20K-0208
BCS-3E

ASSIGNMENT #2

1

QUESTION #1:

a) R is reflexive since there are self-loops for all domain values.

b) R is not symmetric since $(a,c) \in R$ but $(c,a) \notin R$.

c) R is not anti-symmetric since $(b,d) \in R$ and (d,b) also $\in R$ and $b \neq d$.

d) R is not transitive because $(a,c) \in R$ and $(c,b) \in R$ but $(a,b) \notin R$.

e) R is not irreflexive because $(a,a) \in R$.

f) R is not assymmetric because it is neither irreflexive nor anti-symmetric.

QUESTION #2:

$$(a,b) \longleftrightarrow \lfloor a \rfloor = \lfloor b \rfloor$$

a) R is reflexive, because $a=a$ exists for all real numbers.

b) R is symmetric since if $a=b$ then $b=a$.

c) R is not anti-symmetric because ~~if~~ for different (a,b), $(a,b) \in R$ but $(b,a) \notin R$ because of floor function.

d) R is transitive because if $(a,b) \in R$ and $(b,c) \in R$ then by substitution $(a,c) \in R$.

e) R is not irreflexive since $a=a$ exists.

f) R is not assymetric because it is neitheir anti-symmetric nor irreflexive.

Waleef

20K-0208 BCS-3E (2)

QUESTION #3:

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

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

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

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

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

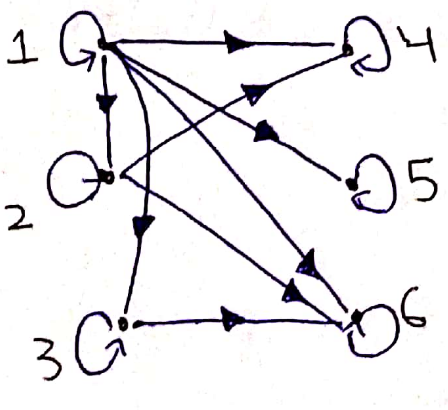
e) $\{(1,1),(1,2),(1,3),(2,1),(3,1),(4,1),(2,3),(3,2),(4,3),(1,0),(0,1)\}$

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

QUESTION #4:

~~[illegible]~~

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



Di-graph

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

Matrix

QUESTION #5:

a) i) R is not reflexive since $(1,1) \notin R$.

ii) R is not symmetric since $(2,4) \in R$ but $(4,2) \notin R$.

iii) R is not anti-symmetric since $(2,3) \in R$ and $(3,2) \in R$ but $2 \neq 3$.

iv) R is transitive because if $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$ for all real numbers.

b) i) R is reflexive because $(1,1),(2,2),(3,3),(4,4) \in R$.

ii) R is symmetric because $(1,2) \in R$ and $(2,1) \in R$.

iii) R is not anti-symmetric because $(1,2) \in R$ and $(2,1) \in R$ but $1 \neq 2$.

iv) R is transitive because for all relations $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$.

c) i) R is not reflexive since $(1,1) \notin R$.

ii) R is symmetric because $(2,4) \in R$ and $(4,2) \in R$.

iii) R is not anti-symmetric because $2 \neq 4$.

iv) R is not transitive since $(2,4),(4,2) \in R$ but $(2,2) \notin R$.

d) i) R is not reflexive since $(1,1) \notin R$.

ii) R is not symmetric since since $(1,2) \in R$ but $(2,1) \notin R$.

iii) R is anti-symmetric since $(1,2) \in R$ but $(2,1) \notin R$.

iv) R is not transitive since $(1,2),(2,3) \in R$ but $(1,3) \notin R$.

Dabaf

e) i) R is reflexive since $(1,1),(2,2),(3,3),(4,4) \in R$.

ii) R is symmetric since $(1,1)$ is symmetric.

iii) R is anti-symmetric because $(a,b)(b,a) \in R$ and $a=b$.

iv) R is transitive because $(a,b)(b,c) \in R$ then $(a,c) \in R$.

f) i) R is not reflexive since $(1,1) \notin R$.

ii) R is not symmetric because $(2,3) \in R$ but $(3,2) \notin R$.

iii) R is not anti-symmetric since $(1,3)(3,1) \in R$ but $1 \neq 3$.

iv) R is not transitive since $(1,3)(3,1) \in R$ but $(1,1) \notin R$.

QUESTION #6:

a) i) R is not reflexive because someone cannot be taller than themselves.

ii) R is not symmetric since if a is taller than b, then b cannot be taller than a.

iii) R is anti-symmetric since if a is taller than b than b can't be taller than a.

iv) R is irreflexive because someone cannot be taller than themselves.

v) R is transitive since if a is taller than b and b is taller than c, then a is taller than c.

vi) R is asymmetric since it is irreflexive and anti-symmetric.

b) i) R is reflexive since a person is born on the same day as himself.

ii) R is symmetric since if (a,b) are born on the same day then (b,a) are also born on the same day.

iii) R is not anti-symmetric since being born on the same day doesn't imply being the same person.

iv) R is not irreflexive since a person is born on the same day as himself.

v) R is transitive because if (a,b) are born on the same day and (b,c) are also born on the same day then (a,c) are born on the same day.

vi) R is not asymmetric since it is not irreflexive.

c) i) R is reflexive because a person ~~first~~ has same name as himself.

ii) R is symmetric since if (a,b) have same first names then (b,a) also have same first names.

iii) R is not antisymmetric since (a,b) (b,a) ∈ R but a and b are not necessarily the same person.

iv) R is not irreflexive since a person's name is same as himself.

v) R is transitive because if a,b and b,c have same names, then a,c have same names.

vi) R is not asymmetric since it is neither irreflexive nor anti-symmetric.

20K-0100

20K-0208 BCS-3E

d) i) R is reflexive since a person has same gp as himself.

ii) R is symmetric as if (a,b) have same gp then (b, a) have same gp.

iii) R is not antisymmetric because (a,b) (b,a) ∈ R but a,b are not necessarily the same.

iv) R is not irreflexive since a person has same gp as himself.

v) R is transitive since if (a,b) and (b,c) have same gp, then (a,c) have same gp.

vi) R is not asymmetric since it is neither anti-symmetric nor irreflexive.

QUESTION #7:

a) Let $A=\{1,2,3\}$

$R=\{(1,1),(2,2),(3,3)\}$ is both symmetric and anti-symmetric.

b) Let $A=\{1,2,3\}$

$R=\{(1,2),(2,3),(3,1)\}$ is neitheir symmetric nor anti-symmetric.

Wahab

20K-0208 BCS-3E

QUESTION #8:

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

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

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

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

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

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

a) $R_2 \cup R_4 = \{(2,1),(3,1),(3,2),(1,1),(2,2),(3,3),(1,2),(1,3),(2,3)\}$

b) $R_3 \cup R_6 = \{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)\}$

c) $R_3 \cap R_6 = \{(1,2),(1,3),(2,3)\}$

d) $R_4 \cap R_6 = \{(1,2),(1,3),(2,3)\}$

e) $R_3 - R_6 = \{\}$

f) $R_6 - R_3 = \{(2,1),(3,1),(3,2)\}$

~~g) $R_2 \oplus R_6 = \{(2,1),(3,1),(3,2)\}$~~

g) $R_2 \oplus R_6 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(2,3)\}$

h) $R_3 \oplus R_5 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(2,3)\}$

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

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

Wahaj

20K-0208 BCS-3E

QUESTION # 9(a):

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

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

QUESTION # 9(b):

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

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

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

QUESTION # 10 (a):

For a relation to have equivalence, it must follow:

① Reflexivity: R is reflexive since a string has same length as itself.

② Symmetry: R is symmetric since if length of a is same as b, then $l(b) = l(a)$.

③ Transitivity: R is transitive since if $l(a) = l(b)$ and $l(b) = l(c)$, then $l(a) = l(c)$.

Hence, R is an equivalence relation.

Wahaj

20K-0208 BCS-3E

QUESTION # 10(b):

For $a \equiv b \pmod{m} \Rightarrow a-b/m$ must hold true.

