23k-2001
BCS-3J

Discrete Struction: A#3

Date

Answer # 01: $q = a \text{ div } d$, $r = a (\text{mod } d)$

a. 19 is divided by 7:
q: $19 \text{ div } 7 = 2$
r: $19 \text{ mod } 7 = 5$

b. −111 is divided by 11:
$q = -111 \text{ div } 11 = -10$
$r = -111 \text{ mod } 11 = -1$

c. 789 is divided by 23:
$q = 789 \text{ div } 23 = 34$
$r = 789 \text{ mod } 23 = 7$

d. 1001 is divided by 13:
$q = 1001 \text{ div } 13 = 77$
$r = 1001 \text{ mod } 23 = 0$

e. 10 is divided by 19:
$q = 10 \text{ div } 19 = 0$
$r = 10 \text{ mod } 19 = 10$

f. 3 is divided by 5:
$q = 3 \text{ div } 5 = 0$
$r = 3 \text{ mod } 5 = 3$

g. −1 is divided by 3:
$q = -1 \text{ div } 3 = -1$
$r = -1 \text{ mod } 3 = 2$

h. 4 is divided by 1:
$q = 4 \text{ div } 1 = 4$
$r = 4 \text{ mod } 01 = 0$

Teacher's Signature

Answer# 02 :

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

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

$a \text{ div } m = q = -111 \text{ div } 99 = -1$

$a \bmod m = r = -111 \bmod 99 = -12$

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

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

$a \bmod m = -9999 \bmod 101 = 0$

iii. $a = 10299$, $m = 999$

$a \text{ div } m = 10299 \text{ div } 999 = 10$

$a \bmod m = 10299 \bmod 999 = 309$

iv. $a = 123456$, $m = 1001$

$a \text{ div } m = 123456 \text{ div } 1001 = 123$

$a \bmod m = 123456 \bmod 1001 = 333$

b. determine congruent to 5 modulo 17

i. 80

$\Rightarrow 80 \not\equiv 5 \bmod 17$ Ans.

since, (Not congruent)

$80 - 5 = 75$

and $17 \nmid 75$

ii. 103

$\Rightarrow 103 \not\equiv 5 \bmod 17$ Ans.

since,

$103 - 5 = 98$

and $17 \nmid 98$ (Not congruent)

iii. -29

$\Rightarrow -29 \equiv 5 \bmod 17$ (congruent)

since, $-29 - 5 = -34$ Ans.

and

$17 \mid -34$, $[-34/17 = -2]$

iv. -122 :

$\Rightarrow -122 \not\equiv 5 \bmod 17$ (Not congruent)

since, $-122 - 5 = -127$ Ans

and

$17 \nmid -127$

Teacher's Signature

Date

Answer # 03.

a. pairwise relatively prime

i) 11, 15, 19

Ans. Yes.

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

ii) 14, 15, 21

Ans. No

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

iii) 12, 17, 31, 37

Ans. Yes

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

Ans. Yes

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. prime factorization

i) 88

Ans. $88 = 2 \times 2 \times 2 \times 11$

$88 = 2^3 \times 11$

ii) 126

Ans. $126 = 2 \times 3 \times 3 \times 7$

$126 = 2 \times 3^2 \times 7$

iii) 729

Ans. $729 = 3 \times 3 \times 3 \times 3 \times 3 \times 3 = 3^6$

iv) 1001

Ans. $1001 = 7 \times 13 \times 11$

v) 1111

Ans. $1111 = 11 \times 101$

vi) 909

Ans. $909 = 3 \times 3 \times 101$

$909 = 3^2 \times 101$

Date

Answer #04:

Express as a linear combination

$\gcd(144, 89)$ & $\gcd(1001, 100001)$

Sol:

$\gcd(144, 89) = (144)(34) + (89)(-55) = 1$

1 $144 = 89 \times 1 + 55$ $\quad r_1 = 55$

2 $89 = 55 \times 1 + 34$ $\quad r_2 = 34$

3 $55 = 34 \times 1 + 21$ $\quad r_3 = 21$

4 $34 = 21 \times 1 + 13$ $\quad r_4 = 13$

5 $21 = 13 \times 1 + 8$ $\quad r_5 = 8$

6 $13 = 8 \times 1 + 5$ $\quad r_6 = 5$

7 $8 = 5 \times 1 + 3$ $\quad r_7 = 3$

8 $5 = 3 \times 1 + 2$ $\quad r_8 = 2$

9 $3 = 2 \times 1 + 1$ $\quad r_9 = 1$ (gcd)

10 $2 = 1 \times 2 + 0$ No remainder, gcd found.

