ASSIGNMENT #03

Discrete Structure

Q#2

(a) 19 is divide by 7?

$19 = (q)(d) + r$

$19 = (2)(7) + 5$

$q = 2, r = 5$

(b) -111 is divided by 11

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

$q = -11, r = 10$

(c) 789 is divide by 23

$789 = (q)(23) + r$

$q = 34 \quad r = 7$

(d) 1001 is divided by 13

$1001 = q(13) + r$

$q = 77, r = 0$

(e) 10 is divided by 19

$10 = (q)(19) + r$

$q = 0, r = 10$

(f) 3 is divided by 5

$3 = (q)(5) + r$

$q = 0, r = 10$

(g) -1 is divide by 3

$-1 = (q)(3) + r$

$q = -1 \quad r = 2$

(h) 4 is divided by 1

$4 = (q)1 + 0$

$q = 4, r = 0$

Q#2 a)

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

$q = a \text{ div } m$

$\Rightarrow q = -111 \text{ div } 99$

$q = -2$

$r = 87$

(v) $a = -9999 \quad m = 101$

$q = -9999 \text{ mod } 101$

$\Rightarrow q = -99$

$\Rightarrow r = 0$

iii) $a = 10299, m = 999$

$q = 10299 \text{ div } 999$

$q = 10$

$r = 309$

(iv) $a = 123456 \quad m = 101$

$q = 123456 \text{ div } 1001$

$q = 123$

$= 333$

(b7)

(i) $a \equiv b \pmod{n(m)}$

$80 = 5 \pmod{17}$

$80 = (4)(17) + 12$

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

(ii) 103

$103 = 17(6) + 1$

$r = 1 \quad$ so $103 \not\equiv 5 \pmod{17}$

(iii) -29

$-29 = 5 \pmod{n}$

$-29 = (-2)(17) + 5$

$r = 5 \quad$ so $29 \equiv 5 \pmod{17}$

(iv) -122

$-122 = 17(-8) + 14)$

$r = 14 =$

$122 \not\equiv 5 \pmod{17}$

Q#3

(a)(i) 11, 15, 19

gcd 11, 15 =

$15 = (1)(11) + 4$

$11 = (2)(4) + 3$

$4 = (1)(3) + 1$

11, 19

$19 = (1)(11) + 9$

$11 = (1)(9) + 2$

$9 = (4)(2) + 1$

15, 19

$19 = 15(1) + 4$

$15 = (3)(4) + 3$

$4 = (1)(3) + 1$

no common divisor so the ae relatively prime

(ii) 14, 15, 21

gcd 14, 15 = (1)

$15 = (1)14 + 1$

$14 = 14(1) + 0$

gcd 14, 21 = (7)

$21 = 1(14) + 7$

$14 = (2)(7) + 0$

$(15, 21) = 3$

$21 = (1)15 + 6$

$15 = (2)(6) + 3$

$6 = (2)(3) + 0$

They common divisor so they are not relatively prime.

(iii) 12, 17, 31, 32

12, 17

$17 = (1)(12) + 5$

$12 = (2)(5) + 2$

$5 = 2(2) + 1 =$

$2 = 2(1) + 0$

(12, 31)

$31 = (2)(12) + 7$

$12 = (1)(7) + 5$

$7 = 1(5) + 2$

$5 = 2(2) + 1 =$

$2 = 2(1) + 0$

12, 37

$37 = (3)(12) + 1$

$12 = 12(1) + 0$

No common divisor so they are not relatively prime

(a) gcd 7,8,9,11

gcd(7,8) = 1
$8 = (1)7 + 1$
$7 = 7(1) + 0$

gcd 7,9 = 1
$9 = (1)(7) + 2$
$7 = (3)(2) + 1$
$2 = 2(1) + 0$

gcd(7,11) = 1
$11 = (1)(7) + 4$
$7 = (1)(4) + 3$
$4 = 1(3) + 1$
$3 = 3(1) + 0$

gcd(8,9) = 1
$9 = (1)(8) + 1$
$8 = (8)(1) + 0$

gcd(8,11) = 1
$11 = (1)8 + 3$
$8 = (2)3 + 2$
$3 = (1)(2) + 1$
$2 = (2)(1) + 0$

gcd (9,4) = 1
$11 = (1)(9) + 2$
$9 = 4(2) + 1$
$2 = 2(1) + 0$

relative prime

(b)