For equivalence relations, three rules must be followed:

Reflexity: R is reflexive since for $(a,a) \Rightarrow a-a/m = 0$
Since $0 = 0 \pmod{m}$

Symmetry: R is symmetric. Suppose $a \equiv b \pmod{m}$ it can be written as $a-b \equiv mk$ where k is any integer. Now if we reverse the equation, it becomes $b-a = (-k)m$ where k still stands as an integer. Hence, $b \equiv a \pmod{m}$.

Transitivity: Suppose that $a \equiv b \pmod{m}$. We get $a-b = km$. and $b \equiv c \pmod{m}$ so $b-c = lm$ where l and m are any integers. Adding these eqns we get $b-c+a-b = km+lm$

$$\Rightarrow a-c \equiv (k+l) \bmod m$$

where $(k+l)$ can be said as any other integer such as r.

$$\Rightarrow a-c \equiv r \bmod m$$

Hence,

$$a \equiv c \pmod{m}$$

Hence, the relation holds equivalency.

20K-0208 BCS-3E

QUESTION # 10(c):

$a \equiv b \pmod m \longleftrightarrow a \bmod m = b \bmod m$

L.H.S $\Rightarrow a \equiv b \pmod m$

$\Rightarrow a - b = km$ (k is any integer) —— ①

Let $r = a \bmod m$ —— ②

By division algorithm,

$a = qd + r$

Let $d = m$ (any int)

$a = mq + r$

put in ①

$mq + r - b = km$

$mq - km = b - r$

$m(q - k) + r = b$

Since, $(q-k)$ is any integer, we can write it as

$r = b \bmod m$ —— ③

by ② & ③

$\boxed{a \bmod m = b \bmod m}$. proved!

R.H.S $\Rightarrow$ Let $r = a \bmod m = b \bmod m$

By division algorithm,

$a = qd + r$

$\Rightarrow a = mk + r$ —— ④

$b = ml + r$ —— ⑤

subtract ④ and ⑤

$a - b = mk - ml + r - r$

$a - b = m(k - l)$, Since $(k-l)$ is any integer

we can write it as $\boxed{a \equiv b \pmod m}$ proved!

QUESTION # 11:

a) $q = 2, r = 5$ b) $q = -11$ ~~-11~~, $r = 10$

c) $q = 34, r = 7$ d) $q = 77, r = 0$

e) $q = 0, r = 10$ f) $q = 0, r = 3$

g) $q = -1, r = 2$ h) $q = 4, r = 0$

QUESTION # 12(a):

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

i) $q = -2, r = 87$ ii) $q = -99, r = 0$

iii) $q = 10, r = 309$ iv) $q = 123, r = 333$

QUESTION # 12(b):

For. $a \equiv b \pmod m$, a number is congruent

if $\frac{a-b}{m} = k$ [an integer].

i) $80 = 5 \pmod{17}$ $= \frac{80-5}{17} = \frac{75}{17} = 4.41$ [Not congruent]

ii) $103 = 5 \pmod{17}$ $= \frac{103-5}{17} = \frac{98}{17} = 5.76$ [Not congruent]

iii) $-29 = 5 \pmod{17}$ $= \frac{-29-5}{17} = \frac{-34}{17} = -2$ [Congruent]

iv) $-122 = 5 \pmod{17}$ $= \frac{-122-5}{17} = \frac{-127}{17} = 7.47$ [Not congruent]

20K-0208 BCS-3E

QUESTION #13(a):

i) (11,15,19)

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

Hence, (11,15,19) are pairwise primes.

ii) (14,15,21)

gcd(14,15) = 1

gcd(15,21) = 3

gcd(14,21) = 7

Hence (14,15,21) are not pairwise primes.

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

Hence, (12,17,31,37) are pairwise primes.

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

Hence, (7,8,9,11) are pairwise primes.

QUESTION #13(b):

i) 88

$\Rightarrow 2^3 \times 11$

2	88
2	44
2	22
11	11
	1

ii) 126

$\Rightarrow 2 \times 3^2 \times 7$

2	126
3	63
3	21
7	7
	1

Wahd

20K-0208 BCS-3E

iii) 729

$\Rightarrow 3^6$

3	729
3	243
3	81
3	27
3	9
3	3
	1

iv) 1001

$\Rightarrow 7 \times 11 \times 13$

7	1001
11	143
13	13
	1

v) 1111

$\Rightarrow 11 \times 101$

11	1111
101	101
	1

vi) 909

$\Rightarrow 3^2 \times 101$

3	909
3	303
101	101
	1

QUESTION #14:

i) gcd (144, 89)

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

Substituting backwards

$$1 = 1 \cdot 3 - 1 \cdot 2 \quad \text{— ①}$$
$$2 = 1 \cdot 5 - 1 \cdot 3$$

put in ①

$$1 = 1 \cdot 3 - 1 \cdot 5 + 1 \cdot 3$$
$$1 = 2 \cdot 3 - 1 \cdot 5 \quad \text{— ②}$$

$3 = 1.8 - 1.5$

put in 2

$1 = 2.(1.8 - 1.5) - 1.5$

$1 = 2.8 - 2.5 - 1.5$

$1 = 2.8 - 3.5$ — 3

$5 = 1.13 - 1.8$

put in 3

$1 = 2.8 - 3.(1.13 - 1.8)$

$1 = 2.8 - 3.13 + 3.8$

$1 = 5.8 - 3.13$ — 4

$8 = 1.21 - 1.13$

$1.13 = \cancel{1}.21 - 1.8$

put in 4

$1 = 5.8 - 3(1.21 - 1.8)$

$1 = 5.8 - 3.21 + 3.8$

$1 = 8.8 - 3.21$ — 5

$13 = 1.34 - 1.21$

$1.21 = 1.34 - 1.13$

put in 5

$1 = 8.8 - 3(1.34 - 1.13)$

$1 = 8.8 - 3.34 + 3.13$ — 6

$21 = 1.55 - 1.34$

$1.34 = 1.55 - 1.21$

put in 6

$1 = 8.8 + 3.13 - 3.(1.55 - 1.21)$

$1 = 8.8 + 3.13 - 3.55 + 3.21$ — 7

Waleed

20K-0208

BCS-3E

$34 = 1 \cdot 89 - 1 \cdot 55$

$1 \cdot 55 = 1 \cdot 89 - 1 \cdot 34$

put in (7)

$1 = 8 \cdot 8 + 3 \cdot 13 - 3(1 \cdot 89 - 1 \cdot 34) + 3 \cdot 21$

$1 = 8 \cdot 8 + 3 \cdot 13 + 3 \cdot 21 + 3 \cdot 34 - 3 \cdot 89$ —— (8)

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

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

put in (8)

$1 = 8 \cdot 8 + 3 \cdot 13 + 3 \cdot 21 + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 8(1 \cdot 21 - 1 \cdot 13) + 3 \cdot 13 + 3 \cdot 21 + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 8 \cdot 21 - 8 \cdot 13 + 3 \cdot 13 + 3 \cdot 21 + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 11 \cdot 21 - 5 \cdot 13 + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 11 \cdot 21 - 5(1 \cdot 34 - 1 \cdot 21) + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 11 \cdot 21 - 5 \cdot 34 + 5 \cdot 21 + 3 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 16 \cdot 21 - 2 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 16(1 \cdot 55 - 1 \cdot 34) - 2 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 16 \cdot 55 - 16 \cdot 34 - 2 \cdot 34 - 3 \cdot 144 + 3 \cdot 55$

$1 = 19 \cdot 55 - 18 \cdot 34 - 3 \cdot 144$

$1 = 19 \cdot 55 - 18(1 \cdot 89 - 1 \cdot 55) - 3 \cdot 144$

$1 = 19 \cdot 55 - 18 \cdot 89 + 18 \cdot 55 - 3 \cdot 144$

$1 = 37 \cdot 55 - 18 \cdot 89 - 3 \cdot 144$

$1 = 37(1 \cdot 144 - 1 \cdot 89) - 3 \cdot 144 - 18 \cdot 89$

$1 = 37 \cdot 144 - 37 \cdot 89 - 3 \cdot 144 - 18 \cdot 89$

$1 = 34 \cdot 144 - 55 \cdot 89$

$\boxed{1 = (34)(144) + (-55)(89)}$ Linear combination of gcd(144, 89)

