Assignment No. 02

Discrete Structures

Name:- Shah Hurain

Roll Number:- 23k-3032

Q1 quotient = q , Remainder = r

(a) 19 is divided by 7

$q = 2$, $r = 5$

(b) -111 is divided by 11

$q = -11$, $r = 10$

(c) 789 is divided by 23

$q = 34$, $r = 7$

(d) 1001 is divided by 13

$q = 77$, $r = 0$

(e) 10 is divided by 19

$q = 0$, $r = 10$

(f) 3 is divided by 5

$q = 0$, $r = 3$

(g) -1 is divided by 3

$q = -1$, $r = 2$

(h) 4 is divided by 1

$q = 4$, $r = 0$

Q2 $\because q = a \text{ div } m$; $r = a \bmod m$

a) (i) $a = -111$, $m = 99$

$q = -2$, $r = 87$

(ii) $a = -9999$, $m = 101$

$q = -399$, $r = 0$

(iii) $a = 10299$, $m = 999$

$q = 10$, $r = 309$

(iv) $a = 123456$, $m = 1001$

$q = 123$, $r = 333$

CamScanner

(a) $\because a \equiv b \pmod{m}$; where b is [illegible]

(i) 80

$80 \not\equiv 5 \pmod{17}$ $\quad \because b = 12$

(ii) 103

$103 \not\equiv 5 \pmod{17}$ $\quad \because b = 1$

(iii) -29

$-29 \equiv 5 \pmod{17}$ $\quad \because b = 5$

(iv) -122

$-122 \not\equiv 5 \pmod{17}$ $\quad \because b = 14$

Q3

(A)

(i) 11, 15, 19

Yes; because gcd of $(11,15)=1$, gcd $(11,19)=1$, gcd $(15,19)=1$

(ii) 14, 15, 21

No;

because gcd $(14,15)=1$, gcd $(14,21)=1$ but gcd $(15,21) = 3$

(iii) 12, 17, 31, 37

Yes;

because gcd. $(12,17)=1$, gcd. $(12,31)=1$, gcd $(12,37)=1$, gcd $(17,31)=1$

gcd $(17,37)=1$, gcd $(31,37)=1$

(iv) 7, 8, 9, 11

Yes;

because gcd $(7,8)=1$, gcd $(7,9)=1$, gcd $(7,11)=1$, gcd $(8,9)=1$, gcd $(8,11)=1$

gcd $(9,11)=1$

(b)

(i) 88

Prime Factors: $88 = 2 \times 2 \times 2 \times 11$

$= 2^3 \times 11$

(ii) 126

Prime Factors: $126 = 2 \times 3 \times 3 \times 7$

$= 2 \times 3^2 \times 7$

CamScanner

(iii) 729

Prime Factors: $729 = 3\times3\times3\times3\times3\times3$
$= 3^6$

(iv) 1001

Prime Factors: $1001 = 7\times11\times13$

(v) 1111

Prime Factors: $1111 = 11\times101$

(vi) 909

Prime Factors: $909 = 3\times3\times101$
$= 3^2\times101$

Q4

gcd (144, 89)

$144 = 89(1) + 55 \Rightarrow 55 = 144 - 89(1)$

$89 = 55(1) + 34 \Rightarrow 34 = 89 - 55(1)$

$55 = 34(1) + 21 \Rightarrow 21 = 55 - 34(1)$

$34 = 21(1) + 13 \Rightarrow 13 = 34 - 21(1)$

$21 = 13(1) + 8 \Rightarrow 8 = 21 - 13(1)$

$13 = 8(1) + 5 \Rightarrow 5 = 13 - 8(1)$

$8 = 5(1) + 3 \Rightarrow 3 = 8 - 5(1)$

$5 = 3(1) + 2 \Rightarrow 2 = 5 - 3(1)$

$3 = 2(1) + 1 \rightarrow$ gcd $\Rightarrow 1 = 3 - 2(1)$

$2 = 1(2) + 0$

Back Ward:-

$1 = 3 - 2(1)$

$1 = 3 - 1[5 - 3(1)]$

$1 = 3 - 5(1) + 3(1)$

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

$1 = 2[8 - 5(1)] - 1(5)$

$1 = 2(8) - 2(5) - 1(5)$

$1 = 2(8) - 3(5)$

$1 = 2(8) - 3[13 - 8(1)]$

$1 = 2(8) - 3(13) + 3(8)$

$1 = 5(8) - 3(13)$

$1 = 5[21 - 13(1)] - 3(13)$

$1 = 5(21) - 5(13) - 3(13)$

$1 = 5(21) - 8(13)$

$1 = 5(21) - 8[34 - 21(1)]$

$= 5(21) - 8(34) + 8(21)$

$= 13(21) - 8(34)$

$= 13[55 - 34(1)] - 8(34)$

$= 13(55) - 13(34) - 8(34)$

$= 13(55) - 21(34)$

$= 13(55) - 21[89 - 55(1)]$

$= 13(55) - 21(89) + 21(55)$

$= 34(55) - 21(89)$

$= 34[144 - 89(1)] - 21(89)$

$= 34(144) - 34(89) - 21(89)$

$= 34(144) - 55(89) \rightarrow$ linear combination

gcd (1001, 100001)

$100001 = 1001(99) + 902$ $\qquad$ $902 = 100001 - 1001(99)$

$1001 = 902(1) + 99$ $\qquad$ $99 = 1001 - 902(1)$

$902 = 99(9) + 11 \rightarrow$ gcd $\qquad$ $\Rightarrow 11 = 902 - 99(9)$

$99 = 11(9) + 0$

Backward:-

$11 = 902 - 99(9)$

$11 = 902 - 9[1001 - 902(1)]$

$11 = 902 - 9(1001) + 9(902)$

$11 = 10(902) - 9(1001)$

$11 = 10[100001 - 1001(99)] - 9(1001)$

$11 = 10(100001) - 990(1001) - 9(1001)$

$11 = 10(100001) - 999(1001) \rightarrow$ linear combination

Q5 (a) $55x \equiv 34 \pmod{89}$

gcd (55, 89)