(i) 88

$2 \times 2 \times 2 \times 11$

2	88
2	44
2	22
11	11
	1

(ii) 729

$3 \times 3 \times 3 \times 3 \times 3 \times 3$

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

(iii) 126

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

2	126
3	63
3	21
7	7
	1

(iv) 1001

$7 \times 13 \times 11 = 1001$

7	1001
13	143
11	11
	1

(v) 1111

$= 11 \times 101$

11	1111
101	101
	1

(vi) 909

$3 \times 3 \times 101$

3	909
3	303
101	101
	1

Q#4 Use the extended Euclidean algorithm to express gcd (144, 89) and gcd (1001, 10000) as linear combination

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

$10000 = 99(1001) + 902$
$1001 = (1)(902) + 99$
$902 = 9(99) + 11$
$99 = (9)(11) + 0$
GCD $(1001, 10000) = 1$

Q#5 (a)
$55x \equiv 34 \pmod{89}$
GCD $(55, 89)$

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

$1 = 1 \cdot 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (5 - 1 \cdot 3) = -1 \cdot 5 + 2 \cdot 3$
$1 = -1 \cdot 5 + 2 \cdot (8 - 1 \cdot 5) = 2 \cdot 8 - 3 \cdot 5$
$1 = 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13$
$1 = 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$
$1 = 5 \cdot (55 - 1 \cdot 34) - 8 \cdot 13 = 5 \cdot 55 - 5 \cdot 34 - 8 \cdot 1$
$1 = 5 \cdot 55 - 5 \cdot 34 - 8 \cdot (34 - 1 \cdot 21)$
$1 = 5 \cdot 55 - 13 \cdot 34 + 8 \cdot 21$
$1 = 5 \cdot 55 - 13 \cdot 89 - 1 \cdot 55) 8 \cdot 21$
$1 = 5 \cdot 55 - 13 \cdot 89 + 13 \cdot 55 + 8 \cdot (55 - 1 \cdot 34)$
$5 \cdot 55 - 13 \cdot 89 + 13 \cdot 55 + 8 \cdot 55 - 8 \cdot 34$
$26 \cdot 55 - 13 \cdot 89 - 8 \cdot 34$
$26 \cdot 55 - 13 \cdot 89 - 8 \cdot 89 - 1 \cdot 55) = 1 = 34 \cdot 55 + (-21) 89$

$55 \times 34 \times x = 34 \times 34 \pmod{89}$
$x = 1156 \pmod{89}$
$x = 88$

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

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

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

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

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

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

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

$3 = (3)(1) + 0$

$89 \times 73_x = 2 \times 73 \pmod{10}$

$x = 146 \bmod 232$

$x = 146$

$1 = 1 \cdot 16 - 5 \cdot 3$

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

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

$1 = 6 \cdot 16 - 5 \cdot 19$

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

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

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

$1 = 6 \cdot 35 - 11 \cdot 19$

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

$1 = 6 \cdot 35 - 11 \cdot 54 + 11 \cdot 35$

$1 = 6 \cdot 75 - 11 \cdot 54 + 11 \cdot 35$

$1 = 17 \cdot 35 - 11 \cdot 54$

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

$1 = 17 \cdot 89 - 17 \cdot 54 - 11 \cdot 54$

$1 = 17 \cdot 89 - 28 \cdot 54$

$1 = 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89)$

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

Q#6

(a)

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

$m = m_1 \times m_2 \times m_3$ $\quad a_1 = 1 \Rightarrow a_2 = 2, a_3 = 3$

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

$M_1 = \frac{210}{5} = 42$, $M_2 = \frac{210}{6} = 35$, $M_3 = \frac{210}{7} = 30$

$y_1 = M_1^{-1} \bmod 5$

$y_1 = 42 \bmod 5$

$42 = 8(5) + 2$

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

$2 = 2(1) + 0$

$1 = 105 - 2 \cdot 2$

$1 = 105 - 2 \cdot (42 - 8 \cdot 5)$

$1 = 105 - 2 \cdot 42 + 16 \cdot 5$

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

$y_1 = -2 + 5 = 3$

$y_2 = 35 \bmod 6$

$35 = 5(6) + 5$

$6 = 1(5) + 1$

$5 = 5(1) + 0$

$1 = 6 - 1 \cdot 5$

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

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

$y_2 = -1 + 6 = 5$

$y_3 = 30 \bmod 7$

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

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

$2 = 2(1) + 0$

$1 = 7 - 3 \cdot 2$

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

$1 = 7 - 3 \cdot 30 + 12 \cdot 7$

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

$y_3 = 7 - 3 = 4$

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

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

$x = 836 \bmod 210$

$x = 206$

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

$a = 1 \Rightarrow a_2 = 2$, $a_3 = 3$, $a_4 = 4$

$M_1 = \frac{330}{2} = 165$ $M_2 = \frac{330}{3} = 110 \Rightarrow M_3 = \frac{330}{5} = 66$, $M_4 = 30$