2) gcd(1001, 100001)

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

Backward substitution,

$$11 = 1\cdot 902 - 9\cdot 99 \quad \text{—} ①$$
$$99 = 1\cdot 1001 - 1\cdot 902$$
$$\cancel{1\cdot 902 = 1\cdot 1001 - 1\cdot 99}$$

put in ①

$$\cancel{11 = 1\cdot(1001 - 1\cdot 99) - 9\cdot 99}$$
$$\cancel{11 = 1\cdot 1001 - 1\cdot 99 - 9\cdot 99}$$
$$\cancel{11 = 1\cdot 1001 - 10\cdot 99 \text{ — } ②}$$
$$\cancel{902 = 1\cdot 100001 - 99\cdot 1001}$$

$$11 = 1\cdot 902 - 9(1\cdot 1001 - 1\cdot 902)$$
$$11 = \cancel{1\cdot 902} - 9\cdot 1001 + 10\cdot 902 \quad \text{—} ②$$
$$902 = 1\cdot 100001 - 99\cdot 1001$$

put in ②

$$11 = \cancel{1\cdot 902} - 9\cdot 1001 + 10(1\cdot 100001 - 99\cdot 1001)$$
$$11 = -9\cdot 1001 + 10\cdot 100001 - 990\cdot 1001$$
$$11 = -999\cdot 1001 + 10\cdot 100001$$
$$\boxed{11 = (10)(100001) + (-999)(1001)}$$

Linear combination of gcd(1001, 100001)

QUESTION #15:

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

$55 = (0)(89) + 55$

$89 = (1)(55) + 34$

$(55) = (1)(34) + 21$

$(34) = (1)(21) + 13$

$21 = (1)(13) + 8$

$13 = (1)(8) + 5$

$8 = (1)(5) + 3$

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

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

Backward substitution

$1 = 1\cdot 3 - 1\cdot 2$ —— ①

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

put in ①

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

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

$1 = 2\cdot 3 - 1\cdot 5$ —— ②

$3 = 1\cdot 8 - 1\cdot 5$

put in ②

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

$1 = 2\cdot 8 - 2\cdot 5 - 1\cdot 5$

$1 = 2\cdot 8 - 3\cdot 5$ —— ③

$5 = 1\cdot 13 - 1\cdot 8$

put in ③

$1 = 2\cdot 8 - 3\cdot(1\cdot 13 - 1\cdot 8)$

$1 = 2\cdot 8 - 3\cdot 13 + 3\cdot 8$

Wahab

Scanned with CamScanner

$$1 = 5.8 - 3.13 \quad \text{—} (4)$$

$$8 = 1.21 - 1.13$$

put in (4)

$$1 = 5(1.21 - 1.13) - 3.13$$

$$1 = 5.21 - 5.13 - 3.13$$

$$1 = 5.21 - 8.13 \quad \text{—} (5)$$

$$13 = 1.34 - 1.21$$

put in (5)

$$1 = 5.21 - 8(1.34 - 1.21)$$

$$1 = 5.21 - 8.34 + 8.21$$

$$1 = 13.21 - 8.34 \quad \text{—} (6)$$

$$21 = 1.55 - 1.34$$

put in (6)

$$1 = 13.(1.55 - 1.34) - 8.34$$

$$1 = 13.55 - 13.34 - 8.34$$

$$1 = 13.55 - 21.34 \quad \text{—} (7)$$

$$34 = 1.89 - 1.55$$

put in (7)

$$1 = 13.55 - 21(1.89 - 1.55)$$

$$1 = 13.55 - 21.89 + 21.55$$

$$1 = 34.55 - 21.89 \quad \text{—} (8)$$

$$55 = 1.55 + 0.89$$

put in (8)

$$1 = 34.55 - 21.89$$

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

inverse of 55 = 34

20K-0208 BCS-3E

$55x = 34 \pmod{89}$

× both side by inverse

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

$x = 1156 \pmod{89}$

$\boxed{x = 88}$

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

$89 = (0)(232) + 89$

$232 = (2)(89) + 54$

$89 = (1)(54) + 35$

$54 = (1)(35) + 19$

$35 = (1)(19) + 16$

$19 = (1)(16) + 3$

$16 = (5)(3) + 1$

Backward substitution

$1 = 1 \cdot 16 - 5 \cdot 3$ — ①

$3 = 1 \cdot 19 - 1 \cdot 16$

put in ①

$1 = 1 \cdot 16 - 5(1 \cdot 19 - 1 \cdot 16)$

$1 = 1 \cdot 16 - 5 \cdot 19 + 5 \cdot 16$

$1 = 6 \cdot 16 - 5 \cdot 19$ — ②

$16 = 1 \cdot 35 - 1 \cdot 19$

put in ②

$1 = 6(1 \cdot 35 - 1 \cdot 19) - 5 \cdot 19$

$1 = 6 \cdot 35 - 6 \cdot 19 - 5 \cdot 19$

$1 = 6 \cdot 35 - 11 \cdot 19$ — ③

20K-0208 BCS-3E

$19 = 1.54 - 1.35$

put in 3

$1 = 6.35 - 11(1.54 - 1.35)$

$1 = 6.35 - 11.54 + 11.35$

$1 = 17.35 - 11.54$ — 4

$35 = 1.89 - 1.54$

put in 4

$1 = 17(1.89 - 1.54) - 11.54$

$1 = 17.89 - 17.54 - 11.154$

$1 = 17.89 - 28.54$ — 5

$54 = 1.232 - 2.89$

put in 5

$1 = 17.89 - 28(1.232 - 2.89)$

$1 = 17.89 - 28.232 + 56.89$

$1 = 73.89 - 28.232$ — 6

$89 = 1.89 - 0.232$

$1 = (73)(89) + (-28)(232)$

$\boxed{\text{inverse} = 73}$

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

$\times$ 73 on both sides

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

$x = 146 \pmod{232}$

$\boxed{x = 146}$

QUESTION #16(a):

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

$\gcd(5,6)=1 \quad \gcd(5,7)=1 \quad \gcd(6,7)=1$

Hence, the modulos are pairwise primes.

$m = 5 \times 6 \times 7 = m_1 m_2 m_3 = 210$

$M_K = \dfrac{m}{m_K} \quad M_1 = \dfrac{210}{5} = 42 \quad M_2 = \dfrac{210}{6} = 35 \quad M_3 = \dfrac{210}{7} = 30$

Now,

$$x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3) \bmod m \quad \text{—— ①}$$

$y_K = \overline{M_K} \bmod m_K$

$y_1 = 42^{-1} \bmod 5$

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

$5 = (2)(2) + 1$

Backward substitution,

$1 = 1.5 - 2.2$ —— ①

$2 = 1.42 - 8.5$

put in ①

$1 = 1.5 - 2(1.42 - 8.5)$

$1 = 1.5 - 2.42 + 32.5$

$1 = 33.5 + (-2)(42)$

$y_1 = -2 + 5$

$\boxed{y_1 = 3}$

$y_2 = 35^{-1} \bmod 6$

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

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

Backward substitution,

$1 = 1.6 - 1.5$ —— ②

$5 = 1.35 - 5.6$

put in ②

$1 = 1.6 - (1.35 - 5.6)$

$1 = 1.6 - 1.35 + 5.6$

$1 = 6.6 - 1.35$

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

$y_2 = -1 + 6$

$\boxed{y_2 = 5}$

20K-0208 BCS-3E

$y_3 = 30^{-1} \pmod 7$

$30 = (4)(7) + 2$

$7 = (3)(2) + 1$

Backward substitution,

$1 = 1\cdot7 - 3\cdot2$ — (1)

$2 = 1\cdot30 - 4\cdot7$

put in (1)

$1 = 1\cdot7 - 3(1\cdot30 - 4\cdot7)$

$1 = 1\cdot7 - 3\cdot30 + 12\cdot7$

$1 = 13\cdot7 - 3\cdot30$

$1 = (13)(7) + (-3)(30)$

$y_3 = -3 + 7$

$\boxed{y_3 = 4}$

put in (1)

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

$x = (126 + 350 + 360) \bmod 210$

$x = 836 \pmod{210}$

$\boxed{x = 206}$

Dahal

20K-0208 BCS-3E

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

$\gcd(2,3)=1$ $\gcd(2,5)=1$ $\gcd(2,11)=1$ $\gcd(3,5)=1$

$\gcd(3,11)=1$ $\gcd(5,11)=1$

Hence, the modulos are pairwise primes.

