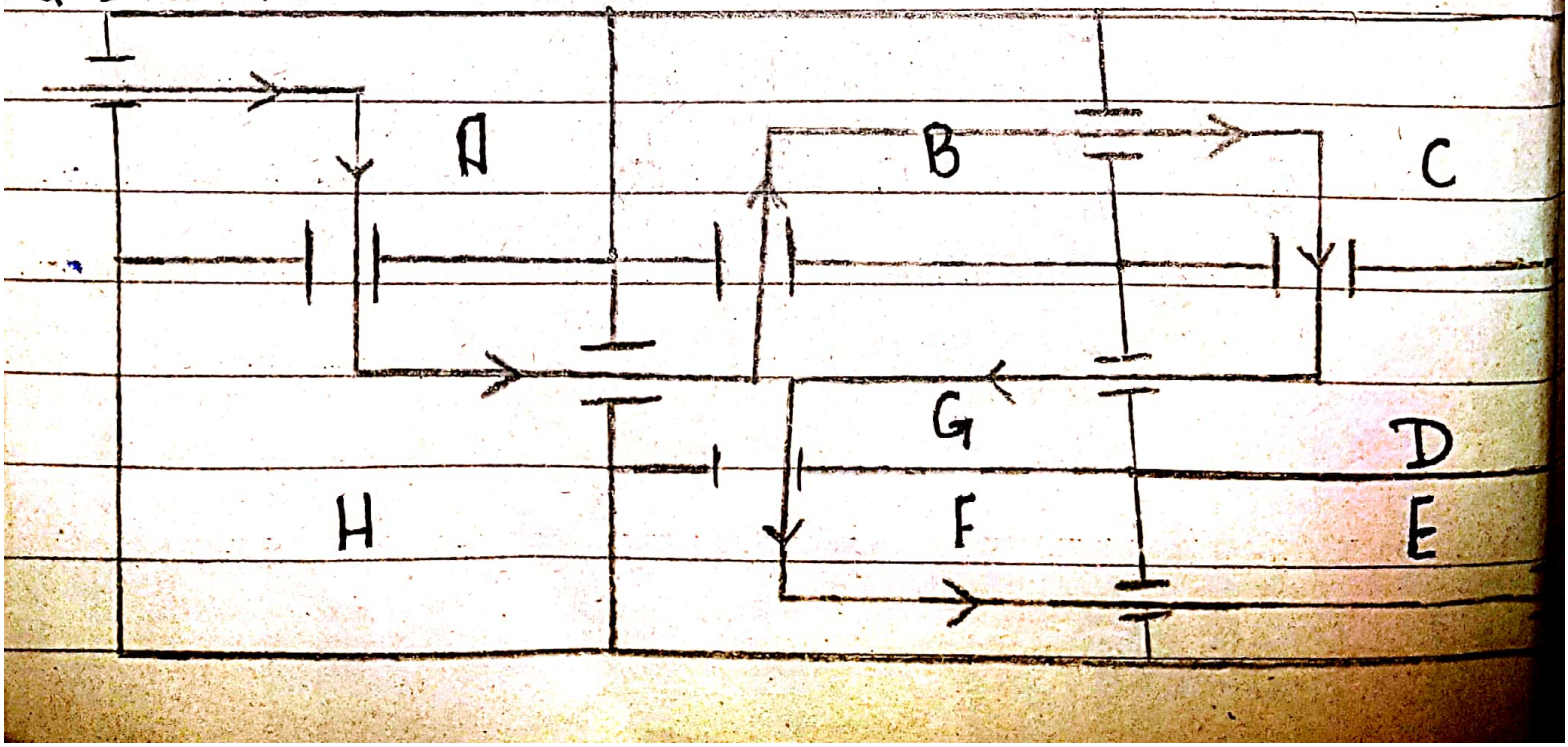
Q.33



- A → B → C → D → A = 195 km — Path 1
- A → C → D → B → A = 140 km — Path 2
- A → C → B → D → A = 155 km — Path 3