$89 = 55(1) + 34$ $\qquad$ $\Rightarrow 34 = 89 - 55(1)$

$55 = 34(1) + 21$ $\qquad$ $\Rightarrow 21 = 55 - 34(1)$

$34 = 21(1) + 13$ $\qquad$ $\Rightarrow 13 = 34 - 21(1)$

$21 = 13(1) + 8$ $\qquad$ $\Rightarrow 8 = 21 - 13(1)$

$13 = 8(1) + 5$ $\qquad$ $\Rightarrow 5 = 13 - 8(1)$

$8 = 5(1) + 3$ $\qquad$ $\Rightarrow 3 = 8 - 5(1)$

$5 = 3(1) + 2$ $\qquad$ $\Rightarrow 2 = 5 - 3(1)$

$3 = 2(1) + 1 \rightarrow$ gcd $\qquad$ $\Rightarrow 1 = 3 - 2(1)$

$2 = 1(2) + 0$

Backward:-

$1 = 3 - 2(1)$

$1 = 3 - 1[5 - 3(1)]$

$1 = 3 - 1(5) + 1(3)$

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

$1 = 2[8 - 5(1)] - 1(5)$

$1 = 2(8) - 2(5) - 1(5)$

$1 = 2(8) - 3(5)$

$1 = 2(8) - 3[13 - 8(1)]$

$1 = 2(8) - 3(13) + 3(8)$

$1 = 5(8) - 3(13)$

CamScanner

$1 = 5(8) - 3(13)$

$1 = 5[21 - 13(1)] - 3(13)$

$1 = 5(21) - 5(13) - 3(13)$

$1 = 5(21) - 8(13)$

$1 = 5(21) - 8[37 - 21(1)]$

$1 = 5(21) - 8(37) + 8(21)$

$1 = 13(21) - 8(37)$

$1 = 13[55 - 37(1)] - 8(37)$

$1 = 13(55) - 13(37) - 8(37)$

$1 = 13(55) - 21(37)$

$1 = 13(55) - 21[89 - 55(1)]$

$1 = 13(55) - 21(89) + 21(55)$

$1 = 34(55) - 21(89)$

Inverse :-

So, inverse $= 34$

Multiplying 34 on both sides, we get

$(55)(34)x = (34)(34) \bmod 89$

$x = 1156 \bmod 89$

$\boxed{x = 88}$

(b) $89x \equiv 2 \pmod{232}$

gcd $(89, 232)$

$232 = 89(2) + 57 \quad \Rightarrow 57 = 232 - 89(2)$

$89 = 57(1) + 35 \quad \Rightarrow 35 = 89 - 57(1)$

$57 = 35(1) + 19 \quad \Rightarrow 19 = 57 - 35(1)$

$35 = 19(1) + 16 \quad \Rightarrow 16 = 35 - 19(1)$

$19 = 16(1) + 3 \quad \Rightarrow 3 = 19 - 16(1)$

$16 = 3(5) + 1 \rightarrow$ gcd $\quad \Rightarrow 1 = 16 - 3(5)$

$3 = 1(3) + 0$

Backinned :-

$1 = 16 - 3(5)$

$= 16 - 5[19 - 16(1)]$

$= 16 - 5(19) + 5(16)$

$= 6(16) - 5(19)$

$= 6[35 - 19(1)] - 5(19)$

$= 6(35) - 6(19) - 5(19)$

$= 6(35) - 11(19)$

$1 = 6(35) - 11(19)$

$1 = 6(35) - 11[57 - 35(1)]$

$1 = 6(35) - 11(57) + 11(35)$

$1 = 17(35) - 11(57)$

$1 = 17[89 - 57(1)] - 11(57)$

$1 = 17(89) - 17(57) - 11(57)$

$1 = 17(89) - 28(57)$

$1 = 17(89) - 28[232 - 89(2)]$

$1 = 17(89) - 28(232) + 56(89)$

$1 = 73(89) - 28(232)$ → linear combination

Inverse:-

so, inverse is '73'

Multiplying '73' on both sides

$(89)(73)x = (2)(73) \bmod 232$

$x = 146 \bmod 232$

$\boxed{x = 146}$

Q6

Q) (i) $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$ and $x \equiv 3 \pmod 7$

$a_1 = 1$, $m_1 = 5$

$a_2 = 2$, $m_2 = 6$

$a_3 = 3$, $m_3 = 7$

$M = (m_1)(m_2)(m_3)$

$= (5)(6)(7)$

$M = 210$

$M_1 = \frac{M}{m_1} = \frac{210}{5} = 42$

$M_2 = \frac{M}{m_2} = \frac{210}{6} = 35$

$M_3 = \frac{M}{m_3} = \frac{210}{7} = 30$

For inverses:-

$M_1 M_1^{-1} \equiv 1 \pmod 5$; $M_2 M_2^{-1} \equiv 1 \pmod 6$; $M_3 M_3^{-1} \equiv 1 \pmod 7$

$(42) M_1^{-1} \equiv 1 \pmod 5$; $(35) M_2^{-1} \equiv 1 \pmod 6$; $(30) M_3^{-1} \equiv 1 \pmod 7$

$\boxed{M_1^{-1} = 3}$; $\boxed{M_2^{-1} = 5}$; $\boxed{M_3^{-1} = 4}$

CamScanner

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

$= [(1)(42)(3) + (2)(35)(5) + (3)(30)(7)] \bmod 210$

$= 836 \bmod 210$

$\boxed{x = 206}$

(ii) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$

$a_1 = 1$, $m_1 = 2$

$a_2 = 2$, $m_2 = 3$

$a_3 = 3$, $m_3 = 5$

$a_4 = 4$, $m_4 = 11$

$M = (m_1)(m_2)(m_3)$

$= (2)(3)(5)(11)$

$M = 330$

Now;

$M_1 = \frac{M}{m_1} = \frac{330}{2} = 165 = 165$

$M_2 = \frac{M}{m_2} = \frac{330}{3} = 110 = 110$ $\quad M_3 = \frac{M}{m_3} = \frac{330}{5} = 66$

