ASSIGNMENT #3

Name: HERMAIN QADIR
ID: 19K-1517
Section: H

Question #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) ~~Ref~~ Reflexive as it has $(a,a), (b,b), (c,c), (d,d)$.

b) Not symmetric as it does not have (c,a) (d,a) but has (a,c) & (a,d).

c) Not Antisymmetric as it has both (b,c) and (c,b) and both (b,d) & (d,b).

d) Not Transitive as it has (a,d) and (d,b) but not (a,b).

e) Not irreflexive as it has all four $\Rightarrow (a,a), (b,b), (c,c)$ & (d,d)

f) Not ~~anti~~ asymmetric as it is neither irreflexive nor antisymmetric.

QUESTION #2:

a) Reflexive since $a=b$, then $\{\lfloor a \rfloor = \lfloor b \rfloor$ for all real nos.

b) Symmetric since $a=b$, then $b=a$

c) Not Antisymmetric as $(2.2, 2.3) \in R$ and $(2.3, 2.2) \in R$ but $2.2 \neq 2.3$

d) Transitive. because $(a,b), (b,c) \in R$ then $(a,c) \in R$

e) Not Irreflexive because it is reflexive

f) Not ~~Asy~~symmetric as it is neither irreflexive nor irreflexive.

Question #3: (0, 1, 2, 3, 4), (0, 1, 2, 3).

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

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

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

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

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

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

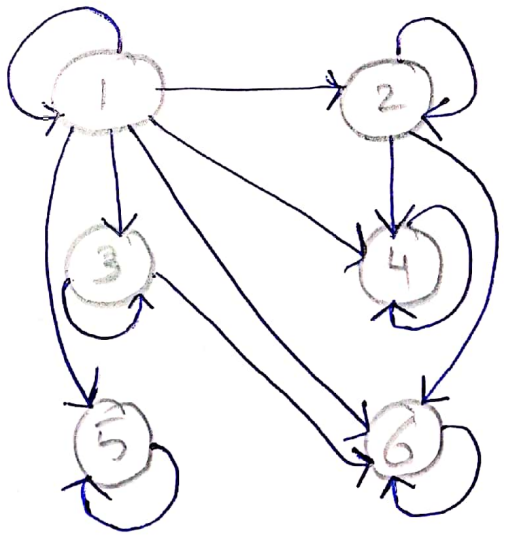
f) $R = \{(1,2), (2,1), (2,2)\}$

Question #4:

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

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

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



Question #5:

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

→ Not reflexive as $(1,1), (4,4) \notin R$
→ Not symmetric as $(2,4), (3,4) \in R$ but $(4,2), (4,3) \notin R$.
→ Not antisymmetric as $(2,3) \in R$ and $(3,2) \in R$.
→ It is transitive.

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

→ Reflexive as $(1,1), (2,2), (3,3), (4,4) \in R$.
→ Symmetric as $(1,2) \in R$ and $(2,1) \in R$.
→ Not antisymmetric.
→ Transitive

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

→ Not reflexive as $(1,1), (2,2), (3,3), (4,4) \notin R$
→ Symmetric as $(2,4) \in R$ and $(4,2) \in R$.
→ Not antisymmetric
→ Not transitive as $(2,2) \notin R$.

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

→ Not reflexive as $(1,1), (2,2), (3,3), (4,4) \notin R$.
→ Not symmetric as $(2,1), (3,2), (4,3) \notin R$.
→ Antisymmetric
→ Not transitive as $(1,3) \notin R$.

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

→ Reflexive
→ Symmetric
→ Antisymmetric
→ Transitive.

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

→ Not reflexive as $(1,1),(2,2),(3,3),(4,4) \notin R$.
→ Not symmetric as $(4,1),(3,2),(4,3),(4,2) \notin R$.
→ Not antisymmetric as $(1,3) \in R$ and $(3,1) \in R$.
→ Not transitive as $(1,1) \notin R$ and both $(1,3) \nexists (3,1) \in R$.