$m = m_1 m_2 m_3 m_4 = 2 \times 3 \times 5 \times 11 = 330$

$M_1 = \frac{330}{2} = 165$ $M_2 = \frac{330}{3} = 110$ $M_3 = \frac{330}{5} = 66$

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

$x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 + a_4 y_4 M_4) \bmod m$ — ①

$y_1 = 165^{-1} \bmod 2$

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

Substituting

$1 = 1.165 - 82.2$

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

$\boxed{y_1 = 1}$

$y_2 = 110^{-1} \bmod 3$

$110 = (36)(3) + 2$

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

Substituting

$1 = 1.3 - 1.2$ — ①

$2 = 1.110 - 36.3$

put in ①

$1 = 1.3 - 1(1.110 - 36.3)$

$1 = 1.3 - 1.110 + 36.3$

$1 = 37.3 - 1.110$

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

$y_2 = -1 + 3$

$\boxed{y_2 = 2}$

$y_3 = 66^{-1} \bmod 5$

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

$1 = 1.66 - 13.5$

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

$\boxed{y_3 = 1}$

$y_4 = 30^{-1} \bmod 11$

$30 = (2)(11) + 8$

$11 = (1)(8) + 3$

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

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

Scanned with CamScanner

20K-0208 BCS-3E

Substituting

$1 = 1\cdot 3 - 1\cdot 2$ —— 1

$2 = 1\cdot 8 - 2\cdot 3$

put in 1

$1 = 1\cdot 3 - 1(1\cdot 8 - 2\cdot 3)$

$1 = 1\cdot 3 - 1\cdot 8 + 2\cdot 3$

$1 = 3\cdot 3 - 1\cdot 8$ —— 2

$3 = 1\cdot 11 - 1\cdot 8$

put in 2

$1 = 3(1\cdot 11 - 1\cdot 8) - 1\cdot 8$

$1 = 3\cdot 11 - 3\cdot 8 - 1\cdot 8$

$1 = 3\cdot 11 - 4\cdot 8$ —— 3

$8 = 1\cdot 30 - 2\cdot 11$

put in 3

$1 = 3\cdot 11 - 4(1\cdot 30 - 2\cdot 11)$

$1 = 3\cdot 11 - 4\cdot 30 + 8\cdot 11$

$1 = 11\cdot 11 - 4\cdot 30$

$1 = (11)(11) + (-4)(30)$

$y_4 = -4 + 11$

$\boxed{y_4 = 7}$

put in 1

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

$x = [165 + 440 + 198 + 840] \bmod 330$

$x = 1643 \bmod 330$

$\boxed{x = 323}$

Scanned with CamScanner

QUESTION #16(b):

$x \equiv 3 \pmod 5$, $x \equiv 3 \pmod 6$, $x \equiv 1 \pmod 7$

$x \equiv 0 \pmod{11}$

$\gcd(5,6)=1$ $\gcd(5,7)=1$ $\gcd(5,11)=1$ $\gcd(6,7)=1$

$\gcd(6,11)=1$ $\gcd(7,11)=1$

Hence, the modulos are pairwise primes.

$m = 5 \times 6 \times 7 \times 11 = 2310$

$M_1 = \frac{2310}{5} = 462$, $M_2 = \frac{2310}{6} = 385$, $M_3 = \frac{2310}{7} = 330$, $M_4 = \frac{2310}{11} = 210$

$y_1 = 462^{-1} \bmod 5$

$462 = (92)(5) + 2$

$5 = (2)(2) + 1$

Substituting

$1 = 1.5 - 2.2$ — ①

$2 = 1.462 - 92.5$

put in ①.

$1 = 1.5 - 2(1.462 - 92.5)$

$1 = 1.5 - 2.462 + 184.5$

$1 = 185.5 - 2.462$

$1 = (185)(5) + (-2)(462)$

$y_1 = -2 + 5$

$\boxed{y_1 = 3}$

$y_2 = 385^{-1} \bmod 6$

$385 = (64)(6) + 1$

Substituting

$1 = 1.385 - 64.6$

$\boxed{y_2 = 1}$

$y_3 = 330^{-1} \bmod 7$

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

Substituting

$1 = 1.330 - 47.7$

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

$\boxed{y_3 = 1}$

Dahal

20K-0208 BCS-3E

$y_4 = 210^{-1} \bmod 11$

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

Substituting

$1 = 1 \cdot 210 - 19 \cdot 11$

$\boxed{y_4 = 1}$

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

$x = [4158 + 1155 + 330] \bmod 2310$

$x = 5643 \bmod 2310$

$\boxed{x = 1023}$

He may have 1023 oranges.

QUESTION # 17:

a) $a = 2, m = 17$

$2 = (0)(17) + 2$

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

Substitute

$1 = 1 \cdot 17 - 8 \cdot 2$ — 1

$2 = 1 \cdot 2 - 0 \cdot 17$

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

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

$\boxed{\bar{a} = 11}$

b) $a = 34, m = 89$

$34 = (0)(89) + 34$

$89 = (2)(34) + 21$

$34 = (1)(21) + 13$

$21 = (1)(13) + 8$

$13 = (1)(8) + 5$

$8 = (1)(5) + 3$

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

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

Substituting

$1 = 1 \cdot 3 - 1 \cdot 2$ — 1

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

Wahaj

Scanned with CamScanner

put in 1

$1 = 1.3 - 1(1.5 - 1.3)$

$1 = 1.3 - 1.5 + 1.3$

$1 = 2.3 - 1.5$ — 2

$3 = 1.8 - 1.5$

put in 2

$1 = 2(1.8 - 1.5) - 1.5$

$1 = 2.8 - 2.5 - 1.5$

$1 = 2.8 - 3.5$ — 3

$5 = 1.13 - 1.8$

put in 3

$1 = 2.8 - 3(1.13 - 1.8)$

$1 = 2.8 - 3.13 + 3.8$

$1 = 5.8 - 3.13$ — 4

$8 = 1.21 - 1.13$

put in 4

$1 = 5.(1.21 - 1.13) - 3.13$

$1 = 5.21 - 5.13 - 3.13$

$1 = 5.21 - 8.13$ — 5

$13 = 1.34 - 1.21$

put in 5

$1 = 5.21 - 8(1.34 - 1.21)$

$1 = 5.21 - 8.34 + 8.21$

$1 = 13.21 - 8.34$ — 6

$21 = 1.89 - 2.34$

put in 6

$1 = 13(1.89 - 2.34) - 8.34$

20K-0208 BCS-3E

$1 = 13.89 - 26.34 - 8.34$

$1 = 13.89 - 34.34$ — 7

$34 = 1.34 - 0.89$

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

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

$\boxed{\bar{a} = 55}$

c) $a = 144, m = 233$

$144 = (0)(233) + (144)$

$233 = (1)(144) + 89$

$144 = (1)(89) + 55$

$89 = (1)(55) + 34$

$55 = (1)(34) + 21$

$34 = (1)(21) + 13$

$21 = (1)(13) + 8$

$13 = (1)(8) + 5$

$8 = (1)(5) + 3$

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

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

Substituting

$1 = 1.3 - 1.2$ — 1

$2 = 1.5 - 1.3$

put in 1

$1 = 1.3 - 1(1.5 - 1.3)$

$1 = 1.3 - 1.5 + 1.3$

$1 = 2.3 - 1.5$ — 2

$3 = 1.8 - 1.5$

put in 2

$1 = 2(1.8 - 1.5) - 1.5$

$1 = 2.8 - 2.5 - 1.5$

$1 = 2.8 - 3.5$ — 3

$5 = 1.13 - 1.8$

put in 3

$1 = 2.8 - 3(1.13 - 1.8)$

$1 = 2.8 - 3.13 + 3.8$

$1 = 5.8 - 3.13$ — 4

$8 = 1.21 - 1.13$

put in 4

$1 = 5(1.21 - 1.13) - 3.13$

$1 = 5.21 - 5.13 - 3.13$

$1 = 5.21 - 8.13$ — 5

$13 = 1.34 - 1.21$

put in 5

$1 = 5.21 - 8(1.34 - 1.21)$

$1 = 5.21 - 8.34 + 8.21$

$1 = 13.21 - 8.34$ — 6

$21 = 1.55 - 1.34$

put in 6

$1 = 13(1.55 - 1.34) - 8.34$

$1 = 13.55 - 13.34 - 8.34$

$1 = 13.55 - 21.34$ — 7

$34 = 1.89 - 1.55$

put in 7

$1 = 13.55 - 21(1.89 - 1.55)$

Scanned with CamScanner

20K-0208 BCS-3E

$1 = 13.55 - 21.89 + 21.55$

$1 = 34.55 - 21.89$ — (8)