$M_4 = \frac{M}{m_3} = \frac{330}{11} = 30$

For inverse:

$M_1 M_1^{-1} \equiv 1 \pmod 2$; $M_2 M_2^{-1} \equiv 1 \pmod 3$; $M_3 M_3^{-1} \equiv 1 \pmod 5$

$(165) M_1^{-1} \equiv 1 \pmod 2$; $(110) M_2^{-1} \equiv 1 \pmod 3$; $(66) M_3^{-1} \equiv 1 \pmod 5$

$\boxed{M_1^{-1} = 1}$; $\boxed{M_2^{-1} = 2}$; $\boxed{M_3^{-1} = 1}$

$M_4 M_4^{-1} \equiv 1 \pmod{11}$

$(30) M_4^{-1} \equiv 1 \pmod{11}$

$\boxed{M_4^{-1} = 7}$

$\because x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1}) \bmod M$

$= [(1)(165)(1) + (2)(110)(2) + (3)(66)(1) + (4)(30)(7)] \bmod 330$

$= 1643 \bmod 330$

$\boxed{x = 323}$

CamScanner

(5)

$x \equiv 3 \pmod 5$

$x \equiv 3 \pmod 6$

$x \equiv 1 \pmod 7$

$x \equiv 0 \pmod{11}$

$a_1 = 3 \quad ; m_1 = 5$

$a_2 = 3 \quad ; m_2 = 6$

$a_3 = 1 \quad ; m_3 = 7$

$a_4 = 0 \quad ; m_4 = 11$

$M = (m_1)(m_2)(m_3)(m_4)$

$= (5)(6)(7)(11)$

$\boxed{M = 2310}$

Now;

$M_1 = \frac{M}{m_1} = \frac{2310}{5} = 462$

$M_2 = \frac{M}{m_2} = \frac{2310}{6} = 385$

$M_3 = \frac{M}{m_3} = \frac{2310}{7} = 330$

$M_4 = \frac{M}{m_4} = \frac{2310}{11} = 210$

For Inverses:

$M_1 M_1^{-1} \equiv 1 \pmod 5$; $M_2 M_2^{-1} \equiv 1 \pmod 6$; $M_3 M_3^{-1} \equiv 1 \pmod 7$; $M_4 M_4^{-1} \equiv 1 \pmod{11}$

$(462) M_1^{-1} \equiv 1 \pmod 5$; $(385) M_2^{-1} \equiv 1 \pmod 6$; $(330) M_3^{-1} \equiv 1 \pmod 7$; $(210) M_4^{-1} \equiv 1 \pmod{11}$

$\boxed{M_1^{-1} = 3}$; $\boxed{M_2^{-1} = 1}$; $\boxed{M_3^{-1} = 1}$; $\boxed{M_4^{-1} = 1}$

$\because x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1}) \bmod M$

$= [(3)(462)(3) + (3)(385)(1) + (1)(330)(1) + (0)(210)(1)] \bmod 2310$

$= 1023 \bmod 2310$

$\boxed{x = 1023}$

Hamed

Q7

(a) $a = 2$, $m = 17$

gcd $(2, 17)$

$17 = 2(8) + 1$ → gcd

$2 = 1(2) + 0$

Backward;

$1 = 17 - 2(8)$

$1 = 1(17) - 8(2)$

Inverse is $-8 \Rightarrow -8 + 17 = \boxed{9}$

(b) $a = 37$, $m = 89$

gcd $(37, 89)$

$89 = 37(2) + 21$ $\Rightarrow 21 = 89 - 37(2)$

$37 = 21(1) + 13$ $\Rightarrow 13 = 37 - 21(1)$

$21 = 13(1) + 8$ $\Rightarrow 8 = 21 - 13(1)$

$13 = 8(1) + 5$ $\Rightarrow 5 = 13 - 8(1)$

$8 = 5(1) + 3$ $\Rightarrow 3 = 8 - 5(1)$

$5 = 3(1) + 2$ $\Rightarrow 2 = 5 - 3(1)$

$3 = 2(1) + 1$ → gcd $\Rightarrow 1 = 3 - 2(1)$

$2 = 1(2) + 0$

Backward;

$1 = 3 - 2(1)$

$1 = 3 - 1[5 - 3(1)]$

$1 = 3 - 1(5) + 1(3)$

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

$1 = 2[8 - 5(1)] - 1(5)$

$1 = 2(8) - 2(5) - 1(5)$

$1 = 2(8) - 3(5)$

$1 = 2(8) - 3[13 - 8(1)]$

$1 = 2(8) - 3(13) + 3(8)$

$1 = 5(8) - 3(13)$

$1 = 5[21 - 13(1)] - 3(13)$

$1 = 5(21) - 5(13) - 3(13)$

$1 = 5(21) - 8(13)$

$1 = 5(21) - 8[37 - 21(1)]$

$1 = 5(21) - 8(37) + 8(21)$

$1 = 13(21) - 8(37)$

$1 = 13[89 - 37(2)] - 8(37)$

$1 = 13(89) - 26(37) - 8(37)$

$1 = 13(89) - 34(37)$

Inverse is $-34 \Rightarrow -34 + 89$

$\boxed{= 55}$

CamScanner

(c) $a = 147$, $m = 233$

$\gcd(147, 233)$

$233 = 147(1) + 89$ $\Rightarrow 89 = 233 - 147(1)$

$147 = 89(1) + 55$ $\Rightarrow 55 = 147 - 89(1)$

$89 = 55(1) + 34$ $\Rightarrow 34 = 89 - 55(1)$

$55 = 34(1) + 21$ $\Rightarrow 21 = 55 - 34(1)$

$34 = 21(1) + 13$ $\Rightarrow 13 = 34 - 21(1)$

$21 = 13(1) + 8$ $\Rightarrow 8 = 21 - 13(1)$

$13 = 8(1) + 5$ $\Rightarrow 5 = 13 - 8(1)$

$8 = 5(1) + 3$ $\Rightarrow 3 = 8 - 5(1)$

$5 = 3(1) + 2$ $\Rightarrow 2 = 5 - 3(1)$

$3 = 2(1) + 1$ $\rightarrow$ gcd $\Rightarrow 1 = 3 - 2(1)$

$2 = 1(2) + 0$

<u>Backward</u>:

