20k-1052.

Date:

CS211 - Discrete Structures

Assignment # 3

BSE-2B (S.M. Hassam Ali)

Q.1 $R = \{(a,a), (a,c), (a,d), (b,a), (b,b), (b,c), (b,d), (c,b), (c,c), (d,b), (d,d)\}$

a) Reflexive

$\forall a [a \in U \rightarrow (a,a) \in R]$

R is reflexive because it has (a,a), (b,b), (c,c) and (d,d) which satisfies the condition and forming loop at every node.

b) Symmetric

$\forall a \forall b [(a,b) \in R \rightarrow (b,a) \in R]$

R is not symmetric because (a,c) exist but (c,a) does not exist. $T \rightarrow F = F$

c) Antisymmetric

$\forall a \forall b [(a,b) \in R \wedge (b,a) \in R \rightarrow a = b]$

R is not antisymmetric because (b,c) and (c,b) exist but they are not equal. $T \wedge T \rightarrow F$

$T \rightarrow F$

F

d) Transitive.

$\forall a \forall b \forall c [(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R]$

R is not transitive because $(a,c) \wedge (c,b)$ exist but no (a,b). $T \wedge T \rightarrow F$

$T \rightarrow F$

F

Date:

e) Irreflexive

$\forall a[(a \in A) \rightarrow (a,a) \notin R]$

R is not Irreflexive because there is a loop at every node.

f) Asymmetric

$\forall a \forall b[((a,b) \in R)) \rightarrow ((b,a) \in R)]$

R is not Asymmetric because (b,c) and (c,b) exist. $T \rightarrow F = F$.

Q.2 $aRb \leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor$ $\lfloor x \rfloor$ is the floor of x.

a) R is reflexive since (a,a), $a = a$ is true for all real numbers.

b) R is symmetric since $a = b$ and can be $b = a$.

c) R is not anti-symmetric since $a = b$ and can be $b = a$ but not necessay at every time.

d) R is transitive because if $(a,b)(b,c) \in R$ and $a = b, b = c$ so $a = c$ therefore $(a,c) \in R$.

Date:

e) R is not irreflexive because $a = a$ is true for all real numbers.

f) R is not asymmetric since R is not antisymmetric.

Date:

Q.3 R $A=\{0,1,2,3,4\}$ to $B=\{0,1,2,3\}$

a) $a=b$

$R=\{(a,b) \mid a=b\}$

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

b) $a+b=4$

$R=\{(a,b) \mid a+b=4\}$

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

c) $a>b$

$R=\{(a,b) \mid a>b\}$

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

d) $a|b$

$R=\{(a,b) \mid a|b\}$

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

Date:

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

GCD is max 1 when no's are pair wise prime.

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

f) $lcm(a,b) = 2$.

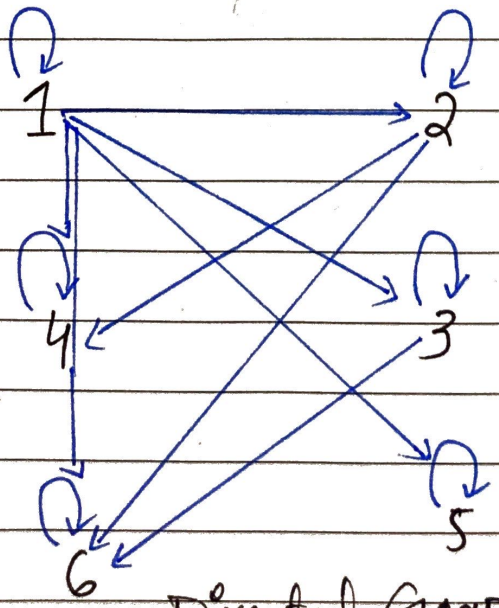
lcm = common x uncommon.
pair

$1 = 1 \times 1$	$2 = 2 \times 1$
$2 = 1 \times 2$	$2 = 2 \times 1$
$lcm = 2 \times 1$	$lcm = 2 \times 1$
$= 2$	$= 2$.