y $165 \bmod 2$

$165 = 82(2) + 1$

$(2) = (2)(1) + 0$

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

$\Rightarrow$ $(1)(165)$ 2

$y_1 = 1$

$y_2 = 110 \bmod 3$

$110 = 36(3) + 2$

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

$2 = 2(1) + 0$

$1 = 3 - 1 \cdot 2$

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

$= 3 - 1 \cdot 110 + 363$

$37 \cdot 3 + (-1)(100$

$y_3 \; 66 \bmod 5$

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

$5 = (1)(15) + 0$

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

$y_3 = 1$

$y_4 = 30 \bmod 11$

$30 = 2(11) + 8$

$11 = 1(8) + 3$

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

$3 = 1(2) + 1$

$2 = 2(1) + 0$

$1 = 103 - 1 \cdot 2$

$1 = 103 - 1 \cdot [108 - (2)(3)]$

$1 = 103 - 108 + 2 \cdot 3$

$1 = 3 \cdot 3 - 108$

~~$3 \cdot 3 - 1$~~

$1 = 3 \cdot (111 - 108) - 1 \cdot 8$

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

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

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

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

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

$y_4 11 - 4 = 7$

$\Rightarrow (a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3 + a_4 m_4 y_4) \bmod m$

$\Rightarrow (11 \times 165 \times 1) + 12(110 \times 2 + (3 \times 66 \times 1) + (4 \times 30 \times 7) \bmod 330$

$\Rightarrow 1643 \bmod 330$

$x = 323$

(b) $a_1 = 3, a_2 = 3, a_3 = 1, a_4 = 0$

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

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

$m = 2310$

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

$M_4 = \frac{2310}{7} = 210$

$y_1 = 462 \bmod 5$

$462 = 92(5) + 2$

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

$2 = 2(1) + 0$

$1 = 5 - 2 \cdot 2$

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

$5 - 2 \cdot 462 + 925$

$93 \cdot 5 - 2 \cdot 462$

$y_1 = 5 + (-2) = 3$

$y_2 = 385 \bmod 6$

$385 = 64(6) + 1$

$6 = 6(1) + 0$

$1 = 385 - 64 \cdot 6$

$y_2 = 1$

$y_3 = 330 \bmod 7$

$330 = 47(7) + 1$

$7 = 7(1) + 0$

$1 = 1 \cdot 330 + (-42)(7)$

$y_3 = 1$

$y_4 = 210 \bmod 11$

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

$11 = 11(1)+0$

$1 = 210 - 19 \cdot 11$

$y_4 = 1$

$x = 5643 \bmod 2310$

$x = 1023$

Q17

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

$17 = 8(2)+1$

$2 = 2(1)+0$

$1 = 17 - 8 \cdot 2$

$y = -8 + 17 = 9$

$\bar{a} = 9$

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

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

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

$21 = 1(13)+8$

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

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

$5 = 1(3)+2$

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

$2 = (2)(1)+0$

$1 = 3 - 1 \cdot 2$

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

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

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

$-34 + 89 = 55$

Inverse $\bar{a} = 55$

(c) $a=144 \quad m=233$

gcd(144, 233)

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

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

$89 = 1(55)+34$

$55 = 1(34)+21$

$34 = 1(21)+13$

$21 = 1(13)+8$

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

$8 = 1(5)+3$

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

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

$2 = 2(1)+0$

$89 - 55 + 233 = 89$

Inverse = 89

$\bar{a} = 89$

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

gcd (200, 1001)

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

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

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

$\bar{a} = 996$

Q#8

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

$F(18+4) \bmod 26 \Rightarrow 22 \bmod 26 \Rightarrow 22$ (W)
$F(19+4) \bmod 26 \Rightarrow 23 \bmod 26 \Rightarrow 23$ (X)
$F(14+4) \bmod 26 \Rightarrow 18 \bmod 26 \Rightarrow 18$ (S)
$F(15+4) \bmod 26 \Rightarrow 19 \bmod 26 \Rightarrow 19$ (T)
11 11 19 (T)
$F(14+4) \bmod 26 \Rightarrow 18 \bmod 26 \Rightarrow 18$ (S)
$F(11+4) \bmod 26 \Rightarrow 15 \bmod 26 \Rightarrow 15$ (P)
$F(20+4) \bmod 26 \Rightarrow 24 \bmod 26 \Rightarrow 24$ (Y)
$F(8+4) \bmod 26 \Rightarrow 12 \bmod 26 \Rightarrow 12$ (M)
$F(13+4) \bmod 26 \Rightarrow 17 \bmod 26 \Rightarrow 17$ (R)