Question #6:

a) Not reflexive as $\nexists a \neq b$.
Not symmetric $(a,b) \in R$ but $(b,a) \notin R$.
Antisymmetric as it is not symmetric.
Irreflexive because $\nexists a \neq b$. in any pair (a,b).
Asymmetric as it's both antisymmetric $\nexists$ irreflexive.
Transitive because $(a,b) \in R \nexists (b,c) \in R$ then $(a,c) \in R$.

b) Reflexive, because $a=b$ as a person share birthdate with himself.
Symmetric because $(a,b) \in R$ and so is (b,a)
Not Antisymmetric
Not Irreflexive
Transitive if ~~a=b~~ a & b's born on same day as b and be is born on same day as c, then $(a,c) \in R$.
Not asymmetric as it's neither antisymmetric nor irreflexive.

c) → Reflexive since (a,a) exists.
→ Symmetric since if a has same last name as b, $(a,b) \in R$ and $(b,a) \in R$.
→ Antisymmetric → no because it is symmetric.
→ Transitive since a, b has the same last name, and if (b,c) has the same name, then $(a,c) \in R$.
→ Irreflexive = no, because it is reflexive.
→ Asymmetric = no, since it is neither irreflexive nor ~~neither~~ antisymmetric.

d) Reflexive because (a,a) exists.
Symmetric because $(a,b) \in R$ and $(b,a) \in R$.
Not Antisymmetric as it is symmetric
Transitive because if $(a,b),(b,c) \in R$ then $(a,c) \in R$.
Not Irreflexive since it is reflexive.
Not asymmetric since it is neither irreflexive nor antisymmetric

Question #7:

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

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

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

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

Question #8:

$R1 = \{(2,1), (3,1), (3,2)\}$

$R2 = \{(1,1), (2,2), (3,3), (2,1), (3,1), (3,2)\}$

$R3 = \{(1,2), (1,3), (2,3)\}$

$R4 = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$

$R5 = \{(1,1), (2,2), (3,3)\}$

$R6 = \{(1,2), (2,1), (1,3), (3,1), (2,3), (3,2)\}$

a) $R2 \cup R4 = \{(1,1), (1,2), (1,3), (2,2), (2,1), (2,3), (3,1), (3,2), (3,3)\}$

b) $R3 \cup R6 = \{(1,2), (1,3), (2,1), (2,3), (3,1), (3,2)\}$

c) $R3 \cap R6 = \{(1,2), (1,3), (2,3)\}$

d) $R4 \cap R6 = \{(1,2), (1,3), (2,3)\}$

e) $R3 - R6 = \{\}$.

f) $R6 - R3 = \{(2,1), (3,1), (3,2)\}$

g) $R2 \oplus R6 = (R2 - R6) \cup (R6 - R2)$

$R2 - R6 = \{(1,1), (2,2), (3,3)\}$

$R6 - R2 = \{(1,2), (1,3), (2,3)\}$

$\therefore R2 \oplus R6 = \{(1,1), (2,2), (3,3), (1,2), (1,3), (2,3)\}$

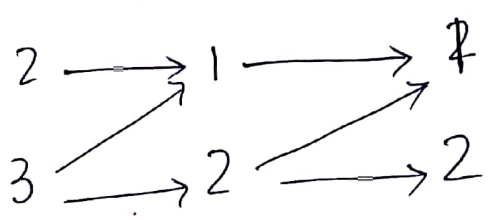
h) $R3 \oplus R5 = (R3 - R5) \cup (R5 - R3)$.

$R3 - R5 = \{(1,2), (1,3), (2,3)\}$

$R5 - R3 = \{(1,1), (2,2), (3,3)\}$

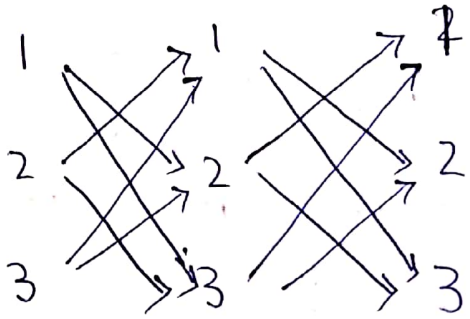
$R3 \oplus R5 = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$

i)



$R2 \circ R1 = \{(2,1), (3,1), (3,2)\}$

j)



2,1,2
2,1,3
2,3,1
2,3,2.

$R6 \circ R6 = \{(1,1), (1,3), (1,2), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$

Question #9:

Part a:

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

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

Part 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) R is a relation on the set of ~~integers~~ English alphabets such aRb if and only if $l(a) = l(b)$ where $l(x)$ is the length of string x.

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

→ Symmetry: Since $l(a) = l(b)$, then $l(b) = l(a)$ also holds and bRa.