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

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

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



Directed Graph

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

Matrix

Date:

Q.5 Check whether R is reflexive, symmetric, antisymmetric, transitive. {1, 2, 3, 4}

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

- Not reflexive since $(1,1) \notin R$
- Not symmetric since $(2,4) \in R$ but $(4,2) \notin R$
- Not antisymmetric since $(2,3) \in R$ and $(3,2) \in R$ but $2 \neq 3$.
- Transitive

(2,2)	(2,3)	(2,3)	(2,3)	(3,2)
(2,3)	(3,3)	(3,2)	(3,4)	(2,2)
(2,3)	(2,3)	(2,2)	(2,4)	(3,2)

(3,3)	(3,3)
(3,2)	(3,3)
(3,2)	(3,3)

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

- Reflexive since $\forall (a,a) \in R$
- Symmetric since (1,2) and (2,1) $\in R$
- Not antisymmetric since (1,2) and (2,1) $\in R$ but $2 \neq 1$
- R is transitive. since all $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$

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

- Not reflexive because ∄(a,a) ∈ R
- Symmetric since (2,4) and (4,2) ∈ R
- Not Antisymmetric because of being symmetric
- Not transitive since (2,4) ∈R and (4,2) ∈R while (2,2) ∉R.

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

- Not reflexive because ∄(a,a) ∈R
- Not symmetric since for (1,2),(2,1) ∉R
- Antisymmetric since ∀(a,b) ∈R then (b,a) ∉R.
- Not transitive since (1,2) ∈R and (2,3) ∈R. but (1,3) ∉R.

e) R = {(1,1),(2,2),(3,3),(4,4)}

- Reflexive since ∀(a,a) ∈ R
- Symmetric since (a,b) ∈R and (b,a) ∈R
- Antisymmetric since (a,b) ∈R and (b,a) ∈R and a=b.
- Transitive

(1,1)	(2,2)	(3,3)	(4,4)
(1,1)	(2,2)	(3,3)	(4,4)
(1,1)	(2,2)	(3,3)	(4,4)

Date:

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

- Not reflexive since $\neg\forall(a,a) \in R$
- Not symmetric since $(1,4) \in R$ but $(4,1) \notin R$
- Not antisymmetric since $(1,3) \in R$ and $(3,1) \in R$ but $1 \neq 3$.
- Not transitive since $(1,3)$ and $(3,1) \in R$ but not $(1,1)$.

Q.6. {all people}.

a) a is taller than b.

- Not reflexive since a cannot be taller than himself
- Not symmetric since a can be taller than b, then person b cannot be taller than A.
- Antisymmetric since both conditions cannot be true and $a \neq b$ so $F \rightarrow F = T$.
- Transitive. because A is taller than B, B is taller then C. So A must be taller than C.

b) a and b were born on the same day.

- Reflexive because 'a' would be born on the same day as himself. (a,a)
- Symmetric because they are born on same day and vice-versa. $(a,b) \rightarrow (b,a)$
- Not Antisymmetric because they are present at the same day does not mean they are same.
- Transitive as in if A and B born on the same day, then B and C, so A and C on the same day.

20K-1052

Date:

c) a has the same first name as b.

- Reflexive since 'a' has the same first name as himself. (a, a).
- Symmetric since it can be written as now (a, b) → (b, a) because of same name.
- Not antisymmetric because they can have same name but be different.
- Transitive since A and B can have same name, then B and C and now A and C have same first name.

d) a and b have a common grandparent.

- Reflexive since they have a common grandparent makes a (a, a).
- Symmetric since A and B have common grandparents can be written as B and A have common grandparent
- Not Antisymmetric because they can have same grandparent but does not mean they are same.
- Not transitive because if A and B have common grandparents, then B and C have, so it does not mean that A and C also have common grandparent Like A and B can have common from father's side and B and C can have common from mother's side and vise-versa.

Date:

Q7. Example on a set that is $\{1,2,3,4\}$ R2 UR

a) Symmetric and antisymmetric

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

$\forall a\,(a,a) \in R$ for symmetric
Here $a=b$ for antisymmetric

b) Neither symmetric nor Antisymmetric
$R = \{(1,2),(2,3),(3,4)\}$

There is not (a,a) for symmetric
No (a,b) and (b,a) for $a=b$ for Antisymmetric.