$55 = 1.144 - 1.89$

put in (8)

$1 = 34(1.144 - 1.89) - 21.89$

$1 = 34.144 - 34.89 - 21.89$

$1 = 34.144 - 55.89$ — (9)

$89 = 1.233 - 1.144$

put in (9)

$1 = 34.144 - 55(1.233 - 1.144)$

$1 = 34.144 - 55.233 + 55.144$

$1 = 89.144 - 55.233$ — (10)

$144 = 1.144 - 0.233$

$1 = (89)(144) + (-55)(233)$

$$\boxed{\bar{a} = 89}$$

d) $a = 200$, $m = 1001$

$200 = (0)(1001) + 200$

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

substitute

$1 = 1.1001 - 5.200$

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

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

$$\boxed{\bar{a} = 996}$$

QUESTION #18(a):

S	T	O	P
18	19	14	15

P	O	L	L	U	T	I	O	N
15	14	11	11	20	19	8	14	13

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

$f(S) = 18 + 4 \pmod{26}$
$= 22 \pmod{26}$
$= 22$ [W]

$f(T) = 19 + 4 \pmod{26}$
$= 23 \pmod{26}$
$= 23$ [X]

$f(O) = 14 + 4 \pmod{26}$
$= 18 \bmod 26$
$= 18$ [S]

$f(P) = 15 + 4 \pmod{26}$
$= 19 \bmod 26$
$= 19$ [T]

$f(L) = 11 + 4 \pmod{26}$
$= 15 \bmod 26$
$= 15$ [P]

$f(U) = 20 + 4 \pmod{26}$
$= 24 \pmod{26}$
$= 24$ [Y]

$f(I) = 8 + 4 \pmod{26}$
$= 12 \pmod{26}$
$= 12$ [M]

$f(N) = 13+4 \pmod{26}$
$= 17 \pmod{26}$
$= 17$ [R]

Message = WXST TSPPYXMSR

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

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

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

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

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

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

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

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

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

Message = NOJK KJGGPODJI

20K-0208 BCS-3E

QUESTION # 18(b):

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

$p = f(p) - 10 \bmod 26$

i) CEBB OXNOBXYG

$f(C) = 2-10 \bmod 26 = (-8+26) \bmod 26 = 18 \bmod 26 = 18$ [S]

$f(E) = (4-10) \bmod 26 = -6+26 \bmod 26 = 20 \bmod 26 = 20$ [U]

$f(B) = 1-10 \bmod 26 = -9+26 \bmod 26 = 17 \bmod 26 = 17$ [R]

$f(O) = 14-10 \bmod 26 = 4 \bmod 26 = 4$ [E]

$f(X) = 23-10 \bmod 26 = 13 \bmod 26 = 13$ [N]

$f(N) = 13-10 \bmod 26 = 3 \bmod 26 = 3$ [D]

$f(Y) = 24-10 \bmod 26 = 14 \bmod 26 = 14$ [O]

$f(G) = 6-10 \bmod 26 = -4+26 \bmod 26 = 22 \bmod 26 = 22$ [W]

$\boxed{\text{Message} = \text{SURRENDER NOW}}$

ii) LO WI PBSOXN

$f(L) = 11-10 \bmod 26 = 1 \bmod 26 = 1$ [B]

$f(O) = 4$ [E]

$f(W) = 22-10 \bmod 26 = 12 \bmod 26 = 12$ [M]

$f(I) = 8-10 \bmod 26 = -2+26 \bmod 26 = 24 \bmod 26 = 24$ [Y]

$f(P) = 15-10 \bmod 26 = 5 \bmod 26 = 5$ [F]

$f(B) = 17$ [R]

$f(S) = 18-10 \bmod 26 = 8 \bmod 26 = 8$ [I]

$f(O) = 4$ [E]

$f(X) = 13$ [N]

$f(N) = 3$ [D]

Wahaj

$\boxed{\text{Message} = \text{BE MY FRIEND}}$

20K-0208 BCS-3E

QUESTION # 19:

$$a^{p-1} \equiv 1 \pmod p$$

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

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

$$5^{6} \equiv 1 \pmod 7 \quad \text{—— (1)}$$

$\Rightarrow$ $a = qd + r$

$$2003 = (333)(6) + 5$$

$\Rightarrow$ $5^{333\times 6 + 5} \pmod 7$

$\Rightarrow$ $(5^{6})^{333} \cdot 5^{5} \pmod 7$

by (1)

$\Rightarrow$ $(1)^{333} \cdot 5^{5} \pmod 7$

$\Rightarrow$ $3125 \pmod 7$ $\Rightarrow$ 3 Ans

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

$$5^{10} \equiv 1 \pmod{11} \quad \text{—— (1)}$$

$\Rightarrow$ $a = qd + r$

$$2003 = (200)(10) + 3$$

$\Rightarrow$ $5^{200\times 10 + 3} \pmod{11}$

$\Rightarrow$ $(5^{10})^{200} \cdot 5^{3} \pmod{11}$

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

$\Rightarrow$ 4 Ans

Waheed

20K-0208 BCS-3E 33

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

$\Rightarrow 5^{12} = 1 \pmod{13}$

$\Rightarrow a = qd + r \quad 2003 = (166)(12) + 11$

$\Rightarrow 5^{166\times12+11} \pmod{13}$

$\Rightarrow (5^{12})^{166} \cdot 5^{11} \pmod{13}$

$\Rightarrow 1 \cdot 48828125 \pmod{13}$

$\Rightarrow 8$ Ans

QUESTION #20 (a):

I LOVE DISCRETE MATHEMATICS

8 11 14 21 4 3 8 18 2 17 4 19 4 12 0 19 7 4 12 0 19 8 2 18

$f(p) = (p+k) \bmod 26$

For caesar cipher, $k = 3$

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

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

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

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

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

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

$f(S) = 18+3 \bmod 26 = 21 \bmod 26 = 21$ [V]

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

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

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

f(M) = 12+3 mod 26 = 15 mod 26 = 15 [P]
f(A) = 0+3 mod 26 = 3 mod 26 = 3 [D]
f(H) = 7+3 mod 26 = 10 mod 26 = 10 [K]

Message = L ORYH GLVFUHWH PDWKHPDWLFV

QUESTION # 20(b):

i) PLG WZR DVVLJQPHQW K=3 [Caesar]
15 11 6 22 25 17 3 21 21 11 9 16 15 7 16 22

f(P) = 15−3 mod 26 = 12 mod 26 = 12 [M]
f(L) = 11−3 mod 26 = 8 mod 26 = 8 [I]
f(G) = 6−3 mod 26 = 3 mod 26 = 3 [D]
f(W) = 22−3 mod 26 = 19 mod 26 = 19 [T]
f(Z) = 25−3 mod 26 = 22 mod 26 = 22 [W]
f(R) = 17−3 mod 26 = 14 mod 26 = 14 [O]
f(D) = 3−3 mod 26 = 0 mod 26 = 0 [A]
f(V) = 21−3 mod 26 = 18 mod 26 = 18 [S]
f(J) = 9−3 mod 26 = 6 mod 26 = 6 [G]
f(Q) = 16−3 mod 26 = 13 mod 26 = 13 [N]
f(H) = 7−3 mod 26 = 4 mod 26 = 4 [E]