→ Transitivity: Suppose aRb and bRc, Since $l(a) = l(b)$ and $l(b) = l(c)$, so $l(a) = l(c)$ also holds and aRc.

b) $a \equiv b \pmod m$ if and only if m divides $a-b$.

→ Reflexivity: If $a \equiv a \pmod m$, $a - a = 0$ and m divides 0 to give integer 0.

→ Symmetry: Suppose that $a \equiv b \pmod m$. Then $a-b$ is divisible by m, and so $a - b = km$ where k is an integer. If $b \equiv a \pmod{}$, $b-a$ divided by will result in $b - a = (-k)m$.

→ Transitivity: Suppose that $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Then m divides both $a-b$ and $b-c$. Hence, these are integers k and l with $a - b = km$, and $b - c = lm$. We By adding equations, we obtain $a - c = km + lm$

$a - c = m(k + l)$, so

$\therefore a \equiv c \pmod m$

c) If $a \equiv b \pmod m$, then m divides $a - b$.

$m \mid a - b = km$ where k is an integer belonging to $\mathbb{Z}$

let $a \bmod m = c$.

then $a = mq + c$ and q is quotient belonging to $\mathbb{Z}$.

$a - b = km$

$mq + c - b = km$

$mq - km + c = b$.

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

This shows that c is the remainder when b is divided by m so $b \bmod m = c = a \bmod m$. Therefore if $a \equiv b \pmod m$ then $a \pmod m = b \pmod m$.

Conversely, assume $a \bmod m = b \pmod m$.

→ $c = a \pmod m = b \pmod m$

→ $a = mq_1 + c$

→ $b = mq_2 + c$

Then $a - b = m(q_1) + r - (mq_2 + r)$

$mq_1 + r = mq_2 - r$

$mq_1 - mq_2 =$

$m(q_1 - q_2)$.

Question # 11:

a) 19 is divided by 7.

$q = 19 \text{ div } 7 \Rightarrow \boxed{2}$

$r = 19 \bmod 7 \Rightarrow \boxed{5}$

b) -111 divided by 11.

$q = 11 \times -11 \Rightarrow -121$

$q = \boxed{-11}$

$r = 121 - 111 = \boxed{10}$

c) 789 divided by 23

$q = 789 \text{ div } 23 \Rightarrow \boxed{34}$

$r = 789 \bmod 23 \Rightarrow$

$23 \times 34 = 782$

$789 - 782 \Rightarrow \boxed{7}$

d) 1001 divided by 13

$q = 1001 \text{ div } 13 = \boxed{77}$

$r = 13 \times 77 = 1001$

$\therefore \boxed{r = 0}$

e) 10 divided by 19

$\boxed{q = 0}$

$\boxed{r = 10}$

f) 3 is divided by 5

$q = 0$

$r = 3$

g) -1 divided by 3.

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

$q = -1$

$r = 2$

h) 4 divided by 1

$q = 4$

$r = 0.$

Question #12:

a).

i) -111 div $99 = -2$

$-111 \bmod 99 \Rightarrow 99(-2) \Rightarrow -198$

$\Rightarrow 198 - 111 = 87$

ii) -9999 div $101 =$

$101 \times -99 = -9999$

$-99.$

$-9999 \bmod 101 = 0.$

iii) 10299 div $999 \Rightarrow 10$

$10299 \bmod 999.$

$999 \times 10 = 9990.$

$10299 - 9990 = 309$

iv) 123456 div 1001 => 123

1001 × 123 => 123123

123456 − 123123 = 333 a mod m.

Part b:

i) $80 \equiv 5 \pmod{17}$.

80 − 5 = 75.

~~75~~ / 17 / 75

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

ii) $103 \equiv 5 \pmod{17}$

103 − 5 = 98

17 | 98 => $\frac{98}{17}$ ≠ an integer.

∴ $103 \not\equiv 5 \pmod{17}$.

iii) $-29 \equiv 5 \pmod{17}$.

−29 − 5 = −34.

17 | −34 => −2.

∴ $29 \equiv 5 \pmod{17}$

iv) $-122 \equiv 5 \pmod{17}$

−122 − 5 = −127.

17 / −127 => $\frac{-127}{17}$ ≠ an integer.

∴ $-122 \not\equiv 5 \pmod{17}$.