Q.8 $A = \{1,2,3\}$

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

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

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

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

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

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

a) $R_2 \cup R_4$

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

b) $R_3 \cup R_6$

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

c) $R_3 \cap R_6$

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

d) $R_4 \cap R_6$

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

e) $R_3 - R_6$

$R = \{\}$

f) $R_6 - R_3$

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

g) $R_2 \oplus R_6$

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

Date:

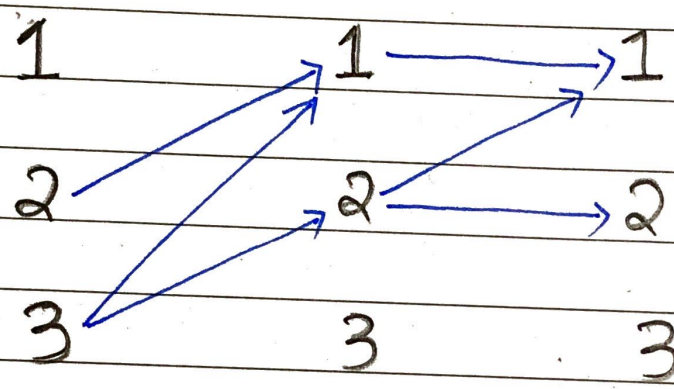
h) $R_3 \oplus R_5$

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

i) $R_2 \cdot R_1$

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

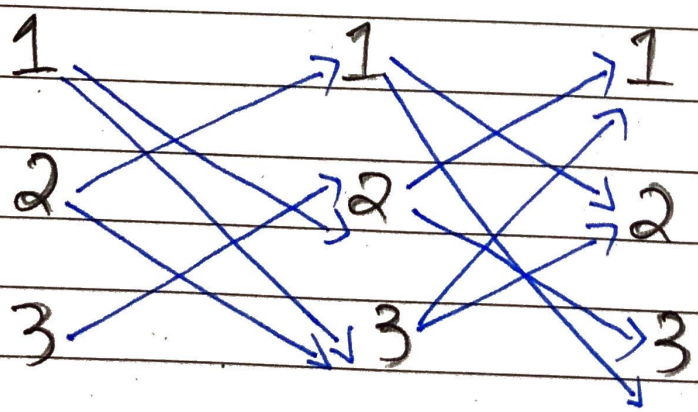
$R_1 = \{(2,1), (3,1), (3,2)\}$



$R_2 \cdot R_1 = \{(2,1), (3,1), (3,2)\}$

j) $R_6 \cdot R_6$

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



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

Victory

Page No.

2.9a) {1, 2, 3}

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)}

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

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

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

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

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

Date:

b) i

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

ii)

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

iii)

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

Q.10 a)

a) Reflexivity as $l(a) = l(a)$ follows aRa for all strings a.
Symmetry, since $l(a) = l(b)$, $l(b) = l(a)$ holds bRa.
Transivity, aRb and bRc. so $l(a) = l(b)$, $l(b) = l(c)$, and $l(a) = l(c)$ thefore aRc.

Q.11 quotient and remainder

a) 19 is divided by 7

$a = qd + r$
$19 = 7(2) + 5$
$q = 2 \quad r = 5$

Date:

Q.10b) $R = \{(a,b) \mid a \equiv b \pmod m\}$ is equivalence if $(a-b)/m$ so $a \equiv b \pmod m$

- Reflexivity since in $a \equiv a \pmod m$ $a-a/m = 0$
- Symmetry since in $a \equiv b \pmod m$ $(a-b/m)$ and $(b-a)/m$, $b-a = (-k)m$, $b \equiv a \pmod m$
- Transitivity since $a \equiv b \pmod m$ and $b \equiv c \pmod m$, means $(a-b/m)$, $(b-c/m)$ so $a-b = xm$, $b-c = ym$

$a-c = (a-b)+(b-c) = xm+ym = (x+y)m$

Hence $a \equiv c \bmod m$.

c) $a \equiv b \pmod m$ if $a \bmod m = b \bmod m$

$(a-b)/m$ for the congruent.