Message = MID TWO ASSIGNMENT

20K-0208 BCS-3E

ii) IDVW QXFHV XQLYHUVLWB
8 3 21 22 16 23 5 7 21 23 16 11 24 7 20 21 11 22 1

$f(I) = 8-3 \mod 26 = 5 \mod 26 = 5$ [F]

$f(D) = 0$ [A]

$f(V) = 18$ [S]

$f(W) = 19$ [T]

$f(Q) = 13$ [N]

$f(X) = 23-3 \mod 26 = 20 \mod 26 = 20$ [U]

$f(F) = 5-3 \mod 26 = 2 \mod 26 = 2$ [C]

$f(H) = 4$ [E]

$f(L) = 8$ [I]

$f(Y) = 24-3 \mod 26 = 21 \mod 26 = 21$ [V]

$f(U) = 20-3 \mod 26 = 17 \mod 26 = 17$ [R]

$f(B) = 1-3 \mod 26 = -2+26 \mod 26 = 24 \mod 26$
$= 24$ [Y]

$\boxed{\text{Message} = \text{FAST NUCES UNIVERSITY}}$

QUESTION # 21(a):

i) $h(034567981) = 034567981 \mod 97 = 91$

ii) $h(183211232) = 183211232 \mod 97 = 57$

iii) $h(220195744) = 220195744 \mod 97 = 21$

iv) $h(987255335) = 987255335 \mod 97 = 5$

Wahaj

QUESTION # 21 (b):

i) $h(104578690) = 104578690 \bmod 101 = 58$

ii) $h(432222187) = 432222187 \bmod 101 = 60$

iii) $h(372201919) = 372201919 \bmod 101 = 52$

iv) $h(501338753) = 501338753 \bmod 101 = 3$

QUESTION # 22:

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

$x_{0+1} = x_1 = (4x_0 + 1) \bmod 7 = 13 \bmod 7 = 6$

$x_{1+1} = x_2 = (24+1) \bmod 7 = 25 \bmod 7 = 4$

$x_{2+1} = x_3 = (16+1) \bmod 7 = 17 \bmod 7 = 3$

$x_{3+1} = x_4 = (12+1) \bmod 7 = 13 \bmod 7 = 6$

$x_{4+1} = x_5 = (24+1) \bmod 7 = 25 \bmod 7 = 4$

$x_6 = 3$ | $x_{13} = 6$ | [Constant repitition]
$x_7 = 6$ | $x_{14} = 4$
$x_8 = 4$ | $x_{15} = 3$
$x_9 = 3$ | $x_{16} = 6$
$x_{10} = 6$ | $x_{17} = 4$
$x_{11} = 4$ | $x_{18} = 3$
$x_{12} = 3$ | $x_{19} = 6$

$x_{20} = 4$

20K-0208 BCS-3E

QUESTION # 23(a):

i) 73232184434 Determine 12th digit

$\Rightarrow (7\times3)+3+(2\times3)+3+(2\times3)+1+(8\times3)+4+(4\times3)+3+(4\times3)+x_{12}$

$\Rightarrow 21+3+6+3+6+1+24+4+12+3+12+x_{12}$

$\Rightarrow 95+x_{12}$

For x_{12} to be valid,

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

$x_{12} = -95 \pmod{10}$

$\boxed{x_{12}=5}$

ii) 63623991346 $x_{12}=?$

$\Rightarrow (6\times3)+3+(6\times3)+2+(3\times3)+9+(9\times3)+1+(3\times3)+4+(6\times3)+x_{12}$

$\Rightarrow 18+3+18+2+9+9+27+1+9+4+18+x_{12}$

$\Rightarrow 118+x_{12}$

For x_{12} to be valid,

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

$x_{12} = -118 \pmod{10}$

$\boxed{x_{12}=2}$

20K-0208 BCS-3E

QUESTION #23(b):

i) 036000291452

$\Rightarrow 0+3+(6\times3)+0+0+0+(2\times3)+9+(1\times3)+4+(5\times3)+2$

$\Rightarrow 3+18+6+9+3+4+15+2$

$\Rightarrow 60$

For validity,

$$60 \equiv 0 \pmod{10}$$

$$0 = 0$$

Hence, it is valid.

ii) 012345678903

$\Rightarrow 0+1+(2\times3)+3+(4\times3)+5+(6\times3)+7+(8\times3)+9+0+3$

$\Rightarrow 1+6+3+12+5+18+7+24+9+3$

$\Rightarrow 88$

For validity,

$$88 \equiv 0 \pmod{10}$$

$$8 \neq 0$$

Hence, it is invalid.

20K-0208

20K-0208 BCS-3E

QUESTION # 24(a):

* 0-07-119881

$x_{10} = 0 + 0 + (7\times3) + (1\times4) + (1\times5) + (9\times6) + (8\times7) + (8\times8) + (9\times1) \bmod 11$

$x_{10} = (21+4+5+54+56+64+9) \bmod 11$

$x_{10} = 213 \pmod{11}$

$\boxed{x_{10} = 4}$

QUESTION # 24(b):

* 0-321-500Q1-8

~~$x_{10} = 0 + (2\times3) + (3\times2) + (4\times1) + (5\times5) + 0 + 0 + (8\times Q_1) + \ldots$~~

$x_{10} = 0 + (2\times3) + (3\times2) + (4\times1) + (5\times5) + 0 + 0 + (8\times Q_1) + (9\times1) \bmod 11$

$x_{10} = (6+6+4+25+8Q_1+9) \bmod 11$

$x_{10} = (50+8Q_1) \bmod 11 \equiv 8$

$8 \equiv 6 \bmod 11 + 8Q \bmod 11$

Subtract 6 from b.s

$(\bmod 11)\ 2 = 8Q \bmod 11$ —— (a)

Finding inverse to eliminate 2

$8 = (0)(11) + 8$

$11 = (1)(8) + 3$

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

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

Backward substituting

$1 = 1\cdot3 - 1\cdot2$ —— (1)

$2 = 1\cdot8 - 2\cdot3$

put in (1)

put in ①

$1 = 1.3 - 1(1.8 - 2.3)$

$1 = 1.3 - 1.8 + 2.3$

$1 = 3.3 - 1.8$ — ②

$3 = 1.11 - 1.8$

put in ②

$1 = 3(1.11 - 1.8) - 1.8$

$1 = 3.11 - 3.8 - 1.8$

$1 = 3.11 - 4.8$ — ③

$1 = (3)(11) + (-4)(8)$

$\bar{a} = -4 + 11$

$\boxed{\bar{a} = 7}$

X eq a with $\bar{a}$

$7 \times 8\, Q \bmod 11 = 2 \times 7 \bmod 11$

$Q \bmod 11 = 14 \bmod 11$

$\boxed{Q = 3}$

QUESTION #25:

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

$n = 43.59 = 2537$

$\boxed{C = M^e \bmod n}$

$K = (43-1)(59-1) = 42 \times 58 = 2436$

$e = 13$

pair 1 $= AT = (0019)^{13} \bmod 2537$

pair 2 $= TA = (1900)^{13} \bmod 2537$

pair 3 $= CK = (0210)^{13} \bmod 2537$

Wafa

20K-0208 BCS-3E

QUESTION #26(a):

i) $1, 3, 7, 15, 31$

ii) $\frac{17}{2}, 7, \frac{11}{2}, 4, \frac{5}{2}$

iii) $-1, \frac{1}{4}, \frac{-1}{9}, \frac{1}{16}, \frac{-1}{25}$

iv) $\frac{7}{1}, \frac{10}{3}, \frac{13}{5}, \frac{16}{7}, \frac{19}{9}$

QUESTION #26(b):

i) Arithmetic progression

$a = -15$

$d = -22 + 15 = -7$

$T_n = a + (n-1)d$

$T_{11} = -15 + 10(-7) = -15 - 70$

$\boxed{T_{11} = -85}$

ii) Arithmetic progression

$a = a - 42b \quad d = a - 39b - a + 42b = 3b$

$T_{15} = a + 14d = a - 42b + 14(3b) = a - 42b + 42b$

$\boxed{T_{15} = a}$

iii) Geometric progression

$a = 4 \quad r = \frac{3}{4}$

$\boxed{T_{17} = ar^{n-1} = 4\left(\frac{3}{4}\right)^{16}}$

iv) Geometric ~~Pro~~ progression

$a = 32 \quad r = 1/2$

$T_9 = 32\left(\frac{1}{2}\right)^8 = \frac{32}{256}$

$\boxed{T_9 = \frac{1}{8}}$

Wahaj

20K-0208 BCS-3E

QUESTION #27(a):

i) $T_3 = 10$, $T_5 = \frac{5}{2}$

In G.P, $T_3 = ar^2$

$10 = ar^2$ — (1)

and, $T_5 = ar^4$

$\frac{5}{2} = ar^4$ — (2)