Question #13:

Part a)

i) 11, 15, 19

gcd(11, 15)

$15 = (1)11 + 4$

$11 = (2)4 + 3$

$4 = (1)3 + 1$ ← GCD

$3 = (3)1 + 0$

↳ GCD.

gcd(11, 19)

$19 = (1)11 + 8$

$11 = (1)8 + 3$

$8 = (2)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd(15, 19)

$19 = (1)15 + 4$

$15 = (3)4 + 3$

$4 = (1)3 + 1$

$3 = (3)1 + 0$

↳ GCD.

∴ pairwise relatively prime.

ii) 14, 15, 21

gcd(15, 21)

$21 = (1)15 + 6$

$15 = (2)6 + 3$

$6 = (2)3 + 0$

↳ GCD(15, 21) = 3 ∴ not pairwise relatively prime.

iii) 12, 17, 31, 37

gcd(12, 17)

$17 = (1)12 + 5$

$12 = (2)5 + 2$

$5 = (2)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd(12, 31) = 1

$31 = (2)12 + 7$

$12 = (1)7 + 5$

$7 = (1)5 + 2$

$5 = (2)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd (12, 37)

$37 = 12(3) + 1$

$3 = (3)1 + 0$

↳ GCD.

gcd (17, 37)

$37 = (2)17 + 3$

$17 = (5)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd (17, 31)

$31 = (1)17 + 14$

$17 = (1)14 + 3$

$14 = (4)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd (31, 37)

$37 = (1)31 + 6$

$31 = (5)6 + 1$

$6 = (6)1 + 0$

↳ GCD.

∴ pairwise relatively prime.

(v) 7, 8, 9, 11

gcd (7, 8)

$8 = (1)7 + 1$

$7 = (7)(1) + 0$

↳ GCD

gcd (7, 9)

$9 = (1)7 + 2$

$7 = (3)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd (7, 11)

$11 = (1)7 + 4$

$7 = (1)4 + 3$

$4 = (1)3 + 1$

$3 = (3)1 + 0$

↳ GCD

gcd (8, 9)

$9 = (1)8 + 1$

$8 = (8)1 + 0$

↳ GCD

gcd (9, 11)

$11 = (1)9 + 2$

$9 = (4)2 + 1$

$2 = (2)1 + 0$

↳ GCD

gcd (8, 11)

$11 = (1)8 + 3$

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

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

∴ pairwise relatively prime.

Part b:

i)

2	88
2	44
2	22
11	11
	1

$\Rightarrow 88 = \boxed{2^3 \times 11}$

ii)

2	126
3	63
3	21
7	7
	1

$\Rightarrow \boxed{2 \times 3^2 \times 7}$

iii)

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

$729 \Rightarrow \boxed{3^6}$

iv)

7	1001
11	143
13	13
	1

$\Rightarrow \boxed{7 \times 11 \times 13}$

v)

11	1111
101	101
	1

$\Downarrow$

$\boxed{11 \times 101}$

vi)

3	909
3	303
101	101
	1

$\Downarrow$

$\boxed{3^2 \times 101}$

Question #14:

gcd (144, 89)

$144 = (1)89 + 55$

$89 = (1)55 + 34$

$55 = (1)34 + 21$

$34 = (1)21 + 13$

$21 = (1)13 + 8$

$13 = (1)8 + 5$

$8 = (1)5 + 3$

$5 = (1)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

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

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

$\Rightarrow -1 \cdot 5 + 2 \cdot 3$

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

$2 \cdot 8 - 3 \cdot 5$

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

$-3 \cdot 13 + 5 \cdot 8$

$-3 \cdot 13 + 5 \cdot (21 - 1 \cdot 13)$

$5 \cdot 21 - 8 \cdot 13$

$5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21)$

$-8 \cdot 34 + 13 \cdot 21$

~~$-8 \cdot 34 + 14 \cdot (55 - 1 \cdot 34)$~~

~~$+14 \cdot 55 \quad -22 \cdot 34$~~

~~$+14 \cdot 55 \quad -22 \cdot (89 - 1 \cdot 55)$~~

~~$6 \cdot 89 \quad -20 \cdot 55$~~

~~$6 \cdot 89 \quad -20 \cdot (144 - 1 \cdot 89)$~~

~~$-20 \cdot 144 \quad +26 \cdot 89$~~

$-8 \cdot 34 + 13 \cdot (55 - 1 \cdot 34)$

$13 \cdot 55 \quad -21 \cdot 34$

$13 \cdot 55 \quad -21 \cdot (89 - 1 \cdot 55)$

$-21 \cdot 89 + 34 \cdot 55$

~~$14 \cdot 55 \quad -22 \cdot (89 - 1 \cdot 55)$~~

~~$-22 \cdot 89 + 36 \cdot 55$~~

~~$-22 \cdot 89 + 36 \cdot (144 - 1 \cdot 89)$~~

$-21 \cdot 89 + 34 \cdot (144 - 1 \cdot 89)$

$34 \cdot 144 \quad -55 \cdot 89$

$1 = (34)(144) + (-55)(89)$

gcd (1001, 100001)