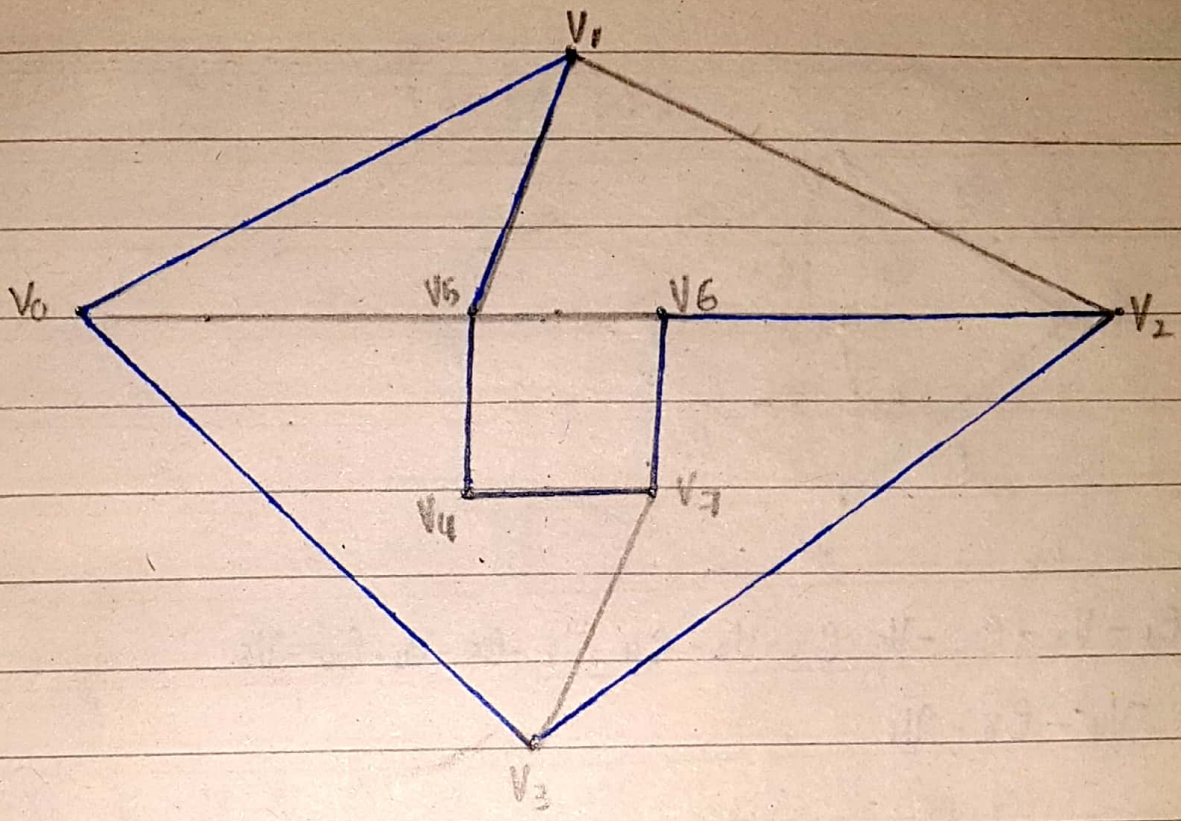
→ Path #1 is the shortest.