Message after Encryption : WXST TSPPMSR
TSPPYXMSR

(i) $F(P) = P+21 \bmod 26$

$\Rightarrow (18+21) \bmod 26 \Rightarrow 39 \bmod 26 \Rightarrow 13$ (N)
$(8+21) \bmod 26 \Rightarrow 40 \bmod 26 = 14$ (O)
$(14+21) \bmod 26 \Rightarrow 35 \bmod 26 = 9$ (J)
$(5+21) \bmod 26 \Rightarrow 26 \bmod 26 = 10$ (K)
$(11+21) \bmod 26 \Rightarrow 32 \bmod 26 = 6$ (G)
$(20+21) \bmod 26 \Rightarrow 41 \bmod 26 = 15$ (P)
$(8+21) \bmod 26 \Rightarrow 29 \bmod 26 = 3$ (D)
$(13+21) \bmod 26 \Rightarrow 34 \bmod 26 \Rightarrow 8$ (I)

Message After Encryption = NOJK KJGGPDII.

(b)

(i) CEBBOXNOBXYQ

C => (2-10) mod 26 = 18 (S)
E => (4-10) mod 26 = 20 (U)
B => (1-10) mod 26 = 17 (R)
O => 14-10 mod 26 = 4 (E)
X => (23-10) mod 26 = 23 (N)
N => (13-10) mod 26 = 3 (D)
Y => (24-10) mod 26 = 14 (O)
Q => (16-10) mod 26 = 22 (W)

After Decryption message is SURRENDER NOW

(ii) LO IN PBSOXN

F(P) = (P+10) mod 26
L => (11-10) mod 26 => 1 mod 26 = (B)
O => (14-10) mod 26 => 4 mod 26 (E)
IN => (22-10) mod 26 => 12 (M)
D => (8-10) mod 26 => 24 (Y)
P => (15-10) mod 26 => 5 (F)
B => (1-10) mod 26 => 17 (R)
S => (18-10) mod 26 => 8 (I)
X => (23-10) mod 26 => 13 (N)
N => (13-10) mod 26 => 3 (D)

After Decryption message is BE MY FRIEND

Q#9 i) $5^{2003} \bmod 7$ $\Rightarrow a^{p-1} = 1 \pmod p$

$5^6 = 1 \pmod 7$

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

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

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

$5^4 \equiv (5^4 \cdot 5) \bmod 7$

$10 \bmod 7$

$3 \bmod 7$

$5^5 \bmod 7 = 3$

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

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

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

$(5^{10})^{2000} \cdot 5^3 \bmod 11$

$5^3 \bmod 11$

$125 = 11(11) + 4$

$125 \bmod 11 \Rightarrow 4$ Ans

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

$5^{12} = 1 \bmod 13$

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

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

$\Rightarrow 5^{11} \bmod 13$

$\Rightarrow (5^5)^{2+1} \bmod 13$

$5^2 \cdot 5^7 \bmod 13$

$125 = 9(13) + 8$

$\Rightarrow 8$ Answer

10 a)

I	LOVE	DISCRETE	MATHEMATICS
8	11 14 21 4	3 8 18 2 17 4 19 4	12, 0, 19, 17, 7, 4, 12, 0, 19, 8, 2, 18

For ~~Encryption~~ key = 3

$E(P) = (P+3) \bmod 26$

$E(8) \Rightarrow (8+3) \bmod 26 \Rightarrow 11\ (L)$

$E(11) \Rightarrow (11+3) \bmod 26 \Rightarrow 14\ (O)$

$E(14) \Rightarrow (14+3) \bmod 26 \Rightarrow 17\ (R)$

$E(21) \Rightarrow (21+3) \bmod 26 \Rightarrow 24\ (Y)$

$E(4) \Rightarrow (4+3) \bmod 26 \Rightarrow 7\ (H)$

$E(3) \Rightarrow (3+3) \bmod 26 \quad 6\ (G)$

$E(15) \Rightarrow (18+3) \bmod 26 \Rightarrow 21\ (V)$

E(2) = E(3+2) mod 26 = 5(F)
E(17) = E(12+7) mod 26 = 20(Q)
E(19) = E(19+3) mod 26 = 22(W)
E(12) = E(12+3) mod 26 = 15(P)
E(0) E(0+3) mod 26 = 3(P)