$100001 = (99)1001 + 902$

$1001 = (1)902 + 99$

$902 = (9)99 + 11$

$99 = (9)11 + 0$

gcd = 11

$11 = 1 \cdot 902 - 9 \cdot 99$

$11 = 1 \cdot 902 - 9 \cdot (1001 - 1 \cdot 902)$

$-9 \cdot 1001 + 10 \cdot 902$

~~$-9 \cdot 1001 + 10 \cdot (100001 -$~~

$-9 \cdot 1001 + 10(100001 - 99 \cdot 1001)$

$\therefore 11 = 10(100001) + (-999)(1001)$

Question #15:

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

gcd(55, 89)

$89 = (1)55 + 34$

$55 = (1)34 + 21$

$34 = (1)21 + 13$

$21 = (1)13 + 8$

$13 = (1)8 + 5$

$8 = (1)5 + 3$

$5 = (1)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD(55, 89) = 1

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

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

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

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

$= 2 \cdot 8 - 3 \cdot 5$

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

$-3 \cdot 13 + 5 \cdot 8$

$= -3 \cdot 13 + 5 \cdot (21 - 1 \cdot 13)$

$= 5 \cdot 21 - 8 \cdot 13$

$= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21)$

$= -8 \cdot 34 + 13 \cdot 21$

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

$= 13 \cdot 55 - 21 \cdot 34$

$13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55)$

$-21 \cdot 89 + 34 \cdot 55$

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

So inverse is:

$\boxed{34}$

Bezout's Coefficients:

34 & -21

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

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

$x = 1156 \bmod 89$

$x = 89(1156) - (89)(12)$

$\boxed{x = 88}$

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

$\gcd(89, 232)$

$232 = (2)89 + 54$

$89 = (1)54 + 35$

$54 = (1)35 + 19$

$35 = (1)19 + 16$

$19 = (1)16 + 3$

$16 = (5)3 + 1$

$3 = (3)1 + 0$

$\boxed{\gcd(89, 232) = 1}$

Backwards substitution:

$1 = 16 - 5 \cdot 3$

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

$-5 \cdot 19 + 6 \cdot 16$

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

$6 \cdot 35 - 11 \cdot 19$

$6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35)$

~~$6 \cdot 35$~~

$-11 \cdot 54 + 17 \cdot 35$

$-11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54)$

$17 \cdot 89 - 28 \cdot 54$

$17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89)$

$-28 \cdot 232 + 73 \cdot 89$

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

Bezout's Coefficients = 73 & -28

Inverse = 73

$89 \times 73x = (1 \times 73) \pmod{232}$

$x = 146 \bmod 232$

$\boxed{x = 146}$

Question #16:

Part a:

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

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

$M_1 = \frac{210}{5}$, $M_2 = \frac{210}{6}$, $M_3 = \frac{210}{7}$

$M_1 = 42$, $M_2 = 35$, $M_3 = 30$

$y_1 = \overline{42} \bmod 5$

$42 = (8)5 + 2$

$5 = (2)2 + 1$

$2 = (2)1 + 0$

↳ GCD

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

$1 = 1 \cdot 5 - 2 \cdot (42 - 8 \cdot 5)$

$1 = -2 \cdot 42 + 17 \cdot 5$

$1 = (17)(5) + (-2)(42)$

Inverse of $\overline{42}$ mod $= -2$

$= -2 + 5$

$\boxed{3}$

$y_2 = \overline{35} \bmod 6$

$35 = (5)6 + 5$

$6 = (1)5 + 1$

$5 = (5)1 + 0$

$\hookrightarrow$ GCD.