Express a gcd as a linear combination

11 $1 = 3 - 2 \times 1$ $\quad \therefore 2 = 5 - 3 \times 1$ $\quad 1 = 3 \times 2 - 5$

12 $1 = (8 - 5) \times 2 - 5$ $\quad \therefore 3 = 8 - 5 \times 1$ $\quad 1 = 8 \times 2 - 5 \times 3$

13 $1 = 8 \times 2 - (13 - 8) \times 3$ $\quad \therefore 5 = 13 - 8 \times 1$ $\quad 1 = 8 \times 5 - 13 \times 3$

14 $1 = (21 - 13) \times 5 - 13 \times 3$ $\quad \therefore 8 = 21 - 13 \times 1$ $\quad 1 = 21 \times 5 - 13 \times 8$

15 $1 = 21 \times 5 - (34 - 21) \times 8$ $\quad \therefore 13 = 34 - 21 \times 1$ $\quad 1 = 21 \times 13 - 34 \times 8$

16 $1 = (55 - 34) \times 13 - 34 \times 8$ $\quad \therefore 21 = 55 - 34 \times 1$ $\quad 1 = 55 \times 13 - 34 \times 21$

17 $1 = 55 \times 13 - (89 - 55) \times 21$ $\quad \therefore 34 = 89 - 55 \times 1$ $\quad 1 = 55 \times 34 - 89 \times 21$

18 $1 = (144 - 89) \times 34 - 89 \times 21$ $\quad \therefore 55 = 144 - 89 \times 1$ $\quad 1 = 144 \times 34 - 89 \times 55$

Final answer:

$\gcd(144, 89) = 34(144) - 55(89)$

$\gcd = 1$

Date

Sol:

$$\gcd(1001, 100001) = 100(1001) - 1(100001) = 1$$

1. $100001 = (1001)99 + 1000$ $r_1 = 1000$
2. $1001 = (1000)1 + 1$ $r_2 = 1$ (gcd)
3. $1000 = (1000)(1) + 0$ No remainder

$\Rightarrow$ 4. $1 = 1001 - (1000)1$ $\therefore 1000 = 100001 - 1001 \times 99$

5. $1 = 1001 \times 100 - 100001 \times 1$

Final answer

$$\gcd(1001, 100001) = 100(1001) - 1(100001)$$

$$\gcd = 1$$

Answer #05:

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

Sol:

$$\gcd(55, 89) = (55)(34) + (89)(-21) = 1$$

inverse: $\bar{a} = 34$

Multiply b/s by 34.

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

$$x = 1156 \pmod{89}$$

$\boxed{x = 88}$ Ans.

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

Sol:

$$\gcd(89, 232) = (73)(89) + (232)(-28) = 1$$

inverse: $\bar{a} = 73$

Multiply b/s by 73

$$\Rightarrow (89)(73)x \equiv (2)(73) \pmod{232}$$

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

$\boxed{x = 146}$ Ans.

Teacher's Signature

Answer #06:

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

$a_1 = 1$ $\quad m_1 = 5$

$a_2 = 2$ $\quad m_2 = 6$

$a_3 = 3$ $\quad m_3 = 7$

$M = 5*6*7 = 210$

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

$M_1 = 42$ $\quad M_2 = 35$ $\quad M_3 = 30$

$M_1 x_1 (\bmod m_1) = 1$

$42 x_1 (\bmod 5) = 1$, $\left[\because \frac{42}{5}, r = 2\right]$

$2 x_1 (\bmod 5) = 1$

$\left[\because \frac{2(3)}{5} = \frac{6}{5}, r = 1\right]$

$\Rightarrow \boxed{x_1 = 3}$

$M_2 x_2 (\bmod m_2) = 1$

$35 x_2 (\bmod 6) = 1$ $\quad \left[\because \frac{35}{6}, r = 5\right]$

$5 x_2 (\bmod 6) = 1$

$\left[\because \frac{5(5)}{6} = \frac{25}{6}, r = 1\right]$

$\Rightarrow \boxed{x_2 = 5}$

$M_3 x_3 (\bmod m_3) = 1$

$30 x_3 (\bmod 7) = 1$, $\left[\because \frac{30}{7}, r = 2\right]$

$2 x_3 (\bmod 7) = 1$

$\left[\because \frac{2(4)}{7} = \frac{8}{7}, r = 1\right]$

$\Rightarrow \boxed{x_3 = 4}$

$\because x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$

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

$x = 836 (\bmod 210)$

$\boxed{x = 206}$ Ans.