$1 = 3 - 2(1)$

$= 3 - 1[5 - 3(1)]$

$= 3 - 1(5) + 3(1)$

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

$= 2[8 - 5(1)] - 1(5)$

$= 2(8) - 2(5) - 1(5)$

$= 2(8) - 3(5)$

$= 2(8) - 3[13 - 8(1)]$

$= 2(8) - 3(13) + 3(8)$

$= 5(8) - 3(13)$

$= 5[21 - 13(1)] - 3(13)$

$= 5(21) - 5(13) - 3(13)$

$= 5(21) - 8(13)$

$= 5(21) - 8[34 - 21(1)]$

$= 5(21) - 8(34) + 8(21)$

$= 13(21) - 8(34)$

$= 13[55 - 34(1)] - 8(34)$

$= 13(55) - 13(34) - 8(34)$

$= 13(55) - 21(34)$

$= 13(55) - 21[89 - 55(1)]$

$= 13(55) - 21(89) + 21(55)$

$= 34(55) - 21(89)$

$= 34[147 - 89(1)] - 21(89)$

$= 34(147) - 34(89) - 21(89)$

$1 = 34(147) - 55(89)$

$= 34(147) - 55[233 - 147(1)]$

$= 34(147) - 55(233) + 55(147)$

$= 89(147) - 55(233)$

Inverse is $\boxed{89}$

(d) $A = 200$, $m = 1001$

gcd (200, 1001)

$1001 = 200(5) + 1 \rightarrow$ gcd

$200 = 1(200) + 0$

Backward;

$1 = 1001 - 200(5)$

$1 = 1(1001) - 5(200)$

Inverse is $-5 \Rightarrow -5 + 1001$

$\boxed{= 996}$

Q8

(a) ~~STOP Pollution~~

STOP POLLUTION

(i) $f(p) = (p+7) \bmod 26$

$f(S) = (18+7) \bmod 26 = 22 \bmod 26 = 22$

$f(T) = (19+7) \bmod 26 = 23 \bmod 26 = 23$

$f(O) = (14+7) \bmod 26 = 18 \bmod 26 = 18$

$f(P) = (15+7) \bmod 26 = 19 \bmod 26 = 19$

$f(L) = (11+7) \bmod 26 = 15 \bmod 26 = 15$

$f(U) = (20+7) \bmod 26 = 27 \bmod 26 = 27$

$f(I) = (8+7) \bmod 26 = 12 \bmod 26 = 12$

$f(N) = (13+7) \bmod 26 = 17 \bmod 26 = 17$

Encrypt Message:-

WXST TSPPYXMSR

(ii) $f(p) = (p+21) \bmod 26$

$f(S) = (18+21) \bmod 26 = 39 \bmod 26 = 13$

$f(T) = (19+21) \bmod 26 = 40 \bmod 26 = 14$

$f(O) = (14+21) \bmod 26 = 35 \bmod 26 = 9$

$f(P) = (15+21) \bmod 26 = 36 \bmod 26 = 10$

$f(L) = (11+21) \bmod 26 = 32 \bmod 26 = 6$

$f(U) = (20+21) \bmod 26 = 41 \bmod 26 = 15$

CamScanner

$f(I) = (8+21) \bmod 26 = 29 \bmod 26 = 3$

$f(N) = (13+21) \bmod 26 = 34 \bmod 26 = 8$

Encrypted Message:-

NDJK KJGGPDDJI

(b) $f(p) = (p+10) \bmod 26$

(i) CEBBOXNOBXYG

$f^{-1}(C) = (2-10) \bmod 26 = -8 \bmod 26 = 18$

$f^{-1}(E) = (4-10) \bmod 26 = -6 \bmod 26 = 20$

$f^{-1}(B) = (1-10) \bmod 26 = -9 \bmod 26 = 17$

$f^{-1}(O) = (14-10) \bmod 26 = 4 \bmod 26 = 4$

$f^{-1}(X) = (23-10) \bmod 26 = 13 \bmod 26 = 13$

$f^{-1}(N) = (13-10) \bmod 26 = 3 \bmod 26 = 3$

$f^{-1}(Y) = (24-10) \bmod 26 = 14 \bmod 26 = 14$

$f^{-1}(G) = (6-10) \bmod 26 = -4 \bmod 26 = 22$

Decrypted Message:-

SURRENDER NOW

(ii) LDWI PBSDXN

$f^{-1}(L) = (11-10) \bmod 26 = 1 \bmod 26 = 1$

$f^{-1}(D) = (14-10) \bmod 26 = 4 \bmod 26 = 4$

$f^{-1}(W) = (22-10) \bmod 26 = 12 \bmod 26 = 12$

$f^{-1}(I) = (8-10) \bmod 26 = -2 \bmod 26 = 24$

$f^{-1}(P) = (15-10) \bmod 26 = 5 \bmod 26 = 5$

$f^{-1}(B) = (1-10) \bmod 26 = -9 \bmod 26 = 17$

$f^{-1}(S) = (18-10) \bmod 26 = 8 \bmod 26 = 8$

$f^{-1}(X) = (23-10) \bmod 26 = 13 \bmod 26 = 13$

$f^{-1}(N) = (13-10) \bmod 26 = 3 \bmod 26 = 3$

Decrypted Message:-

BE MY FRIEND

CamScanner

Q7

(i) $5^{2003} \bmod 7$

$5^1 \bmod 7 = 5$

~~$5^2 \bmod 7 = 25 \bmod 7 = 4$~~

~~$5^4 \bmod 7 = 625 \bmod 7 = 2$~~

~~$5^8 \bmod 7 = 390625 \bmod 7 = 4$~~

$5^2 \bmod 7 = (5)^2 \bmod 7 = 7$

$5^4 \bmod 7 = (4)^2 \bmod 7 = 2$

$5^8 \bmod 7 = (2)^2 \bmod 7 = 4$

$5^{16} \bmod 7 = (4)^2 \bmod 7 = 2$

$5^{32} \bmod 7 = (2)^2 \bmod 7 = 4$

$5^{64} \bmod 7 = (4)^2 \bmod 7 = 2$

$5^{128} \bmod 7 = (2)^2 \bmod 7 = 4$

$5^{256} \bmod 7 = (4)^2 \bmod 7 = 2$

$5^{512} \bmod 7 = (2)^2 \bmod 7 = 4$

$5^{1027} \bmod 7 = (4)^2 \bmod 7 = 2$

$2003 = 1027 + 512 + 252 + 128 + 64 + 16 + 2 + 1$

$(5^{1027} \cdot 5^{512} \cdot 5^{256} \cdot 5^{128} \cdot 5^{64} \cdot 5^{16} \cdot 5^{2} \cdot 5^{1}) \bmod 7$