After Encryption
12 oryh glvfuhwh pdwkhpdwfv

b(i) PLG IN2R DVV2IQPAOMI
15 11 16 22 25 17 3 21 21 11 9 16 15 2 16 22

E(P) = E(P-3) mod 26
E(18) => 12 (M)
E(11) => 8 (I)
E(6) => 03 (D)
E(22) => 19 (T)
E(25) => 22 (W)
E(17) => 14 (O)
E(3) => 0 (A)
E(9) => 18 (S)
E(9) => 06 (G)
E(16) => 13 (N)
E(7) => 04 (E)
After Decryp Message
is => MIDT Two Assignment

ii) I OvW OYFHV XBLHUVLWC
E(P) = E(23) mod 26
E(8) = (8-3) mod 26 = 5(F)
E(3) => 0(A)
E(21) => 18(S)
E(22) => 19(T)
E(16) => 13(N)
E(23) => 20(U)
E(5) => 2(C)
E(7) => 4(E)
E(11) => 08(I)
E(20) => 21(V)
E(26) => 17(R)
E(22) => 24(4)

After Decryption
FAST NUCES UNIVERSITY

Q#11

a) i) $034567981 \bmod 97$

$\Rightarrow 034567981 = 1356770\,(97) + 91$

$\Rightarrow 91$ answer

ii) $183211232 \bmod 97$

$183211232 = (1888775)(97) + 57 = 57$ Answer

iii) $220195744 \bmod 97$

$220195744 = 188\,(2270059)(97) + 21 = 21$ Answer

iv) $987255335 \bmod 97$

$987255335 = (10177890)(97) + 5 \Rightarrow 5$ Answer

(b)

i) 104578690

$104578690 = (1035432)(101) + (58)$

58 Answer

ii) $4322222187 \bmod 101$

$4322222187 = (4279427)(101) + 60$

iii) $37201919 \bmod 101$

$37201919 = 3685167\,(101) + 52$

52 Answer

iv) $501338753 \bmod 101$

$501338753 = (496375)(101) + 3$

$\Rightarrow$ 3 Answer

Q#12 $x_{n+1} = (4x_{n+1}) \bmod 7$

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

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

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

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

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

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

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

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

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

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

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

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

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

$x_{14} = 4(6)+1 \bmod 7 = 25 \bmod 7 = 4$

$x_{15} = (4(4)+1) \bmod 7 = 17 \bmod 7 = 3$

$x_{16} = (4(3)+1) \bmod 7 = 13 \bmod 7 = 6$

$x_{17} = (4(6)+1) \bmod 7 = 25 \bmod 7 = 4$

$x_{18} = (4(4)+1) \bmod 7 = 17 \bmod 7 = 3$

$x_{19} = (4(3)+1) \bmod 7 = 13 \bmod 7 = 6$

$x_{20} = (4(6)+1) \bmod 7 = 25 \bmod 7 = 4$

$= 17 \bmod 7 = 3$

Sequence is 6, 4, 3, 6, 4, 2 = 6

13 (a)(i) 7323184434

$7+3+3+2\cdot3+3+2\cdot3+1+8\cdot3+4+4\cdot3+3+4\cdot3+x_{12} = 0 \bmod 10$

$21+3+6+3+6+1+24+4+12+3+12+x_{12} = 0 \bmod 10$

$95 + x_{12} = 0 \bmod 10 \Rightarrow x_{12} = -95 \bmod 10 \Rightarrow x_{12} = 5$ Ans

(ii) 6362399134 6

$6\cdot3+3+6\cdot3+2+3\cdot3+9+9\cdot3+1+3\cdot3+4+6+3+x_{12} = 0 \bmod 10$

$18+3+18+2+9+9+27+1+9+4+18+x_{12} = 0 \bmod 10$

$118 + x_{12} = 0 \bmod 10 \Rightarrow x_{12} = -118 \bmod 10 \Rightarrow -118 = (-12)(10)+2$

$x_{12} = 2$ Ans

b

i) 0360002914 52

$0\cdot3+3+6\cdot3+0+0+0+2\cdot3+9+1\cdot3+4+5\cdot3+2 = 0 \bmod 10$

$60 = 0 \bmod 10$

$\gcd(60,10) \Rightarrow 60 = 6(10)+0$

valid upc code

ii) 012345678903

$0\cdot3+1+6+4+15+6+21+8+27+0+9$

$\Rightarrow 0\cdot3+1+2\cdot3+3+4\cdot3+5+6\cdot3+7+8\cdot3+9+0+0\cdot3+3 = 0 \bmod 10$