Date

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

$a_1 = 1$ $\quad m_1 = 2$

$a_2 = 2$ $\quad m_2 = 3$ $\quad M = 2*3*5*11$

$a_3 = 3$ $\quad m_3 = 5$ $\quad M = 330$

$a_4 = 4$ $\quad m_4 = 11$

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

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

$M_1 x_1 (\mathrm{mod}\ m_1) = 1$ $\quad M_2 x_2 (\mathrm{mod}\ m_2) = 1$ $\quad M_3 x_3 (\mathrm{mod}\ m_3) = 1$

$165 x_1 (\mathrm{mod}\ 2) = 1$ $\quad 110 x_2 (\mathrm{mod}\ 3) = 1$ $\quad 66 x_3 (\mathrm{mod}\ 5) = 1$

$(1) x_1 (\mathrm{mod}\ 2) = 1$ $\quad 2 x_2 (\mathrm{mod}\ 3) = 1$ $\quad 1 x_3 (\mathrm{mod}\ 5) = 1$

$\Rightarrow x_1 = 1$ $\quad \Rightarrow x_2 = 2$ $\quad \Rightarrow x_3 = 1$

$M_4 x_4 (\mathrm{mod}\ m_4) = 1$

$30 x_4 (\mathrm{mod}\ 11) = 1$

$8 x_4 (\mathrm{mod}\ 11) = 1$

$\Rightarrow x_4 = 7$

Now,

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3 + M_4 x_4 a_4) \bmod M$

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

$x = 1643 (\mathrm{mod}\ 330)$

$\boxed{x = 323}$ Ans.

Date

Answer # 07:

inverse of a mod m

a. $a = 2$, $m = 17$

Sol:

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

$\Rightarrow -8 + 17 = 9$

$\Rightarrow$ inverse: $\bar{a} = 9$. Ans.

b. $a = 34$, $m = 89$

Sol:

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

$\Rightarrow -34 + 89 = 55$

$\Rightarrow$ inverse: $\bar{a} = 55$ Ans.

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

Sol:

$gcd(144, 233) = (89)(144) + (-55)(233) = 1$.

$\Rightarrow \because (89)$ is already positive

$\Rightarrow$ inverse: $\bar{a} = 89$

d. $a = 200$, $b = 1001$

Sol:

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

$\Rightarrow -5 + 1001 = 996$

$\Rightarrow$ inverse: $\bar{a} = 996$ Ans.

Date

Answer #08:

a. "STOP POLLUTION"

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

Sol:

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

Apply $f(p)$:

$\Rightarrow$ 22 23 18 19 19 18 15 15 24 23 12 18 17

W X S T T S P P Y X M S R Ans. (encrypted)

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

Sol:

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

Apply $f(p)$:

$\Rightarrow$ 13 14 9 10 10 9 6 6 15 14 3 9 8

N O J K K J G G P O D J I Ans. (encrypted)

b. Shift Cipher: $f(p) = (p+10) \mod 26$

i)

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

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

Decryption: $f^{-1}(p) = (p-10) \mod 26$

$\Rightarrow$ 18 20 17 17 4 13 3 4 17 13 14 22

S U R R E N D E R N O W

Ans. "SURRENDER NOW"

ii)

LO WI PBSOXN

11 14 22 8 15 1 18 14 23 13

Decryption: $f^{-1}(p) = (p-10) \mod 26$

$\Rightarrow$ 1 4 12 24 5 17 8 4 13 3

B E M Y F R I E N D

 Ans. "BE MY FRIEND"

Teacher's Signature

Answer#09:

a. Fermat's Little Theorem

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

Sol:

$$\because \quad 5^6 = 1 \bmod 7$$
$$\Rightarrow \quad = (5^6)^{333} \cdot 5^5 \bmod 7$$
$$= 5^5 \bmod 7$$
$$= 3 \qquad \text{Ans.}$$

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

Sol:

$$\because \quad 5^{10} = 1 \bmod 11$$
$$\Rightarrow \quad = (5^{10})^{2000} \cdot 5^3 \bmod 11$$
$$= 5^3 \bmod 11$$
$$= 4 \qquad \text{Ans.}$$