$(2 \cdot 4 \cdot 2 \cdot 4 \cdot 2 \cdot 2 \cdot 4 \cdot 5) \bmod 7$

$= 5120 \bmod 7$

$\boxed{= 3}$

(ii) $5^{2003} \bmod 11$

$5^1 \bmod 11 = 5$

$5^2 \bmod 11 = 25 \bmod 11 = 3$

$5^4 \bmod 11 = (3)^2 \bmod 11 = 9$

$5^8 \bmod 11 = (9)^2 \bmod 11 = 4$

$5^{16} \bmod 11 = (4)^2 \bmod 11 = 5$

$5^{32} \bmod 11 = (5)^2 \bmod 11 = 3$

$5^{64} \bmod 11 = (3)^2 \bmod 11 = 9$

$5^{128} \bmod 11 = (9)^2 \bmod 11 = 4$

$5^{256} \bmod 11 = (4)^2 \bmod 11 = 5$

CamScanner

$5^{512} \bmod 11 = (5)^2 \bmod 11 = 3$

$5^{1024} \bmod 11 = (3)^2 \bmod 11 = 9$

$= (5^{1024} \cdot 5^{512} \cdot 5^{256} \cdot 5^{128} \cdot 5^{64} \cdot 5^{16} \cdot 5^{2} \cdot 5^{1}) \bmod 11$

$= (9 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 5 \cdot 3 \cdot 5) \bmod 11$

$= 364500 \bmod 11$

$\boxed{= 7}$

(iii) $5^{2003} \bmod 13$

$5^{1} \bmod 13 = 5$

$5^{2} \bmod 13 = (5)^2 \bmod 13 = 12$

$5^{4} \bmod 13 = (12)^2 \bmod 13 = 1$

$5^{8} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{16} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{32} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{64} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{128} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{256} \bmod 13 = (1)^2 \bmod 13 = 1$

$2^{512} \bmod 13 = (1)^2 \bmod 13 = 1$

$5^{1024} \bmod 13 = (1)^2 \bmod 13 = 1$

$= (5^{1024} \cdot 5^{512} \cdot 5^{256} \cdot 5^{128} \cdot 5^{64} \cdot 5^{16} \cdot 5^{2} \cdot 5^{1}) \bmod 13$