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

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

$1 = -1 \cdot 35 + 6 \cdot 6$

Inverse of $\overline{35} = -1$

$= -1 + 6 \Rightarrow 5$

$y_3 = \overline{30} \bmod 7$

$30 = (4)7 + 2$

$7 = (3)2 + 1$

$2 = (2)1 + 0$

$\hookrightarrow$ GCD

$1 = 1 \cdot 7 - 3 \cdot 2$

$1 = 1 \cdot 7 - 3 \cdot (30 - 4 \cdot 7)$

$1 = -3 \cdot 30 + 13 \cdot 7$

$\overline{30} = -3$

$= -3 + 7 \Rightarrow \boxed{4}$

$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 y_3 M_3) \bmod m$

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

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

$x = 836 \bmod 210$

$= 836 - 210(3)$

$x = \boxed{206}$

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

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

$m = 2 \times 3 \times 5 \times 11 = \underline{330}$

$M_1 = \frac{330}{2}$, $M_2 = \frac{330}{3}$, $M_3 = \frac{330}{5}$, $M_4 = \frac{330}{11}$

$M_1 = 165$, $M_2 = 110$, $M_3 = 66$, $M_4 = 30$

$y_1 = \overline{165} \bmod 2$

$165 = (82)2 + 1$

$2 = (2)1 + 0$

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

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

$\overline{165} = \boxed{1}$ y_1

$y_2 = \overline{110} \bmod 3$

$110 = (36)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

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

$1 = 1 \cdot 3 - 1 \cdot (110 - 36 \cdot 3)$

$1 = -1 \cdot 110 + 37 \cdot 3$

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

$\overline{110} = -1$

$= -1 + 3 = \boxed{2}$ y_2

$y_3 = \overline{66} \bmod 5$

$66 = (13)5 + 1$

$5 = (5)1 + 0$

↳ GCD

$1 = 1 \cdot 66 - 13 \cdot 5$

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

$y_3 = \boxed{1}$

$y_4 = \overline{30} \bmod 11$

$30 = (2)11 + 8$

$11 = (1)8 + 3$

$8 = (2)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

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

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

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

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

$3 \cdot 11 - 4 \cdot 8$

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

$-4 \cdot 30 + 11 \cdot 11$

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

Inverse $= -4$

$= -4 + 11 = \boxed{7}$ y_4

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

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

$$x = (165 + 440 + 198 + 840) \bmod 330$$

$$x = 1643 \bmod 330$$

$$x = 1643 - 330(4)$$

$$\boxed{x = 323}$$

Part b:

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

$x = 0 \pmod{11}$

$a_1 = 3$, $a_2 = 3$, $a_3 = 7$, $a_4 = 0$

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

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

$M_1 = 462$, $M_2 = 385$, $M_3 = 330$, $M_4 = 210$

$y_1 = \overline{462} \bmod 5$

$462 = (92)5 + 2$

$5 = (2)2 + 1$

$2 = (2)1 + 0$

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

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

$1 = -2 \cdot 462 + 185 \cdot 5$

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

Inverse $= -2$

$= -2 + 5 = \boxed{3}$ y_1

$y_2 = \overline{385} \bmod 6$

$385 = (64)6 + 1$

$6 = (6)1 + 0$

↳ GCD

$1 = 1 \cdot 385 - 64 \cdot 6$

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

Inverse $= \boxed{1}$ y_2

$y_3 = \overline{330} \bmod 7$

$330 = (47)7 + 1$

$7 = (7)1 + 0$

↳ GCD

$1 = 1 \cdot 330 - 47 \cdot 7$

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

Inverse = $\boxed{1}\ y_3$

$x = \left((3)(462)(3) + (3)(385)(1) + (1)(330)(1)\right) \bmod$

$x = (4158 + 1155 + 330) \bmod$

$x = 5643 \bmod 2310$

$x = 5643 - (2310)(2)$.

$\boxed{x = 1023}$

Question #17:

a) $\overline{2} \bmod 17$

gcd(2, 17)

$17 = (8)2 + 1$

$2 = (2)1 + 0$

↳ GCD

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

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

inverse = $-8 + 17$

$\boxed{9}$

b) $\overline{34} \bmod 89$

gcd(89, 34)

$89 = (2)34 + 21$

$34 = (1)21 + 13$

$21 = (1)13 + 8$

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

$8 = (1)5 + 3$

$5 = (1)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0$

↳ GCD

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

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

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

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

$= 2 \cdot 8 - 3 \cdot 5$

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

$= -3 \cdot 13 + 5 \cdot 8$

$= -3 \cdot 13 + 5 \cdot (21 - 1 \cdot 13)$

$= 5 \cdot 21 - 8 \cdot 13$

$= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21)$

$= -8 \cdot 34 + 13 \cdot 21$

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

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

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

Inverse $= -34$

$= -34 + 89$

$= \boxed{55}$

c) $\overline{144}$ mod 233

gcd(233, 144)