Q.34: A → H → B → C → D → G → F → E



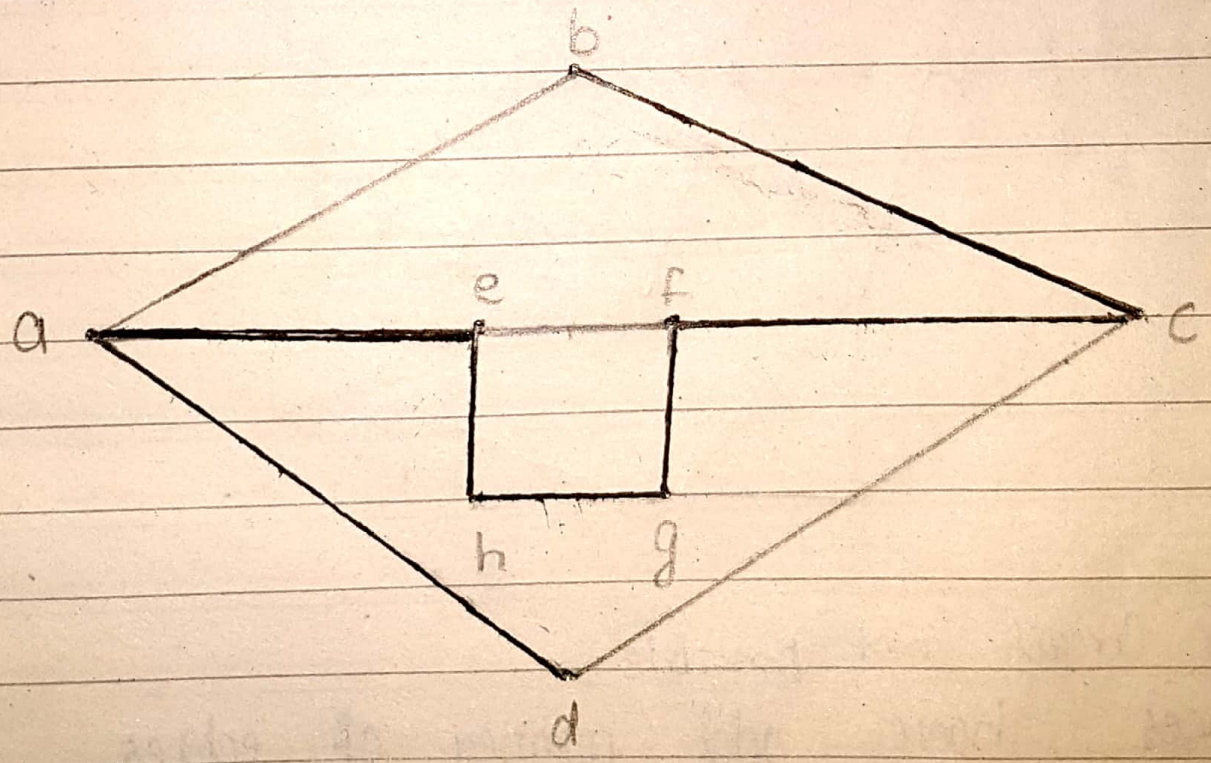
Q. 35

a)



- Circuit: $V_1 \rightarrow V_0 \rightarrow V_3 \rightarrow V_2 \rightarrow V_6 \rightarrow V_7 \rightarrow V_4 \rightarrow V_5 \rightarrow V_1$

b)

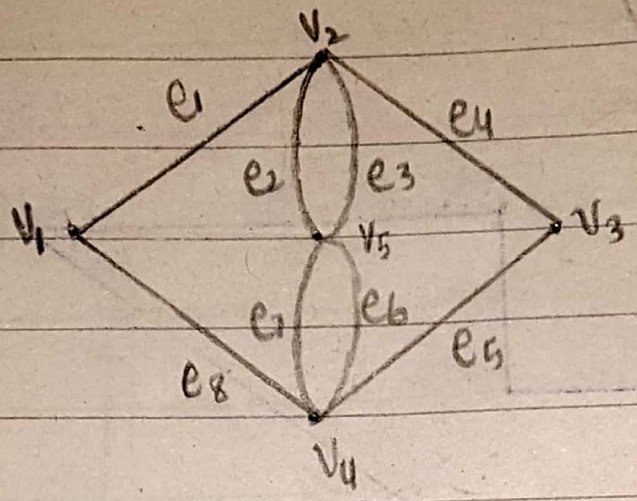


Path: $d \rightarrow a \rightarrow e \rightarrow h \rightarrow g \rightarrow f \rightarrow c \rightarrow b$