$= (1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 12 \cdot 5) \bmod 13$

$= 60 \bmod 13$

$\boxed{= 8}$

CamScanner

Q10

(a) I LOVE DISCRETE MATHEMATICS

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

$f(L) = (11+3) \bmod 26 = 14 \bmod 26 = 14$

$f(O) = (14+3) \bmod 26 = 17 \bmod 26 = 17$

$f(V) = (21+3) \bmod 26 = 24 \bmod 26 = 24$

$f(E) = (4+3) \bmod 26 = 7 \bmod 26 = 7$

$f(D) = (3+3) \bmod 26 = 6 \bmod 26 = 6$

$f(I) = (18+3) \bmod 26 = 21 \bmod 26 = 21$

$f(C) = (2+3) \bmod 26 = 5 \bmod 26 = 5$

$f(R) = (17+3) \bmod 26 = 20 \bmod 26 = 20$

$f(T) = (19+3) \bmod 26 = 22 \bmod 26 = 22$

$f(M) = (12+3) \bmod 26 = 15 \bmod 26 = 15$

$f(A) = (0+3) \bmod 26 = 3 \bmod 26 = 3$

$f(H) = (7+3) \bmod 26 = 10 \bmod 26 = 10$

Encrypted Message:-

L ORYH GLVFUHWH PDWKHPDWLFV

(b) (i) PLG WZR DYVLJQPHQW

$f^{-1}(P) = (15-3) \bmod 26 = 12 \bmod 26 = 12$

$f^{-1}(L) = (11-3) \bmod 26 = 8 \bmod 26 = 8$

$f^{-1}(G) = (6-3) \bmod 26 = 3 \bmod 26 = 3$

$f^{-1}(W) = (22-3) \bmod 26 = 19 \bmod 26 = 19$

$f^{-1}(Z) = (25-3) \bmod 26 = 22 \bmod 26 = 22$

$f^{-1}(R) = (17-3) \bmod 26 = 14 \bmod 26 = 14$

$f^{-1}(D) = (3-3) \bmod 26 = 0 \bmod 26 = 0$

$f^{-1}(V) = (21-3) \bmod 26 = 18 \bmod 26 = 18$

$f^{-1}(J) = (9-3) \bmod 26 = 6 \bmod 26 = 6$

$f^{-1}(Q) = (16-3) \bmod 26 = 13 \bmod 26 = 13$

$f^{-1}(H) = (7-3) \bmod 26 = 4 \bmod 26 = 4$

Decrypted Message:-

MID SEM ASSIGNMENT

CamScanner

(ii) IDVW DXFHV XDLYHUVLWB

$f^{-1}(I) = (8-3) \bmod 26 = 5 \bmod 26 = 5$

$f^{-1}(D) = (3-3) \bmod 26 = 0 \bmod 26 = 0$

$f^{-1}(V) = (21-3) \bmod 26 = 18 \bmod 26 = 18$

$f^{-1}(W) = (22-3) \bmod 26 = 19 \bmod 26 = 19$

$f^{-1}(Q) = (16-3) \bmod 26 = 13 \bmod 26 = 13$

$f^{-1}(X) = (23-3) \bmod 26 = 20 \bmod 26 = 20$

$f^{-1}(F) = (5-3) \bmod 26 = 2 \bmod 26 = 2$

$f^{-1}(H) = (7-3) \bmod 26 = 4 \bmod 26 = 4$

$f^{-1}(L) = (11-3) \bmod 26 = 8 \bmod 26 = 8$

$f^{-1}(Y) = (24-3) \bmod 26 = 21 \bmod 26 = 21$

$f^{-1}(U) = (20-3) \bmod 26 = 17 \bmod 26 = 17$

$f^{-1}(B) = (1-3) \bmod 26 = -2 \bmod 26 = 24$

<u>Decrypted Message:-</u>

FAST NUCES UNIVERSITY

CamScanner

Q11 (a)

$h(k) = k \bmod 97$

(i) 034567981

$h(034567981) = 034567981 \bmod 97$

$\boxed{= 91}$

(ii) 183211232

$h(183211232) = 183211232 \bmod 97$

$\boxed{= 57}$

(iii) 220195744

$h(220195744) = 220195744 \bmod 97$

$\boxed{= 21}$

(iv) 987255335

$h(987255335) = 987255335 \bmod 97$

$\boxed{= 5}$

(b) $h(k) = k \bmod 101$

(i) 104578690

$h(104578690) = 104578690 \bmod 101$

$\boxed{= 58}$

(ii) 732222187

$h(732222187) = 732222187 \bmod 101$

$\boxed{= 60}$

(iii) 372201919

$h(372201919) = 372201919 \bmod 101$

$\boxed{= 57}$

(iv) 501338753

$h(501338753) = 501338753 \bmod 101$

$\boxed{= 3}$

CamScanner

Q12

$x_{n+1} = (4x_n + 1) \bmod 7 \quad , x_0 = 3$

$x_1 = [4(3)+1] \bmod 7 = 13 \bmod 7 = 6$

$x_2 = [4(6)+1] \bmod 7 = 25 \bmod 7 = 4$

$x_3 = [4(4)+1] \bmod 7 = 17 \bmod 7 = 3$

$x_4 = [4(3)+1] \bmod 7 = 13 \bmod 7 = 6$

$x_5 = [4(6)+1] \bmod 7 = 25 \bmod 7 = 4$

$x_6 = [4(4)+1] \bmod 7 = 17 \bmod 7 = 3$

$x_7 = [4(3)+1] \bmod 7 = 13 \bmod 7 = 6$

$x_8 = [4(6)+1] \bmod 7 = 25 \bmod 7 = 4$

$x_9 = [4(4)+1] \bmod 7 = 17 \bmod 7 = 3$

$x_{10} = [4(3)+1] \bmod 7 = 13 \bmod 7 = 6$

$x_{11} = [4(6)+1] \bmod 7 = 25 \bmod 7 = 4$

$x_{12} = [4(4)+1] \bmod 7 = 17 \bmod 7 = 3$

$x_{13} = [4(3)+1] \bmod 7 = 6$

$x_{14} = [4(6)+1] \bmod 7 = 4$

$x_{15} = [4(4)+1] \bmod 7 = 3$

$x_{16} = [4(3)+1] \bmod 7 = 6$

$x_{17} = [4(6)+1] \bmod 7 = 4$

$x_{18} = [4(4)+1] \bmod 7 = 3$

$x_{19} = [4(3)+1] \bmod 7 = 6$

$x_{20} = [4(6)+1] \bmod 7 = 4$

Q13

(a) (i) 73232187437

$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$

$3(7) + 3 + 3(2) + 3 + 3(2) + 1 + 3(8) + 7 + 3(7) + 3 + 3(4) + x_{12} \equiv 0 \pmod{10}$

$95 + x_{12} \equiv 0 \pmod{10}$

$95 + 5 \equiv 0 \pmod{10}$

$100 \equiv 0 \pmod{10}$

$\boxed{x_{12} = 5}$ is the check digit

(ii) 636239913 46

$3(6) + 3 + 3(6) + 2 + 3(3) + 9 + 3(9) + 1 + 3(3) + 7 + 3(4) + x_{12} \equiv 0 \pmod{10}$

$118 + x_{12} \equiv 0 \pmod{10}$

$\boxed{x_{12} = 2}$ is the check digit.

CamScanner

(b)

(i) 0360000291452

$3(0)+3+3(6)+0+3(0)+0+3(2)+9+3(1)+4+3(5)+2 \equiv 0 \pmod{10}$

$60 \equiv 0 \pmod{10}$

$\boxed{\text{valid}}$

(ii) 0123456789 03

$3(0)+1+3(2)+3+3(4)+5+3(6)+7+3(8)+9+3(0)+3 \equiv 0 \pmod{10}$

$88 \not\equiv 0 \pmod{10}$

$\boxed{\text{invalid}}$

1.4

(a) 0-07-119881

$\because x_1+2x_2+3x_3+4x_4+5x_5+6x_6+7x_7+8x_8+9x_9+10x_{10} \equiv 0 \pmod{11}$

$0+2(0)+3(7)+4(1)+5(1)+6(9)+7(8)+8(8)+9(1)+x_{10} \equiv 0 \pmod{11}$

$213+x_{10} \equiv 0 \pmod{11}$

$\boxed{x_{10}=7}$

is the check digit

(b) 0-321-50021-8

$0+2(3)+3(2)+4(1)+5(5)+6(0)+7(0)+8(2)+9(1)+10(8) \equiv 0 \pmod{11}$

$82+130 \equiv 0 \pmod{11}$

$8(3)+130 \equiv 0 \pmod{11}$

$154 \equiv 0 \pmod{11}$

Thus;