$0+1+6+3+12+5+18+7+24+9+3 = 0 \bmod 10$

$88 = 0 \bmod 10 \Rightarrow \gcd(88,10) \Rightarrow 88 = 8(10)+8$

Not a valid UPC code

Q#14

a) $0\text{-}07\text{-}119881$

$1\cdot0+2\cdot0+3\cdot7+4\cdot1+5\cdot1+6\cdot9+7\cdot8+8\cdot8+9\cdot1+x_{10}$

$0+0+21+4+5+54+56+64+9+x_{10} = 0 \bmod 11$

$213+x_{10} = 0 \bmod 11 \Rightarrow x_{10} = -213 \bmod 11 \Rightarrow x_{10} = 4$

b) $0\text{-}321\text{-}5001\text{-}8$

$x_{10} = 1\cdot0+2\cdot3+3\cdot2+4\cdot1+5\cdot5+6\cdot0+7\cdot0+8\cdot0+9\cdot1 \bmod 11$

$\Rightarrow 0+6+6+4+25+0+0+80+9 \bmod 11$

$80+50 \bmod 11$

$80+50 \bmod 11 = 8 \Rightarrow 80+6 \bmod 11 = 8 \Rightarrow 86 \bmod 11 = 2$

$8Q = 2 \pmod{11}$

$\gcd(8,11) = 1$

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

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

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

$\Rightarrow 7 \times 2 \bmod 11$

$Q = 14 \pmod{11}$

$Q = 3$

$50 \bmod 11$

$50 = (4)(11)+6$

6 Answer

$1 = 1\cdot3-1\cdot2$

$1 = 1\cdot3-1\cdot(1\cdot8-2\cdot3)$

$1 = 1\cdot3-1\cdot8+2\cdot3$

$1 = 3\cdot3-1\cdot8$

$1 = 3\cdot(1\cdot11-1\cdot8)-1\cdot8$

$1 = 3\cdot11-3\cdot8-1\cdot8$

$1 = 3\cdot11-4\cdot8$

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

$a = -4+11 = 7$

Q#15(a) ATTACK, $n = 43 \cdot 59$ and $e = 13$

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

$n = p \times q = 43 \cdot 59$

$n = 2537$

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

$k = 2436$

$e = 13 \quad (1 < e < k)$

$GCD\ (13, 2436) = 1$

$C = M^e \bmod n$

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

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

$C = 0210^3 \bmod 2537$

(b) Assignment $n = 13 \cdot 19$ and $e = 47$

A	S	S	I	G	N	M	E	N	T
00	18	18	08	06	13	12	04	13	19

$n = p \times q = 13 \cdot 19 = 247$

$k = (p-1)(q-1) = (13-1)(19-1) = 216$

$e = 47 \quad (1 < e < 216(k))$

$GCD\ (47, 216) = 1$

$C = 0018^{47} \bmod 247$

$C = 180^{847} \bmod 247$

$C = 0613^{47} \bmod 247$

$C = 1204^{47} \bmod 247$

$C = 1819^{47} \bmod 247$

Q#16

a) Total offices per floor × NO of floors = 36×27

Total offices = 999

b) Colors = 12 ⇒ size = 3 ⇒ sex = 2

Total types of shirts = 12×3×2 = 72 different types of shirts

Q#17 a) Total Initials: 26 26 26 ⇒ $2^3 = 17576$ different three Initials

b) Total Initials = 26×54×24 ⇒ 15,600

So there are 15,600 different three-letter Initials.

Q#18

a) Total WEP Keys $= 16^{10} + 16^{26} + 16^{58} \Rightarrow 6.902 \times 6^{9}$

b)