Q. 36

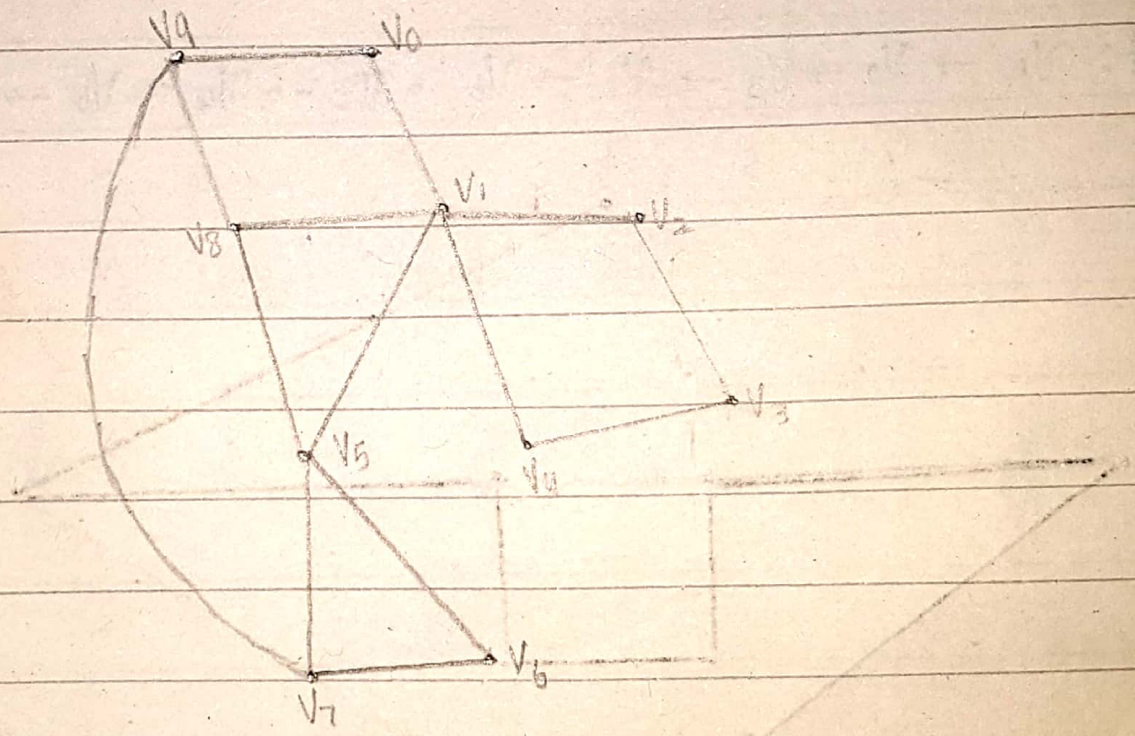
a)

i)



- $v_1 - e_1 - v_2 - e_2 - v_5 - e_3 - v_2 - e_4 - v_3 - e_5 - v_4 - e_6 - v_5 - e_7 - v_4 - e_8 - v_1$.

ii)