$a-b = mc$

$b + a - b = mc + b$

$a = mc+b$

$d = b \bmod m$

$b = me + d$.

$c+e$ = quotient

d = remainder

$0 \leq d < m$

$a = mc + mc + d$.

$a = m(c+e) + d$

$a \bmod m = d = b \bmod m$

Date:

b) -111 is divided by 11

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

$q = -11 \quad r = 10$

h) 4 is divided 1

$4 = 1(4) + 0$

$q = 4 \quad r = 0$

c) 789 is divided by 23

$789 = 23(34) + 7$

$q = 34 \quad r = 7$

d) 1001 is divisy by 13

$1001 = 13(77) + 0$

$q = 77 \quad r = 0$

e) 10 is divided by 19.

$10 = 19(0) + 10$

$q = 0 \quad r = 10$

f) 3 is divided by 5

$3 = 5(0) + 3$

g) -1 is divided by 3.

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

Date:

Q.12a) a div m , a mod m. $q = a \text{ div } m$
$r = a \bmod m$

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

$-2 = -111 \text{ div } 99$
↳ q

$87 = -111 \text{ div } 99$
↳ r.

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

$-99 = -9999 \text{ div } 101$

$0 = -9999 \bmod 101$

iii) $a = 10299, m = 99.$

$10 = 10299 \text{ div } 999$

$0 = -9999 \bmod 101$

iv) $a = 123456, m = 101$

$113 = 123456 \text{ div } 1001$

$333 = 123456 \bmod 1001$

b) congruent to 5 modulo 17 = 2

i) 80.

$a = 80 \quad b = 5 \quad m = 17$

$$\frac{a-b}{17} = \frac{80-5}{17} = \frac{75}{17}$$

so $80 \not\equiv 5 \pmod{17}$

ii) 103

$a = 103 \quad b = 5 \quad m = 17$

$$\frac{a-b}{m} = \frac{103-5}{17} = \frac{98}{17}$$

so $103 \not\equiv 5 \pmod{17}$

iii) -29

$a = \cancel{-103}\ -29 \quad b = 5 \quad m = 17$

$$\frac{-29-5}{17} = \frac{-34}{17} = -2$$

so $-29 \equiv 5 \bmod 17$

iv) -122

$a = -122 \quad b = 5 \quad m = 17$

$$\frac{-122-5}{17} = \frac{-127}{17}$$

so $-122 \equiv 5 \bmod 17$.

Q.13

i) 11, 15, 19.

gcd(11,15) = 1, gcd(15,19) = 1, gcd(11,19) = 1

Yes

ii) 14, 15, 21

NO

gcd(14,15) = 1, gcd(14,21) = 7, gcd(15,21) = 3

gcd(14,21) = 7
14 = 7 × 2
21 = 7 × 3

gcd(15,21) = 3
15 = 5 × 3
21 = 7 × 3.

iii) 12, 17, 31, 37

gcd(12,17) = 1, gcd(12,31) = 1, gcd(12,37) = 1,
gcd(17,31) = 1, gcd(17,37) = 1, gcd(31,37) = 1

YES

iv) 7, 8, 9, 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

Yes

Date:

b) Prime factorization

i) 88

$= 2 \times 2 \times 2 \times 11 = 2^3 \times 11.$

ii) 126

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

iii) 729

$= 3 \times 3 \times 3 \times 3 \times 3 \times 3 = 3^6$

iv) 1001

$= 7 \times 13 \times 11$

v) 1111

$= 11 \times 101$

vi) 909

$= 3^2 \times 101$

Q.14 GCD(144, 89) using Euclidean Algorithm.