All strings $= 26 \times 26 \times 26 \times 26 = 26^4$

No x in string $= 25 \times 25 \times 25 \times 25 = 25^4$

x in string = All string − No x in string

$= 26^4 - 25^4 \Rightarrow 66351$

Q19

a) No of elements $= m$

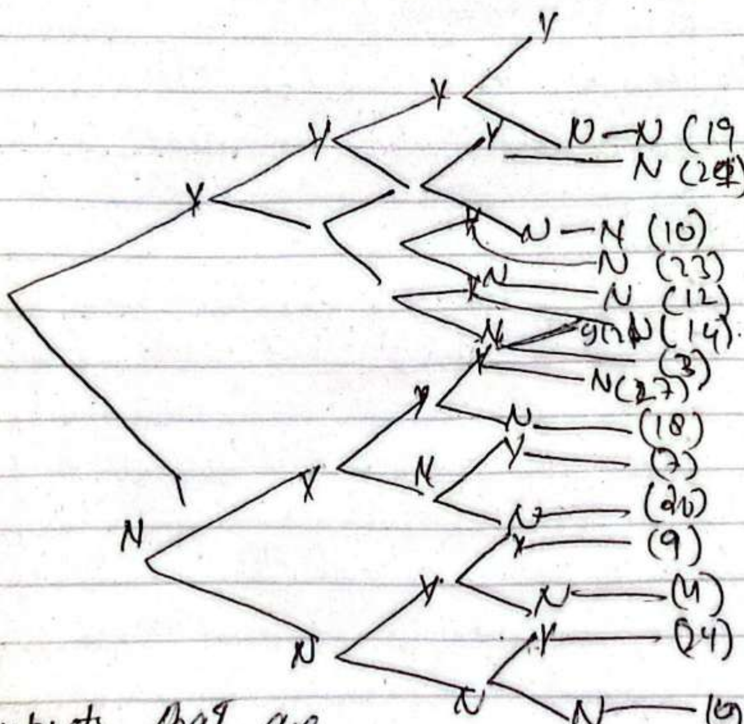
Possibilities $= 2$

So there are 2^m function

b) No of elements $= 5$

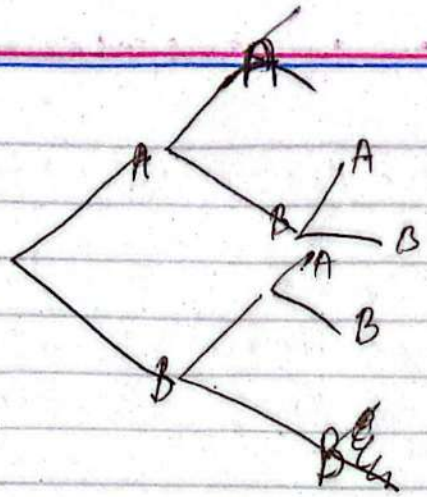
$5 \times 4 \times 3 \times 2 \times 1 = 5! = 120$

Q#20 a) 3 7 9 11



17 subsets that are less than 28

b)



= 6 ways

Q#21

a) $C(n,k)$

$n=8 \quad k=3$

$C(8,3) = \frac{8!}{3!(5!)} \Rightarrow 56$

56 ways to chose 3 drum majors from a pool of students.

b) $C(12,6)$

$\binom{12}{6} = \frac{12!}{6!(12-6)!} \Rightarrow 924$ ways to select elective courses

(c) $C(9,5)$

$\binom{9}{5} = \frac{9!}{5!(9-5)!} \Rightarrow 126$ ways to chose a 5 person basketball team

Q#23 a) $P(20,5) = \frac{20!}{(20-5)!} = 1860480$ ways

(b) $(16,4) = \frac{16!}{(16-4)!} = \frac{16!}{12!} \Rightarrow 43680$ ways

(c) $P(15,2) = \frac{15!}{13!} = 210$ ways

Q#23 a)

Total Combination = $C(5,1)+C(3,2)+C(4,1)+C(6,3)$

$\Rightarrow \frac{5!}{(5-1)!} \times \frac{3!}{2!(3-2)!} \times \frac{4!}{(4-1)!} \times \frac{6!}{3!(6-3)!} = 5\times3\times4\times20 = 1200$ ways

b) Total No of faces = Hairline × Eyes × Eyebrows × Nose × mouth × Chains × Cheeks

$= 15 \times 48 \times 24 \times 34 \times 28 \times 28 = 460615680$ diffrent faces

Q#24

a) A = string that begin with three 0's

B = string that ends with two 0's

$|A| = 2^7$

$|B| = 2^8$

$|A \cap B| = 2^5 \Rightarrow |A \cup B| = |A| + |B| - |A \cap B| = 2^7 + 2^8 - 2^5$

$128 + 256 - 32 \Rightarrow 352$

b) A = string begin with 0

B = string end with 1's

$|A| = 2^4$, $|B| = 2^3$

$|A \cap B| = 2^2$

$|A \cup B| = |A| + |B| - |A \cap B| \Rightarrow 2^4 + 2^3 - 2^2 \Rightarrow 16 + 8 - 4 = 20$

Q#25

a) $N = 30$, $K = 26$ $\left\lceil \frac{30}{26} \right\rceil = \lceil 1.153 \rceil = 2$

Hence proved there are at least two students who have last names that begins with same letters.

b) $N = 8,008,278$

$K = 1,000,000 \Rightarrow \left\lceil \frac{8,008,278}{1,000,000} \right\rceil \Rightarrow 9.008827$

$\Rightarrow 9$ hence proved that people who had the same amount of hair on their head

c) $N = 677 \quad r = 38$

$\Rightarrow \left[\frac{677}{38}\right] \Rightarrow 17.815 \Rightarrow 18$ different can will be needed

Q#26

a) x^7 Coefficient = ?