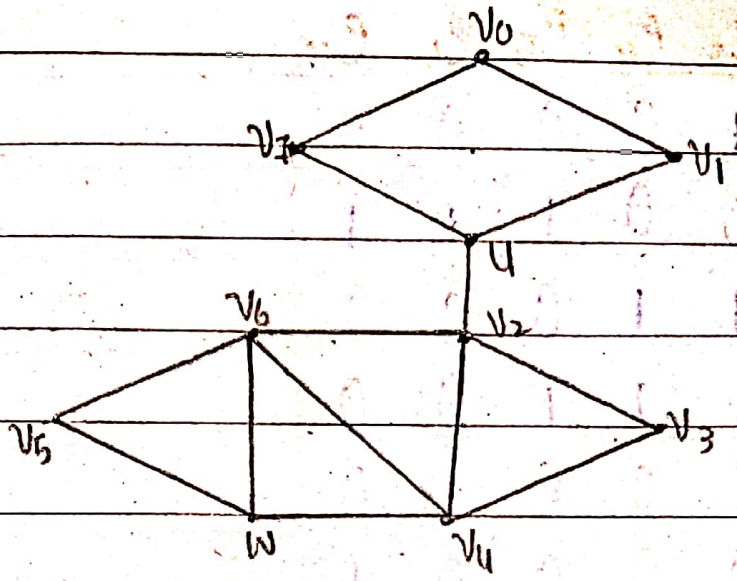


→ Euler Circuit not possible.

→ Vertices have odd number of edges.

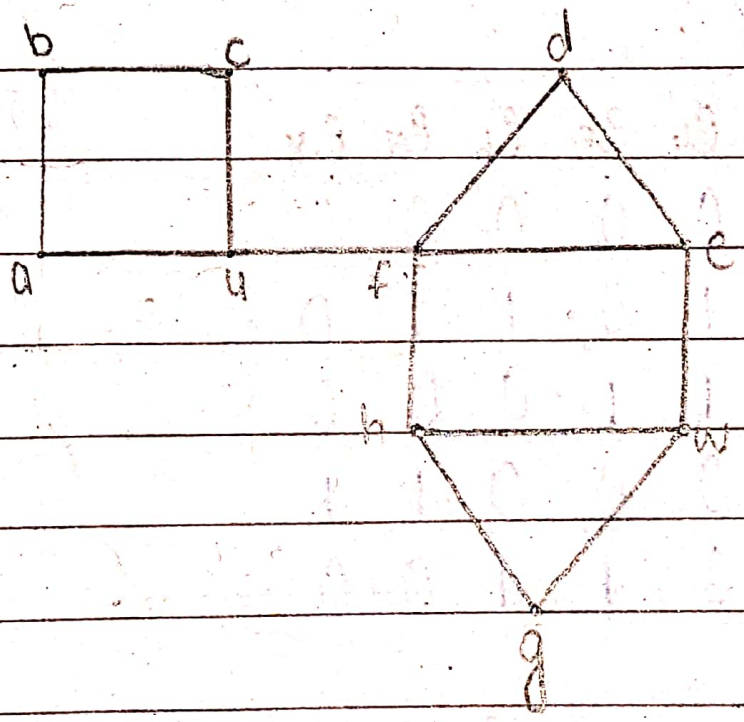
b) Euler Path (u to w)

i)



- $u - v_7 - v_0 - v_1 - u - v_2 - v_3 - v_4 - v_2 - v_6 - v_5 - w - v_6 - v_4 - w$

ii)



- More than 2 vertices with odd no of edges (u, f, e, h, w)

Q. 37

a)

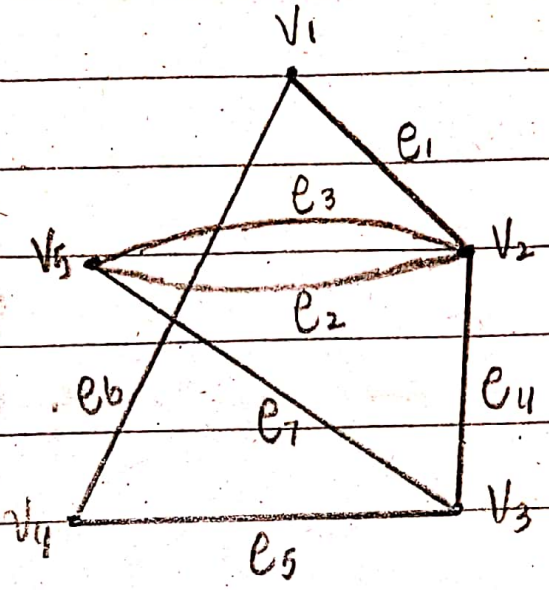
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
V_1	1	1	1	0	0	0	0
V_2	0	0	0	0	1	1	1
V_3	0	1	1	1	0	0	0
V_4	0	0	0	1	1	0	0
V_5	0	0	0	0	0	1	0
V_6	1	0	0	0	0	0	1

b)