$\div$ (2) by (1)

$\frac{5}{20} = \frac{\cancel{a}r^4}{\cancel{a}r^2} \Rightarrow r^2 = \frac{5}{20}$

$\boxed{r = \sqrt{\frac{5}{20}}}$

put in (1)

${}^{2}\cancel{10} = a \times \frac{\cancel{5}^{1}}{20}$

$\boxed{a = 40}$

Sequence $= 40, 20, 10, 5, \frac{5}{2}, \frac{5}{4}, \ldots$

ii) $T_5 = 8$, $T_6 = -\frac{64}{27}$

$T_5 = ar^4$

$8 = ar^4$ — (1)

$T_6 = ar^5$

$-\frac{64}{27} = ar^5$ — (2)

$\div$ (2) by (1)

Wafa

20K-0208

BCS-3E

$$\frac{-64}{8(27)} = \frac{ar^5}{ar^4}$$

$$\boxed{r = -\frac{8}{27}}$$

put in 1

$$8 = a\left(-\frac{8}{27}\right)^4$$

$$\boxed{a = \frac{531441}{512}}$$

Sequence = $\frac{531441}{512}, -\frac{19683}{64}, \frac{729}{8}, -27, 8, -\frac{64}{27}, \ldots$

QUESTION #27(b):

i) $T_4 = 7$, $T_{16} = 31$

$$T_n = a + (n-1)d$$

$$T_4 = a + 3d$$

$$7 = a + 3d \quad \text{— } ①$$

$$T_{16} = a + 15d$$

$$31 = a + 15d \quad \text{— } ②$$

Subtract 2 by 1

$$31 - 7 = a + 15d - a - 3d$$

$$24 = 12d$$

$$\boxed{d = 2}$$

put in 1

$$7 = a + 3(2) = a + 6$$

$$\boxed{a = 1}$$

Sequence = $1, 3, 5, 7, 9, 11, \ldots$

ii) $T_5 = 86$, $T_{10} = 146$

$T_5 = a + 4d$

$86 = a + 4d$ — (1)

$T_{10} = a + 9d$

$146 = a + 9d$ — (2)

Subtract (2) and (1)

$146 - 86 = a + 9d - a - 4d$

$60 = 5d$

$\boxed{d = 12}$

put in (1)

$86 = a + 4(12) = a + 48$

$\boxed{a = 38}$

Sequence = 38, 50, 62, 74, 86, 98, 110, ...

QUESTION #28(a):

Closest number to 256 divisible by 7 = a = 259

Closest last no. to 789 divisible by 7 = T_n = 784

Common difference = d = 7

To find number of term,

$T_n = a + (n-1)d$

$784 = 259 + (n-1)7$

$525 = 7(n-1)$

$75 = n - 1$

$\boxed{n = 76}$

$Sum = \frac{n}{2}[2a + (n-1)d] = \frac{76}{2}[518 + 525]$

$\boxed{Sum = 39634}$

QUESTION #28(b):

$$a = \frac{1}{n} \qquad l = \frac{n^2 - n + 1}{n}$$

Sum to n terms $= S_n = \frac{n}{2}[a + l]$

$$S_n = \frac{n}{2}\left[\frac{1}{n} + \frac{n^2 - n + 1}{n}\right]$$

$$S_n = \frac{\cancel{n}}{2}\left[\frac{1 + n^2 - n + 1}{\cancel{n}}\right]$$

$$\boxed{S_n = \frac{1}{2}[n^2 - n + 2]}$$

QUESTION #29(a):

$$a_j = \frac{1}{j} \qquad j = 1, 2, 3, \ldots$$

$n = 100$

$$\Rightarrow \sum_{K=1}^{100} \frac{1}{K}$$

QUESTION #29(b):

i) $\sum_{K=4}^{8} (-1)^K = (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8 = 1 - 1 + 1 - 1 + 1 = \underline{1}$

ii) $\sum_{j=1}^{5} (j)^2 = (1)^2 + (2)^2 + (3)^2 + (4)^2 + (5)^2 = 1 + 4 + 9 + 16 + 25 = 55$

20K-0208 BCS-3E

QUESTION #30: first six terms

a) $a_n = -2a_{n-1}$, $a_0 = -1$

$a_1 = -2a_0 = -2(-1) = 2$

$a_2 = -2a_1 = -2(2) = -4$

$a_3 = -2a_2 = -2(-4) = 8$

$a_4 = -2a_3 = -2(8) = -16$

$a_5 = -2a_4 = -2(-16) = 32$

$a_6 = -2a_5 = -2(32) = -64$

b) $a_n = a_{n-1} - a_{n-2}$, $a_0 = 2$, $a_1 = -1$

$a_2 = a_1 - a_0 = -1 - 2 = -3$

$a_3 = a_2 - a_1 = -3 + 1 = -2$

$a_4 = a_3 - a_2 = -2 + 3 = 1$

$a_5 = a_4 - a_3 = 1 + 2 = 3$

$a_6 = a_5 - a_4 = 3 - 1 = 2$

c) $a_n = 3a_{n-1}^2$, $a_0 = 1$

$a_1 = 3a_0^2 = 3(1)^2 = 3$

$a_2 = 3a_1^2 = 3(3)^2 = 3(9) = 27$

$a_3 = 3a_2^2 = 3(27)^2 = 3(729) = 2187$

$a_4 = 3a_3^2 = 3(2187)^2 = 3(4782969) = 14348907$

$a_5 = 3a_4^2 = 3(14348907)^2 = 6.176 \times 10^{14}$

$a_6 = 3a_5^2 = 3(6.176 \times 10^{14})^2 = 1.144 \times 10^{30}$

@ahy

20K-0208 BCS-3E

d) $a_n = na_{n-1} + a_{n-2}^2$, $a_0 = -1$, $a_1 = 0$

$a_2 = 2a_1 + a_0^2 = 2(0) + (-1)^2 = 1$

$a_3 = 3a_2 + (a_1)^2 = 3(1) + (0)^2 = 3$

$a_4 = 4a_3 + (a_2)^2 = 4(3) + (1)^2 = 12 + 1 = 13$

$a_5 = 5a_4 + (a_3)^2 = 5(13) + (3)^2 = 65 + 9 = 74$

$a_6 = 6a_5 + (a_4)^2 = 6(74) + (13)^2 = 444 + 169 = 613$

QUESTION # 31(a):

Proof by exhaustion,

$\exists x[(x > 5) \to 2^x - 1 \text{ is prime}]$

Let $n = 7$, by trivial proof

$2^n - 1 = 2^7 - 1 = 128 - 1 = 127$

Since, 127 is a prime number, the statement is true.

QUESTION # 31(b):

Prove by contradiction

Contradictive statement => if $p|a$, then $p|(a+1)$

Let k be an integer such that

$$\frac{a}{p} = k$$

$$a = kp \quad \text{—} (1)$$

Let s be an integer such that

$$\frac{a+1}{p} = s$$

$$a+1 = ps \quad \text{—} (2)$$

Wafaf

Scanned with CamScanner

Subtract eq ② and ①

$a+1-a = ps-kp$

$1 = p(s-k)$

Let $r=s-k$ since both are integers

$1=pr$

$\frac{1}{p}=r$

This statement says that p divides 1, which is impossible since primes are always greater than 1. Hence, our supposition is false.

So, the given statement is true.

QUESTION #32(a):

Proof by exhaustion,

$\sqrt{a+b} = \sqrt{a}+\sqrt{b}$

Let $a=16$ and $b=0$.