$233 = (1)144 + 89$

$144 = (1)89 + 55$

$89 = (1)55 + 34$

$55 = (1)34 + 21$

$34 = (1)21 + 13$

$21 = (1)13 + 8$

$13 = (1)8 + 5$

$8 = (1)5 + 3$

$5 = (1)3 + 2$

$3 = (1)2 + 1$

$2 = (2)1 + 0.$

↳ GCD.

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

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

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

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

$2 \cdot 8 - 3 \cdot 5$

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

$-3 \cdot 13 + 5 \cdot 8$

$-3 \cdot 13 + 5 \cdot (21 - 1 \cdot 13)$

$5 \cdot 21 - 8 \cdot 13$

$5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21)$

$-8 \cdot 34 + 13 \cdot 21$

$-8 \cdot 34 + 13 \cdot (55 - 1 \cdot 34)$

$13 \cdot 55 - 21 \cdot 34$

$13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55)$

~~$13 \cdot 55$~~ $-21 \cdot 89 + 34 \cdot 55$

$-21 \cdot 89 + 34 \cdot (144 - 1 \cdot 89)$

~~$21 \cdot 89$~~ $34 \cdot 144 - 55 \cdot 89$

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

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

~~$1 = (47)(144) + (-13)(233)$~~ $1 = (89)(144) + (-55)(233)$

Inverse $=$ ~~47~~ $\boxed{89}$

d) $\overline{200} \bmod 1001$

gcd (200, 1001)

$1001 = (5)200 + 1$

$200 = (200)1 + 0.$

↳ GCD

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

$1 = (1)(100) + (-5)(200)$

Inverse $= -5$

$= -5 + 1001$

$\boxed{996}$

Question #18:

Part a:

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

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

Corresponding ~~alphabets~~ nos:

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

p+4:

22 23 18 19 19 18 15 15 24 23 12 18 17

mod 26:

22 23 18 19 19 18 15 15 24 23 12 18 17

Corresponding alphabets:

~~WXSX~~

$\boxed{\text{WXST } \cancel{\#}\text{TSPPYXMSR}}$ Encrypted message

i) $f(p) = (p + 21) \bmod 26$.

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

p + 21:

39 40 35 36 36 35 32 32 41 40 29 35 34

mod 26:

13 14 9 10 10 9 6 6 15 14 3 9 8

corresponding alphabets.

N O J K K J G G P O D J I

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

corresponding no.s

2 4 1 1 14 23 13 14 1 23 24 6

p-10:

-8 -6 -9 -9 4 13 3 4 -9 13 14 -4

~~mod~~ +26 26:

18 20 17 17 4 13 3 4 17 13 14 22

corresponding letters:

S U R R E N D E R N O W decrypted message.

ii) L O W I P B S O X N

corresponding no.s:

11 14 22 8 15 1 18 14 23 13

p-10:

1 4 12 -2 5 -9 8 4 13 3

~~+26:~~

1 4 12 24 5 17 8 4 13 3

corresponding alphabets:

B E M Y F R I E N D decrypted message

Question #19:

a) $5^{2003} \mod 7$

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

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

$5^6 = 1 \pmod 7$.

$5^{6(333)+5} \mod 7$

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

$1 \cdot 3125 \mod 7$

$3125 - 7(446)$

$\boxed{3}$

b) $5^{2003} \mod 11$

$5^{11-1} = 1 \pmod{11}$

$5^{10} = 1 \pmod{11}$

$5^{10(2000)+3} \mod 11$

$(5^{10})^{2003} \cdot 5^3 \mod 11$

$1 \cdot 125 \mod 11$.

$\boxed{4}$

$5^{2003} \mod 13$

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

$5^{12} \equiv 1 \pmod{13}$

$5^{12(166)+11} \mod 13$

$(5^{12})^{166} \cdot 5^{11} \mod 13$.

$1 \cdot 5^{11} \mod 13$

$\boxed{8}$

Question #20:

a). I LOVE MATHEMATICS

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

p+3:

11 14 17 24 7 15 3 22 10 7 15 3 22 11 5 21

mod 26:

11 14 17 24 7 15 3 22 10 7 15 3 22 11 5 21

corresponding alphabets.