$\boxed{2=3}$

CamScanner

Q15 ATTACK

$n = 43 \cdot 59$

$e = 13$

A	T	T	A	C	K
00	19	19	00	02	10

$n = \overset{p}{43} \cdot \overset{q}{59} = 2537$

$k = (p-1)(q-1)$

$k = (43-1)(59-1)$

$k = (42)(58) = 2436$

$\because c = M^e \bmod n$

Make group up four digits

$c = 0019^{13} \bmod 2537 = 2299$

$c = 1900^{13} \bmod 2537 = 1317$

$c = 0210^{13} \bmod 2537 = 2117$

2299 1317 2117

d16

(a) floors = 27

offices on each = 37

No. of office in building = (27)(37) = $\boxed{999}$

(b) colors = 12

version = 2

sizes = 3

types of shirts = (12)(2)(3) = $\boxed{72}$

d17

(a)

26	26	26

$= 26^3$

Different three letter initials $= 26^3 = \boxed{17576}$

(b)

26	25	24

$= 26 \times 25 \times 24$

$\boxed{= 15600}$ non-repeated three letter initials

d18

(a)

$= \boxed{16^{10} + 16^{22} + 16^{58}}$ different WEP keys

(b) Total letters = 26

$= 26^4 - 25^4$

$\boxed{= 66351}$

CamScanner

Q19

(a)

Since each value of domain can be mapped on either $\{0, 1\}$

Therefore;

Number of functions are $= 2 \times 2 \times 2 \times \ldots\ldots \times m$

$$\boxed{= 2^m}$$

(b)

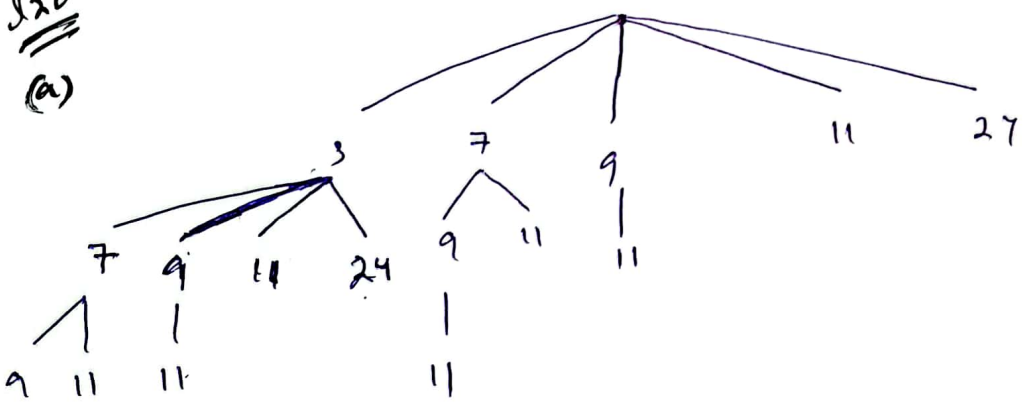
Number of one-to-one functions $= 5!$

$= 5 \times 4 \times 3 \times 2 \times 1$

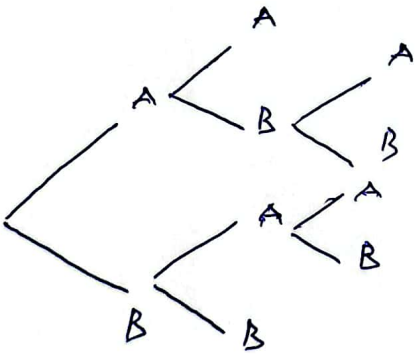
$$\boxed{= 120}$$

Q20

(a)



(b)



21

(a) ${}^8C_3 = \boxed{56 \text{ ways}}$ to choose students

(b) ${}^{12}C_6 = \boxed{924 \text{ ways}}$ to select elective courses

(c) ${}^9C_5 = \boxed{126 \text{ ways}}$ to select different teams

22

(a) $20 \times 19 \times 18 \times 17 \times 16 = \boxed{1860480 \text{ ways}}$

(b) ${}^{16}P_4 = \dfrac{16!}{(16-4)!} = \boxed{73680 \text{ ways}}$

(c) $15 \times 14 = \boxed{210 \text{ ways}}$

23

(a) ${}^5C_1 \cdot {}^3C_2 \cdot {}^7C_1 \cdot {}^4C_3 = \boxed{1200 \text{ ways}}$ sandwiches can be made

(b) $(15)(48)(27)(34)(28)(28) = \boxed{460615680 \text{ ways}}$

24

(a)

0	0	0	2	2	2	2	2	2	2

$= 2^7 = 128$ begin with three 0's

2	2	2	2	2	2	2	2	0	0

$= 2^8 = 256$ end with two 0's

0	0	0	2	2	2	2	2	0	0

$= 2^5 = 32$ begin with three 0's and end with two 0's

Therefore;

$= 128 + 256 - 32 \boxed{= 352}$

1)

0	2	2	2	2

$= 2^4 = 16$ begin with 0

2	2	2	1	1

$= 2^3 = 8$ end with two 1's

0	2	2	1	1

$= 2^2 = 4$ begin with 0 and end with two 1's

Therefore;

$= 16 + 8 - 4 \boxed{= 20}$.

Q25

(a) $N = 30$

$k = 26$

Therefore;

$\left\lceil \frac{N}{k} \right\rceil = \left\lceil \frac{30}{26} \right\rceil$

$\boxed{= 2}$

(b) $N = 8008278$

$k = 1000000$

$= \left\lceil \frac{N}{k} \right\rceil$

$= \left\lceil \frac{8008278}{1000000} \right\rceil$

$\boxed{= 9}$

(c) $N = 677$, $k = 38$

$\left\lceil \frac{N}{k} \right\rceil = \left\lceil \frac{677}{38} \right\rceil$

$\boxed{= 18}$

CamScanner

Q26

(a) x^5 in $(1+x)^{11}$

$$= \binom{11}{5} (1)^{11-5} (x)^5$$

$$= \binom{11}{5} (1)^6 x^5$$

$$\boxed{= 462x^5}$$

"462" is co-efficient of x^5 in $(1+x)^{11}$

(b) $a^7 b^{17}$ in $(2a-b)^{24}$

$$= \binom{24}{17} (2a)^{24-17} (-b)^{17}$$

$$= -\binom{24}{17} (2a)^7 (b)^{17}$$

$$\boxed{= -47301312\, a^7 b^{17}}$$

Q27

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

(a) Reflexive

R is reflexive because it contains $(a,a), (b,b), (c,c), (d,d)$

(b) Symmetric

R is not symmetric because it contains (a,c) but not (c,a).