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

Sol:

$$\because \quad 5^{12} = 1 \bmod 13$$
$$\Rightarrow \quad = (5^{12})^{166} \cdot 5^{11} \bmod 13$$
$$= 5^{11} \bmod 13$$
$$= 8 \qquad \text{Ans.}$$

b. "ATTACK", RSA system, $n = 43 \cdot 59$
$e = 13$

$n = 43 \cdot 59 = 2537$

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

$\Rightarrow (0, 19), (19, 0), (2, 10)$

$\Rightarrow (019), (190), (210)$

$$\because \quad C = M^e \bmod n$$

$M = 19$
$C = 19^{13} \bmod 2537$
$C = 1991$

$M = 190$
$C = 190^{13} \bmod 2537$
$C = 849$

$M = 210$
$C = 210^{13} \bmod 2537$
$C = 120$

Encrypted message = (1991, 849, 120)

Ans.

Page No.

Teacher's Signature

Answer # 10:

a. "I LOVE DISCRETE MATHEMATICS"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ans. Encrypted:

"L ORYH GLVFUHWH PDWKHPDWLFV"

b. i) $P = f^{-1}(15) = (15-3) \bmod 26 = 12 = M$, $\because f^{-1}(P) = (P-3) \bmod 26$

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

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

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

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

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

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

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

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

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

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

Ans. Decrypted:

"MID TWO ASSIGNMENT"

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

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

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

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

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

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

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

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

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

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

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

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

Ans. Decrypted:
"FAST NUCES UNIVERSITY"

COUNTENG TECHNIQUES

Answer #01:

a. 8C3:

$$\Rightarrow \frac{8!}{3!(8-3)!} = \frac{8 \times 7 \times 6 \times \cancel{5!}}{3!\,\cancel{5!}} = 56 \text{ ways}$$ Ans.

b. 12C6:

$$\Rightarrow \frac{12!}{6!(12-6)!} = \frac{12 \times 11 \times 10 \times 9 \times 8 \times 7 \times \cancel{6!}}{6!\,\cancel{6!}} = 924 \text{ ways}$$ Ans.

c. 9C5:

$$\Rightarrow \frac{9!}{5!(9-5)!} = \frac{9 \times 8 \times 7 \times 6 \times \cancel{5!}}{\cancel{5!}\,4!} = 126 \text{ ways}$$ Ans.

Answer #02:

a. $20P5 = \frac{20!}{(20-5)!} = 1860480$ ways Ans.

b. $16P4 = \frac{16!}{(16-4)!} = 43680$ ways Ans.

c. $15P2 = \frac{15!}{(15-2)!} = 210$ ways Ans.

Date

Answer # 03 :

a. Sol:

1 meat = $5C1$, 2 bread = $3C2$, 1 cheese = $4C1$, 3 condiment = $6C3$

$\Rightarrow$ Sandwiches = $5C1 \times 3C2 \times 4C1 \times 6C3$

= 1200 Ans.

b. Sol:

$\Rightarrow$ faces = $15 \times 48 \times 24 \times 34 \times 28 \times 28$ = 460,615,680 Ans.

Answer # 04 :

a. length : 10

$\rightarrow$ begin : 3 0's or end : 2 0's

$\Rightarrow 2^7 = 128$ $\Rightarrow 2^8 = 256$

$\rightarrow$ begin : 3 0's and end : 2 0's

$\Rightarrow 2^5 = 32$

Total = 128 + 256 − 32

Total = 352 Ans.

b. length : 5

$\rightarrow$ begin : 0 or end : 2 1's

$\Rightarrow 2^4 = 16$ $\Rightarrow 2^3 = 8$

$\rightarrow$ begin : 0 and end : 2 1's

$\Rightarrow 2^2 = 4$

Total = 16 + 8 − 4

Total = 20 Ans.

23k-2001

Date

Answer # 05:

a. Sol:

pairs with sum: 13 $\Rightarrow$ $\{(1,12), (2,11), (3,10), (4,9), (5,8), (6,7)\}$

Total = 6

If 7 numbers are chosen,
pigeon-hole principle tells there is atleast one pair which adds up to 13. Ans.

b. Sol:

Number of people : 8
Total days in week : 7

$\Rightarrow \left\lceil \frac{8}{7} \right\rceil = 2$ (ceiled)

There are only 7 days/week, if we choose 8 people the pigeon-hole principle tells atleast two people had born on the same day. Ans.

c. Sol:

Number of people : 30
Days in week : 7

$\Rightarrow \left\lceil \frac{30}{7} \right\rceil = 5$

Thus, 5 people from a group of 30 were born on the same day of the week. Ans.