$144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + 1$
$2 = 1(2) + 0$
↳ GCD = 1

GCD(1001, 100001)
$100001 = 1001(99) + 902$
$1001 = 902(1) + 99$
$902 = 99(9) + 11$
$99 = 11(9) + 0$
↳ GCD = 11

Date:

Q.15 Find modular inverses

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

a b m

GCD(a, m) = 1

GCD(55, 89)

$89 = 55(1) + 34$

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$1 = 3 \times 1 - 2 \times 1$

$= 3 \times 1 - 1(5 - 3 \times 1)$

$= 3 \times 1 - 5 + 3 \times 1$

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

~~$= 16 - 2 \times 5 - 5 \times 1$~~

~~$= 16 - 3 \times (13 \times 8 \times 1)$~~

~~$= 16 - 39 - 3 \times 8$~~

~~$= -23 - 3 \times (21$~~

$2 \times 8 - 2 \times 5 - 1 \times 5$

$2 \times 8 - 3(13 \times 8 \times 1)$

$2 \times 8 - 39 - 3 \times 8$

$-3 \times 13 - 1(21 - 13 \times 1)$

$-3 \times 13 - 1 \times 21 + 1 \times 13$

$-2(34 - 21 \times 1) - 1 \times 21$

$-2 \times 34 + 2 \times 21 - 1 \times 21$

$-2 \times 34 + 1 \times (55 - 34 \times 1)$

$-2 \times 34 + 1 \times 55 - 1 \times 34$

$-3 \times (89 - 55 \times 1) + 1 \times 55$

$-3 \times 89 + 3 \times 55 + 1 \times 55$

$-3 \times 89 + 4 \times 55$

m a

$55 \times 4 \times x = 34 \times 4 \pmod{89}$

$x = 136 \pmod{89}$

$= 47$

$89x = 0$

20K-1052.

Date:

$89x \equiv 2 \pmod{232}$

$a \quad b \quad m$

GCD(89, 232)

$232 = 89(2) + 54$
$89 = 54(1) + 35$
$54 = 35(1) + 19$
$35 = 19(1) + 16$
$19 = 16(1) + 3$
$16 = 3(5) + 1$
$3 = 1(3) + 0$

$89 \times 73 \times x \equiv 2 \times 73 \pmod{232}$

$x \equiv 146 \pmod{232}$
$= 146$

$1 = 16 \times 1 - 3 \times 5$
$= 16 \times 1 - 5(19 - 16 \times 1)$
$= 16 \times 1 - 5 \times 19 + 5 \times 16$
$= 6 \times (35 \times 1 - 19 \times 1) - 5 \times 19$
$= 6 \times 35 - 6 \times 19 - 5 \times 19$
$= 6 \times 35 - 11(54 \times 1 - 35 \times 1)$
$= 6 \times 35 - 11 \times 54 + 11 \times 35$
$= 17 \times (89 \times 1 - 54 \times 1) - 11 \times 54$
$= 17 \times 89 - 17 \times 54 - 11 \times 54$
$= 17 \times 89 - 28(232 \times 1 - 89 \times 2)$
$= 17 \times 89 - 28 \times 232 + 56 \times 89$
$= 73 \times 89 - 28 \times 232$
$= 73(89) + (-28)(232)$

$\rightarrow a = 73$

Date:

Q.16 Chinese remainder theorem.

i) $x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 6$
$x \equiv 3 \pmod 7$

$m = 5 \times 6 \times 7$
$= 210$

$a_1 = 1$ $\quad M_1 = \frac{210}{5} = 42$ $\quad M_3 = 210/7 = 30$

$a_2 = 2$

$a_3 = 3$ $\quad M_2 = 210/6 = 35$

$y_k = M_k^{-1} \bmod m_k$

* $y_1 = 42 \bmod 5$

$42 = 5(8) + 2$
$5 = 2(2) + 1$
$2 = 2(1) + 0$

$1 = 5 \times 1 - 2 \times 2$
$= 5 \times 1 - 2(42 \times 1 - 5 \times 8)$
$= 5 \times 1 - 2 \times 42 + 16 \times 5$
$= 21(5) + (-2)(42)$

$a_1 = -2 + 5$
$= 3$

* $y_2 = 35 \bmod 6$

$35 = 6(5) + 5$
$6 = 5(1) + 1$
$5 = 5(1) + 0$

$1 = 6 \times 1 - 5 \times 1$
$= 6 \times 1 - 1(35 \times 1 - 6 \times 5)$
$= 6(6) + (-1)(35)$