(c) Anti-symmetric

R is not Anti-symmetric because it contains both (b,c) and (c,b)

(d) Transitive

R is not transitive because it contains (a,d) and (d,b) but not (a,b)

(e) Irreflexive

R is not irreflexive because it contains $(a,a), (b,b), (c,c), (d,d)$

(f) Asymmetric

R is not Asymmetric because it contains (b,c) and (c,b)

CamScanner

28 $A = \{0,1,2,3,4\}$ to $B = \{0,1,2,3\}$

(a) $a = b$

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

b) $a+b = 4$

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

(c) $a > b$

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

d) $a \mid b \rightarrow b/a$

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

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

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

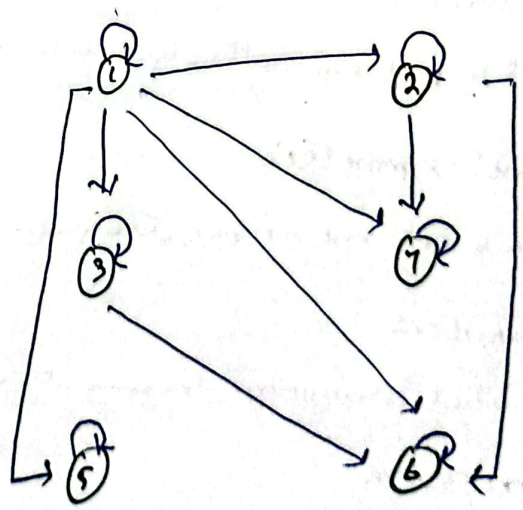
f) $\operatorname{Lcm}(a,b) = 2$

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

29 $\{1,2,3,4,5,6\}$; $R = \{(a,b) \mid a \text{ divides } b\}$

$\{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(5,5),(6,6)\}$

$$\begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$



Q30 $\{1, 2, 3, 4\}$

(a) $\{(2,2), (2,3), (2,4), (3,2), (3,3), (3,4)\}$

Not reflexive, symmetric, not Anti-symmetric, not transitive

(b) $\{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$

Reflexive, symmetric, not anti-symmetric, transitive

(c) $\{(2,4), (4,2)\}$

Not Reflexive, symmetric, not anti-symmetric, not transitive

(d) $\{(1,2), (2,3), (3,4)\}$

Not Reflexive, not symmetric, anti-symmetric, not transitive

(e) $\{(1,1), (2,2), (3,3), (4,4)\}$

Reflexive, symmetric, ~~N/A~~ anti-symmetric, not transitive

f) $\{(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)\}$

Not Reflexive, symmetric, not anti-symmetric, not transitive

Q31

(A) A is taller Than b

(i) Not reflexive ; because person can not be taller Than himself

(ii) Not symmetric ; because A > B then B > A ; which is not possible

(iii) Anti-symmetric ; because if A > B Then B > A not possible

(iv) Transitive ; because not reflexive

(B) a and b were born on The same day.

(i) Reflexive ; because A person can born on same day as himself/herself.

(ii) symmetric ; because A = B, Then B = A

(iii) Not anti-symmetric ; because symmetric

(iv) Transitive.

CamScanner

(c) a has the same first name as b.

(i) Reflexive

(ii) symmetric

(iii) not anti-symmetric

(iv) Transitive.

(d) a and b have a common grandparent.

(i) Reflexive

(ii) symmetric

(iii) not-antisymmetric

(iv) not-transitive.

132

(a) both symmetric and anti-symmetric

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

(b) neither symmetric nor anti-symmetric

$\{(1,3),(2,4),(3,1),(4,3)\}$

133 $A=\{1,2,3\}$

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

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

$R_3=\{(1,2),(1,3),(2,3)\}$

$R_4=\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$

$R_5=\{(1,1),(2,2),(3,3)\}$

$R_6=\{(1,2),(1,3),(2,1),(2,3),(3,1),(3,3)\}$

(a) $R_2 \cup R_4$

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

(b) $R_3 \cup R_6$

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

(c) $R_3 \cap R_6$

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

CamScanner

(d) $R_4 \cap R_6$

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

(e) $R_3 - R_6$?

$\{\ \}$

(f) $R_6 - R_3$

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

(g) $R_2 \oplus R_5$

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

(h) $R_3 \oplus R_5$

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

(i) $R_2 \circ R_1$

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \Rightarrow \{(2,1),(3,1),(3,2)\}$$

(j) $R_6 \circ R_6$

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

<u>all pairs</u>

<u>Q37</u> <u>(a)</u>

(i) $\{(1,1),(1,2),(1,3)\}$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

(ii) $\{(1,2),(2,1),(2,2),(3,3)\}$

$$\begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 3 & 0 & 0 & 1 \end{array}$$

(iii) $\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

CamScanner

iv) $\{(1,3), (3,1)\}$

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

(b)

(i) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

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

(ii) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

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

(iii) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

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

J35 (a)

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

Symmetry:- Since $l(a) = l(b)$, $l(b) = l(a)$

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

(b)

Reflexivity:- $a \equiv a \pmod m$, since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$

Symmetry:- $a \equiv b \pmod m$, $a-b$ is divisible by m so $a - b = km$

Similarly $b \equiv a \pmod m$, $b-a$ is divisible by m

$b - a = (-k)m$ $\quad \because k \in \mathbb{Z}$

J36 (a)

Transivity:-

$a \equiv b \pmod m$ and $b \equiv c \pmod m$

Then; m divides both $a-b$ and $b-c$

$a - b = km$, $b - c = lm$

$a - c = (a-b) + (b-c)$

$= km + lm$

$= (k+l)m$

Therefore; $a \equiv c \pmod m$

CamScanner