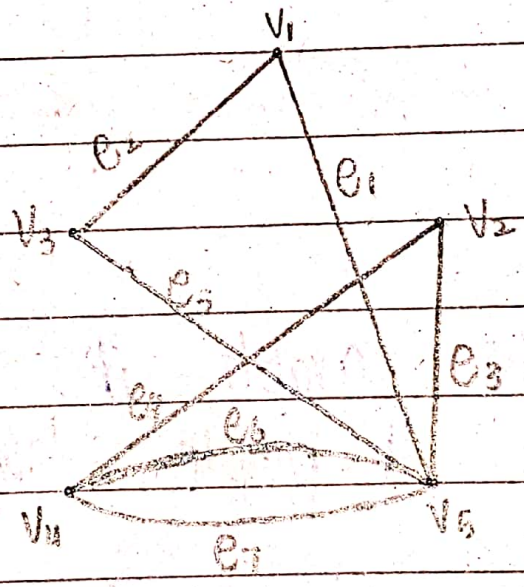
	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
V_1	1	1	1	0	0	0	0	0
V_2	0	1	1	1	0	1	1	0
V_3	0	0	0	1	1	0	0	0
V_4	0	0	0	0	0	0	1	1
V_5	0	0	0	0	1	1	0	0

Q.38

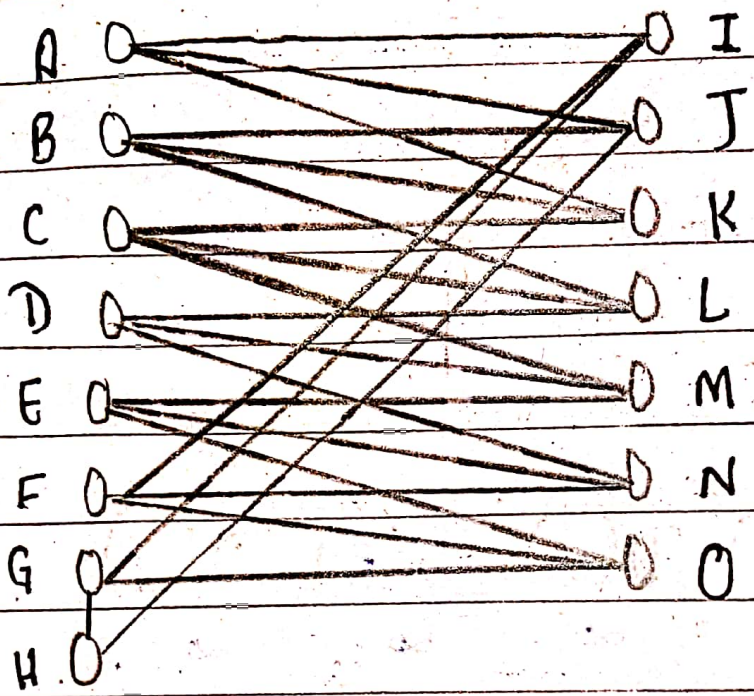
a)



b)