$a_2 = -1 + 6 = 5$

* $y_3 = 30 \bmod 7$

$30 = 7(4) + 2$
$7 = 2(3) + 1$
$2 = 2(2) + 0$

$1 = 7 \times 1 - 2 \times 3$
$= 7 \times 1 - 3(30 - 7 \times 4)$
$= 7 \times 1 - 3 \times 30 + 14 \times 7$
$= 15 \times 7 - 3 \times 30$
$= 15(7) + (-3)(30)$

$a_3 = -3 + 7 = 4$

Date:

$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3) \bmod m$

$= (1 \times 42 \times 3) + (2 \times 35 \times 5) + (3 \times 30 \times 4) \bmod 210$

$= 836 \bmod (210)$

$= 206$

ii) $x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod{11}$

$a_1 = 1, a_2 = 2, a_3 = 3\ a_4 = 4$

$m = 2 \times 3 \times 5 \times 11 = 330$

$M_1 = \frac{330}{2} = 165, \quad M_2 = \frac{330}{3} = 110$

$M_3 = 66 \qquad M_4 = 30$

* $y_1 = 165 \bmod 2$

$165 = 2(82) + 1$

$2 = 1(2) + 0$

$1 = 1 \times 165 - 2 \times 82$

$= 165(1) + (-2)(82)$

$a_1 = 1$

* $y_2 = 110 \bmod 3$

$110 = 3(36) + 2$

$3 = 2(1) + 1$

$1 = 3x1 - 2x1$

$= 3x1 - 1(110x1 - 3x36)$

$3x1 - 110x1 + 3x36$

$3x37 + (-1)(110)$

$= 3(37) + (-1)(110)$

$a_2 = -1 + 3 = 2$

* $y_3 = 66 \bmod 5$

$66 = 5(13) + 1$

$5 = 1(5) + 0$

$1 = 66(1) + (-13)(5)$

$a_3 = 1$

* $y_4 = 30 \bmod 11$

$30 = 11(2) + 8$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

Date:

$1 = 3x1 - 1x2$

$= 3x1 - 1(8x1 - 3x2)$

$= 3x1 - 8x1 + 3x2$

$= 3x3 - 8x1$

$= 3(11x1 - 8x1) - 8x1$

$= 3x11 - 3x8 - 8x1$

$= 3x11 - 4x(30 - 11x2)$

$= 3x11 - 4x30 + 8x11$

$= 11x11 - 4x30$

$= 11(11) + (-4)(30)$

$a_4 = -4 + 11$

$= 7$

$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \mod m$

$= (3x462x3) + (3x385x1) + (1x330x1) +$

$= (1x165x1) + (2x110x2) + (3x66x1) + (4x30x7) \mod 330$

$= 1643 \mod 330$

$= 323$

20K-1052.

Date:

b)

$m = m_1 \times m_2 \times m_3 \times m_4$

$= 5 \times 6 \times 7 \times 11$

$= 2316$

$a_1 = 3 \quad a_2 = 3 \quad a_3 = 1 \quad a_4 = 0$

$M_1 = 462 \quad M_3 = 330$

$M_2 = 385 \quad M_4 = 210$

$y_1 = 462 \bmod 5$

$462 = 5(92) + 2$

$5 = 2(2) + 1$

$1 = 5 \times 1 - 2 \times 2$

$= 5 \times 1 - 2(462 \times 1 - 5 \times 92)$

$= 5 \times 1 - 2 \times 462 + 184 \times 5$

$= 5(185) + (-2)(462)$

$y_1 = -2 + 5 = 3$

$y_2 = 330 \bmod 6$

385

$330 = 6(64) + 1$

$1 = 1 \times 385 + (-64)(6)$

$y_2 = 1$

$y_3 = 330 \bmod 7$

$330 = 7(47) + 1$

$1 = (1)(330) + (-47)(7)$

$y_3 = 1$

$y_4 = 210 \bmod 11$

$210 = 11(19) + 1$

$1 = (1)(210) + (-19)(11)$

$y_4 = 1$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4 \bmod m$

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

$x = 5643 \bmod 2310$

$= 1023.$

Date:

Q.17 Inverse of a modulo m.