L O R Y H P D W K H P D W L F V

DISCRETE= 3 8 18 2 17 4 19 4

↳ 6 11 21 5 20 7 22 7

(missed this above by mistake) ← ↳ G L V F U H W H

b) i) P L G W Z R D V V L J Q P H Q W

corresponding no.s:

15 11 6 22 25 17 3 21 21 11 9 16 15 7 16 22

(p-3) mod 26:

12 8 3 19 22 14 0 18 18 8 6 13 12 4 13 19

corresponding alphabets:

M I D T W O A S S I G N M E N T

ii) I D V W Q X F H V X Q L Y H U V L W B

8 3 21 22 16 23 5 7 21 23 16 11 24 7 20 21 17 22 1

(p-3) mod 26:

5 0 18 19 13 20 2 4 18 20 13 8 21 4 17 18 8 19 24

corresponding alphabets:

F A S T N U C E S U N I V E R S I T Y.

Question #21:

Part a:

i) 034567981 mod 97

$r = 034567981 - 97(356370)$

$r = \boxed{91}$ memory location

ii) 183211232 mod 97

$r = 183211232 - 97(1888775)$

$r = \boxed{57}$ memory location

iii) 2201195744 mod 97

$r = 2201195744 - 97(2270059)$

$r = \boxed{21}$ memory location.

iv) 987255335 mod 97

$r = 987255335 - 97(10177890)$

$r = \boxed{5}$ memory location.

Part b:

i) 104578690 mod 101

$r = 104578690 - 101(1035432)$

$r = \boxed{58}$ memory location.

ii) 432222187 mod 101

$r = 432222187 - 101(4279427)$

$r = \boxed{60}$ memory location.

iii) 372201919 mod 101

$r = 372201919 - 101(3685167)$

$r = \boxed{52}$ memory location.

iv) 5013338753 mod 101

$r = 5013338753 - 101(49637750)$

$r = \boxed{3}$ memory location

Question #22:

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

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

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

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

$x_4 = (4(3)+1) \bmod 7 \Rightarrow 13 \bmod 7 \Rightarrow 6.$

series: 3, 6, 4, 3, 6, 4 .....

repeats.

Question #23:

Part a:

i) 73232184434

$3(7)+3+3(2)+3+3(2)+1+3(8)+4+3(4)+3+3(4)+$

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

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

$\boxed{x_{12} = 5}$ => check digit

ii) 636239913 46

$3(6)+3+3(6)+2+3(3)+9+3(9)+1+3(3)+4+3(6)+$

$x_{12} \equiv 0 \pmod{10}$.

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

$\boxed{x_{12} = 2}$ => check digit

Part b:

i) 036000291452

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

2

=> 60

since $60 \not\equiv 0 \pmod{10}$

It is a valid UPC

ii) 012345678903

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

$0+1+6+3+12+5+18+7+24+9+0+3$

88

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

It is not a valid UPC

Question #24:

Part a:

~~$x_{10} =$~~ 0-07-119881

$x_{10} = [1(0)+2(0)+3(7)+4(1)+5(1)+6(9)+7(8)+8(8)+9(1)] \bmod 11$

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

$= 213 \bmod 11$

$= 213 - 11(19)$

$\boxed{x_{10} = 4 \Rightarrow}$ check digit.

Part b:

0-321-500Q1-8

$x_{10} = [1(0)+2(3)+3(2)+4(1)+5(5)+6(0)+7(0)+8(Q)+9(1)] \bmod 11$

$8 = [0+6+6+4+25+8Q+9] \bmod 11$

$8 = (8Q+50) \bmod 11$

If $Q = 1$

$8 \neq (8(1)+50) \bmod 11$

If $Q = 22$

$8 \neq (66) \bmod 11$

If $Q = 3$

$8 = (8(3)+50) \bmod 11$

$8 = 74 \bmod 11$

$8 = 8$

$\boxed{\text{ie } Q = 3}$

Question #25:

A	T	T	A	C	K
0	19	19	0	2	10

$\Rightarrow$ corresponding no.s.

$n = 43.59$,

$k = (43-1)(59-1).2436$

$e = 13$

$C = M^e \bmod n$

$C = 0019^{13} \bmod 2537$

$C = 1900^{13} \bmod 2537$

$C = 0210^{13} \bmod 2537$