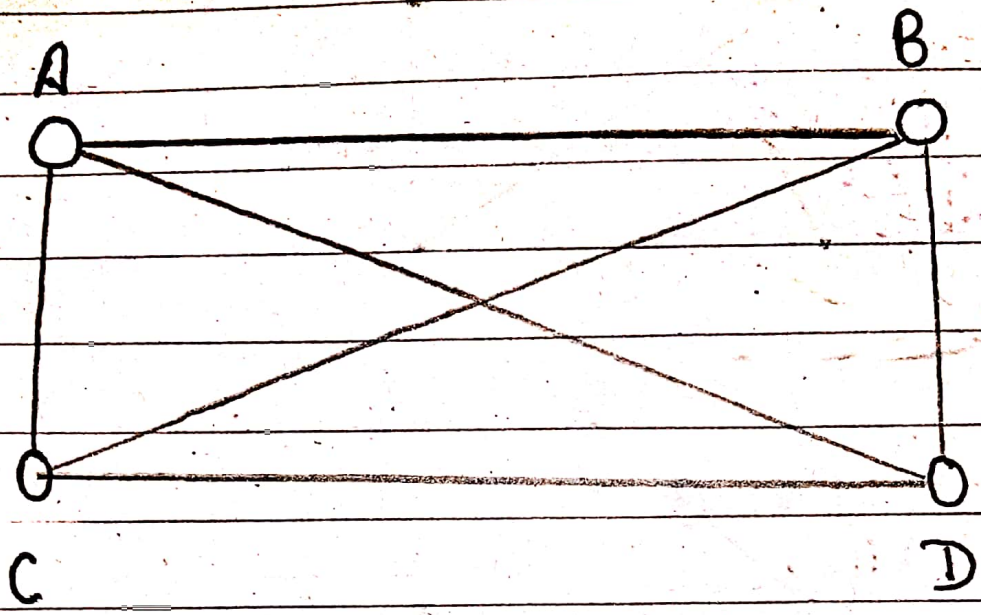


Q.39(a):



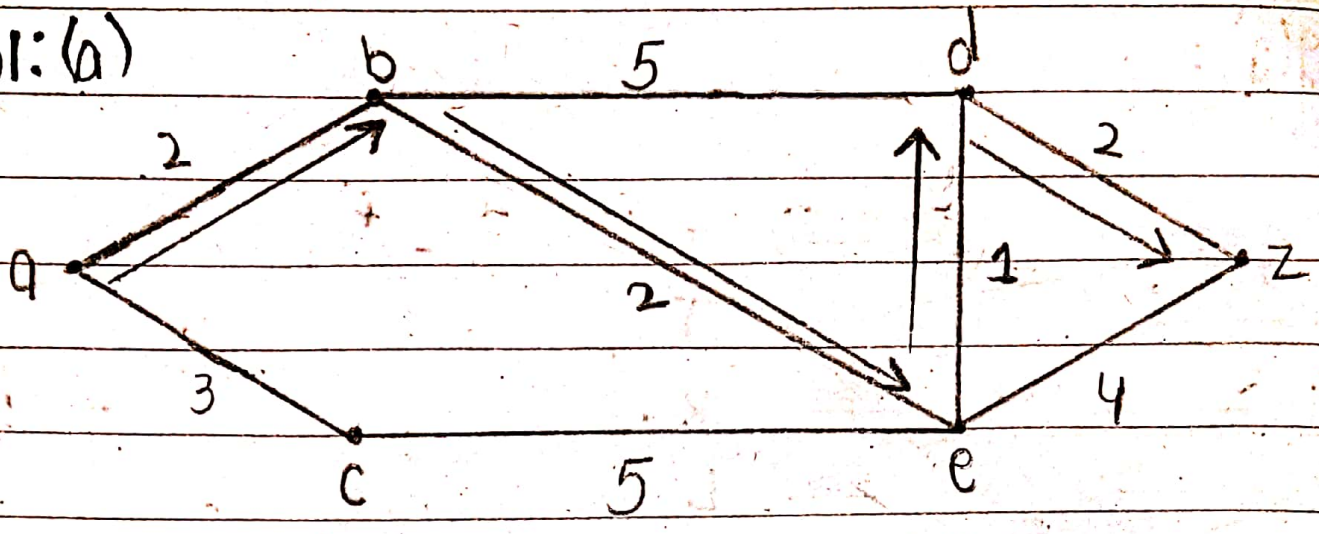
→ It is not possible for 15 people to have exactly 3 friends, as it is evident from the graph above, (H) cannot have 3 friends.