$\sqrt{16+0} = \sqrt{16}+\sqrt{0}$

$4=4$

Hence, the there are real numbers such that $\sqrt{a+b} = \sqrt{a}+\sqrt{b}$.

QUESTION #32(b):

Proof by cases,

i) x is +ve ii) x is -ve

i) Let $x=5$ ii) Let $x=-5$

$|5|=5>1$ $|-5|=5>1$

Hence, the statement is true.

Wahaj

QUESTION #33(a):

For every prime, n+2 is prime.

By counter example,

$$\text{Let } n=2$$
$$n+2=2+2$$
$$n+2=4$$

Since, 4 is not a prime number, the statement is disproved.

QUESTION #33(b):

Proof by contradiction,

the set of prime numbers is finite.

Let $S=\{P_1,P_2,\ldots,P_n\}$ be the set of all ~~of~~ prime numbers.

Let x be the sum of all elements of S.

$$x=P_1 \times P_2 \times \ldots \times P_n$$

Now add 1 to ~~set~~ x,

$$x=x+1$$

Now, if this number x is divided by any of the ~~new~~ primes in the list, the remainder will be 1. So, this new number is either a prime proving our supposition wrong or it is a composite such that there is a prime factor of this number which is not in the list, hence our supposition is wrong.

So, original statement is true.

Wahaj

20K-0208 BCS-3E

QUESTION #34(a):

By contradiction,

if n and m are odd, then n+m is odd integer.

Let $m=2k+1$ and $n=2k+1$ be two odd integers.

$$m+n = 2k+1+2k+1$$

$$m+n = 4k+2$$

$$m+n = 2(2k+1)$$

Let $r=2k+1$ is an integer

$$m+n = 2r$$

Since, 2r stands for even numbers, our supposition is wrong and the original statement is true.

QUESTION #34(b):

By contraposition,

If m is odd ~~or~~ and n is even, m+n is odd.

Let $m=2k+1$ be an odd integer.

Let $n=2k$ be an even integer.

$$m+n = 2k+1+2k$$

$$m+n = 4k+1$$

$$m+n = 2(2k)+1$$

Let $r=2k$ be an integer

$$m+n = 2r+1$$

Since, 2r+1 is odd and the contrapositive is true, the original statement is also true.

20K-0208 BCS-3E

QUESTION #35(a):

By contradiction,

$6-7\sqrt{2}$ is rational.

Since, rational numbers are $x = p/q$.

$$6-7\sqrt{2} = \frac{p}{q}$$

$$6-\frac{p}{q} = 7\sqrt{2}$$

$$\frac{6q-p}{q} = 7\sqrt{2}$$

$$\frac{6q-p}{7q} = \sqrt{2}$$

According to this statement, $\frac{6q-p}{7q}$ is rational but $\sqrt{2}$ is irrational, hence our supposition is wrong and the original statement was true.

QUESTION #35(b):

By contradiction,

$\sqrt{2}+\sqrt{3}$ is rational.

For rational numbers, the squares of their sum is also rational, so

$$\Rightarrow (\sqrt{2}+\sqrt{3})^2 \Rightarrow 2+3+2\sqrt{6}$$

$$\Rightarrow 5+2\sqrt{6}$$

From this statement, it can be seen that $\sqrt{6}$ is an irrational number so the sum must be irrational hence our supposition was wrong and the original statement is true.

QUESTION #36(a):

Base case => $n=1$

$$n = \frac{1(\cancel{2})(\cancel{3})}{\cancel{6}\,3}$$

$1=1$ proved.

Inductive case =>

Let $n=k$,

$$1^2+2^2+3^2+\ldots+k^2=(k(k+1)(2k+1))/6 \quad \text{—— (1)}$$

Let $n=k+1$

$$1^2+2^2+3^2+\ldots+(k+1)^2=\left[\frac{(k+1)(k+2)\{2(k+1)+1\}}{6}\right]$$

$$=\left[\frac{(k+1)(k+2)(2k+3)}{6}\right] \quad \text{—— (2)}$$

Add $(k+1)^2$ on both sides of eq (1)

$$1^2+2^2+3^2+\ldots+k^2+(k+1)^2=\left[\frac{(k)(k+1)(2k+1)}{6}\right]+(k+1)^2$$

$$=\frac{(k)(k+1)(2k+1)+6(k+1)^2}{6}$$

$$=(k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right]$$

$$=(k+1)\left[\frac{2k^2+k+6k+6}{6}\right]=\frac{(k+1)(2k^2+7k+6)}{6}$$

$$=\frac{(k+1)(2k^2+3k+4k+6)}{6}=\frac{(k+1)\{k(2k+3)+2(2k+3)\}}{6}$$

$$=\frac{(k+1)(k+2)(2k+3)}{6} \quad \text{—— (3)}$$

eq (2) = eq (3) Hence, proved!

20K-0208 BCS-3E

QUESTION #36(b):

Base case => $n=0$,

$$1 = 2^1 - 1$$
$$1 = 2 - 1$$
$$1 = 1 \text{ proved}$$

Inductive case =>

Let $n = k$,

$$1 + 2 + 2^2 + \dots + 2^k = 2^{k+1} - 1 \quad \text{—— (1)}$$

Let $n = k+1$,

$$1 + 2 + 2^2 + \dots + 2^{k+1} = 2^{k+1+1} - 1$$
$$= 2^{k+2} - 1 \quad \text{—— (2)}$$

Add 2^{k+1} on both sides of eq (1)

$$1 + 2 + 2^2 + \dots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1}$$
$$= 4^{k+1} - 1$$
$$= 2 \cdot 2^{k+1} - 1$$
$$= 2^{k+1+1} - 1$$
$$= 2^{k+2} - 1 \quad \text{—— (3)}$$

Since eq (2) = eq (3),

Hence proved!

20K-0208 BCS-3E

QUESTION #36(c):

Base case, $n = 1$

$$1 = \frac{1}{4}(1)(2)^2$$

$$1 = \frac{4}{4}$$

$$1 = 1 \quad \text{proved!}$$

Inductive case,

Let $n = k$

$$1^3 + 2^3 + 3^3 + \dots + k^3 = \frac{1}{4}k^2(k+1)^2 \quad \text{—— (1)}$$

Let $n = k+1$

$$1^3 + 2^3 + 3^3 + \dots + (k+1)^3 = \frac{1}{4}(k+1)^2(k+2)^2 \quad \text{—— (2)}$$

Adding $(k+1)^3$ on both sides of eq (1)

$$1^3 + 2^3 + 3^3 + \dots + k^3 + (k+1)^3 = \cancel{\frac{1}{4}(k+1)^2(k+2)^2 + (k+1)^3}\ \frac{1}{4}k^2(k+1)^2 + (k+1)^3$$

$$\cancel{= (k+1)^2\left[\frac{1}{4}(k+2)^2 + k+1\right]}$$

$$\Rightarrow (k+1)^2\left[\frac{1}{4}k^2 + k + 1\right]$$

$$\Rightarrow (k+1)^2\left[\frac{k^2+4k+4}{4}\right]$$

$$\Rightarrow \frac{1}{4}(k+1)^2(k+2)^2 \quad \text{—— (3)}$$

Since, eq (2) = eq (3)

Hence, proved!

BCS-3E 20K-0208

QUESTION #37:

a) i) to construct computer programs.
~~ii) to understand system specification~~
ii) designing hardware

b) i) to ~~spe~~ write and understand system specifications.
ii) drawing conclusions from premises.

c) i) determining if something belongs somewhere.
ii) The concept of big data is based on studying large data[sets].

d) i) handling input-output situations.
ii) calculating tax money on basis of salary.

e) ~~i) Functions are used in Hashing to determine memory blocks for values.~~
i) Relations help to map pairs onto graphs.
ii) They help in deriving inferences to other relations.

f) i) They are used in business and financial analysis to assist in decision making.
ii) They help in quantitative analysis.

g) i) climbing a ladder requires knowledge of getting through the first step. The rest are inductively increasing steps.
ii) The determination if a popper zip can be zipped if the first teeth is successfully zipped.