a) $a = 2 \quad m = 17$

$y = 2 \bmod 17 \quad \text{Gcd}(17, 2)$

$17 = 2(8) + 1$

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

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

$\bar{a} = -8 + 17 = 9$

b) $a = 34, \quad m = 89$

$\text{Gcd}(34, 89)$

$89 = 34(2) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = (2)(1) + 1$

$1 = 3 \times 2 - 1(5 \times 1 - 3 \times 1)$
$= 2 \times 3 - 5 \times 1$
$= 2(8 \times 1 - 5 \times 1) - 5 \times 1$
$= 8 \times 2 - 3 \times 5$
$= 8 \times 2 - 3(13 \times 1 - 8 \times 1)$
$= 8 \times 2 - 3 \times 13 + 8 \times 3$
$= 5 \times (21 \times 1 - 13 \times 1) - 3 \times 13$
$= 5 \times 21 - 8 \times (34 \times 1 - 21 \times 1)$
$= 5 \times 21 - 8 \times 34 + 8 \times 21$
$= 13 \times (89 - 34 \times 2) - 8 \times 34$
$= 13 \times 89 - 26 \times 34 - 8 \times 34$
$= (13)(89) + (-34)(34)$

$\bar{a} = -34 + 89 = 55$

Victory

Page No.

c) $a = 144, m = 233$

GCD (144, 233)

$233 = 144(1) + 89$
$144 = 89(1) + 55$
$89 = 55(1) + 34$
$55 = 34(1) + 21$
$34 = 21(1) + 13$
$21 = 13(1) + 8$
$13 = 8(1) + 5$
$8 = 5(1) + 3$
$5 = 3(1) + 2$
$3 = 2(1) + 1$

$= 8 \times 34 + 13 \times 55 - 13 \times 34$
$= -21(89 \times 1 - 55 \times 1) + 13 \times 55$
$= -21 \times 89 + 21 \times 55 + 13 \times 55$
$= -21 \times 89 + 34(144 \times 1 - 89 \times 1)$
$= -21 \times 89 + 34 \times 144 - 89 \times 34$
$= -55(233 \times 1 - 144 \times 1) + 34 \times 144$
$= -55 \times 233 + 55 \times 144 + 34 \times 144$
$= (233)(-55) + (89)(144)$

$\bar{a} = 89$

$1 = 3 \times 1 - 2 \times 1$
$= 3 \times 1 - 1(5 \times 1 - 3 \times 1)$
$= 3 \times 1 - 5 \times 1 + 3 \times 1$
$= 2 \times (8 \times 1 - 5 \times 1) - 5 \times 1$
$= 2 \times 8 - 5 \times 2 - 5 \times 1$
$= 2 \times 8 - 3(13 \times 1 - 8 \times 1)$
$= 2 \times 8 - 3 \times 13 + 3 \times 8$
$= -3 \times 13 + 5(21 - 13 \times 1)$
$= -3 \times 13 + 5 \times 21 - 5 \times 13$
$= -8 \times (34 \times 1 - 21 \times 1) + 5 \times 21$
$= -8 \times 34 + 8 \times 21 + 5 \times 21$
$= -8 \times 34 + 13(55 \times 1 - 34(1))$

Date:

d) $a = 200 \quad m = 1001$

Gcd (200, 1001)

$1001 = 200(5) + 1$

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

$\bar{a} = -5 + 1001 = 996$

Q.18 Encrypt STOP POLLUTION

i) $f(p) = (p+4) \bmod 26$

S T O P P O L L U T I O N

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

$f(18) = (18+4) \bmod 26 = 22$ (W)

$f(19) = (19+4) \bmod 26 = 23$ (W) (X)

$f(14) = (14+4) \bmod 26 = 18$ (S)

$f(15) = (15+4) \bmod 26 = 19$ (T)

$f(11) = (11+4) \bmod 26 = 15$ (P)

$f(20) = (20+4) \bmod 26 = 24$ (Y)

$f(8) = (8+4) \bmod 26 = 12$ (M)

$f(13) = (13+4) \bmod 26 = 17$ (R)

Encrypted message is:

WXST TSPPYXMSR