Q. 39(b)



- Looking at the graph it is evident that each of 4 people have exactly 3 friends.

Q. 31: (a)

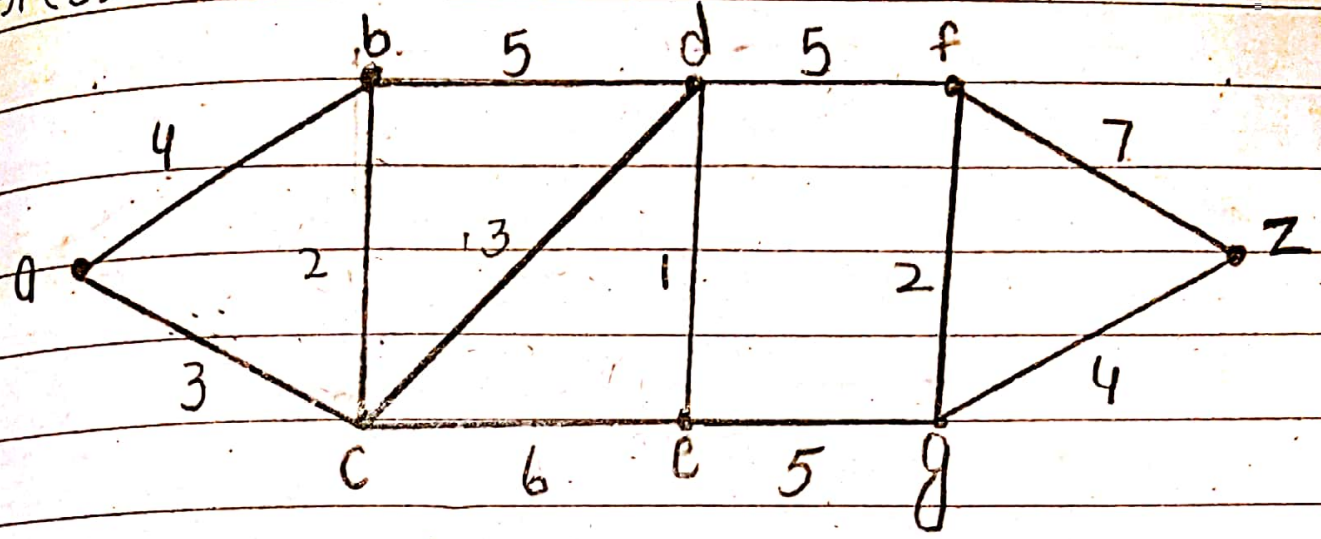


Step Num:	N'	D(b)	D(c)	D(d)	D(e)	D(z)
1	a	2,a	3,a	∞	∞	∞
2	ab			7,b	4,b	∞
3	abe			5,e		8,e
4.	abed					7,d

→ Shortest path to z is 7.

→ a, b, e, d, z ⇒ 7

Q.31(b)



Steps	N'	D(a)	D(b)	D(c)	D(d)	D(e)	D(f)	D(g)	D(z)
	a	0	~~4,a~~	~~3,a~~	∞	∞	∞	∞	∞
	ac		4,a	3,a	∞	∞	∞	∞	∞
	acb		4,a		6,c	9,c	∞	∞	∞
	acbd				6,c	9,c	∞	∞	∞
	acbde					7,d	11,d	∞	∞
	acbdef						11,d	13,e	∞
	acbdefg							13,e	18,f
									16,g

Shortest path to z is 16

0, c, d, e, g, z ⇒ 16