$(1+x)^{11}$

$r = 5$

$^{11}C_5 (x)^5 (1)^{11-5} \Rightarrow 462 x^5$ Coefficient of x^5 is 462

b)

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

To find r :-

$(b)^r (a)^{24-r} = a^7 b^{17}$

$b^r a^{24-r} = a^7 b^{17} \Rightarrow b^r = b^{17} \qquad a^{24-r} = a^7$

$r = 17 \qquad 24 - r = 7 \quad r = 17$

$^{24}C_{17} (-b^{10}) 2a^{24-17}$

$-346404 b^{17} \times 2^7 a^7$

$\Rightarrow -44301312 a^7 b^{17}$

The Coefficient of $a^7 b^{17}$ is -44301312

Q27 a) No of student = 36

$36!$ ways to put all students in a row

b) Row $36 \times 35 \times 34 \times 33 \times 32 \times 31 \times 30$ Or $^{36}P_7$

4.2072×10^{10} ways

c) 20 women left, 16 men right

$20! \times 16!$ ways

Q#28 a) 3 question each

$C(15,3) \times C(12,3) \times C(7,3) \times C(5,3) \times C(9,3) \times C(10,1)$

$\Rightarrow \frac{15!}{3!(15-3)!} \times \frac{12!}{3!(12-3)!} \times \frac{7!}{3!(7-3)!} \times \frac{5!}{3!(5-3)!} \times \frac{9!}{3!(9-3)!} \times \frac{10!}{1!(10-1)!}$

b) No of students = 97
No of grades = 10

$\left\lceil \frac{N}{K} \right\rceil = \left\lceil \frac{97}{10} \right\rceil = 9.7 \Rightarrow 10$ Studen

c) For Captain:- $P(15,1) = \frac{15!}{14!} = 15$

For Vice Captain :- $P(14,1) = \frac{14!}{13!} = 14$

For wicketkeeper (2nd) $\frac{2!}{1!} = 2$

$15 \times 14 \times 2 = 420$ total ways

Q#29 a) Pascal triangle (six rows)

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5  10  10   5   1
    1   6  15  20  15   6   1
```

b) $(3x-2)^4$

$(3x-2)^4 = {}^4C_0 (3x)^4 (-2)^0 + {}^4C_1 (3x)^3 \cdot (-2)^1 + {}^4C_2 (3x)^2 (-2)^2 + {}^4C_3 (3x)^1 (-2)^3 + {}^4C_4 (3x)^0 (-2)^4$

$(3x-2)^4 = 81x^4 - 216x^3 + 216x^2 - 96x + 16$

Q#30

a) let $n=6$

$2^6 - 1 = 64 - 1 = 63$ not prime let $n=7$

$2^7 - 1 = 128 - 1 = 127$ is prime

b) Proof By Contradiction

$\frac{a}{p} = k$, $\frac{a+1}{p} = j$

$a = kp$, $a+1 = jp$

$kp + 1 = jp$

$1 = JP - KP$

$1 = P(J-K)$

Let $J-K = r \Rightarrow 1 = Pr$ or $r = 1/p$

P is prime thus It not possible

Q#31 a) $a=16 \quad b=0$

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

$4=4$

Contradiction is true if $a=16$ and $b=0$

b)

Proof by Contrapositive if $|x| < 1$ and $x \geq -1$ Then $|x| \leq 1$ for all $x \in R$

If $x \leq 1$ & $x \geq 1 \Rightarrow -1 < x \leq 1$

i.e $-1 \leq x \leq 1$

$|x| < 1$

Let $x = 1/2 \Rightarrow 1/2 < 1 \rightarrow -1 \leq 1/2 \leq 1$ Hence proved

Q#32 (a) Counter Example

Let $n=2$

$n+2 = 2+2 = 4$ which is not prime let $n=7$

$n+2 = 7+2 = 9$ (not prime)

Hence proved for prime n, $n+2$ is prime

b) $P_1, P_2, P_3 \ldots P_k$ be all prime

Every prime num divides the product $P_1 P_2 P_3 \ldots P_k$

$(2 \times 3 \times 5 = 30)$ Consider num $P_1 P_2 P_3 \ldots P_{n+1} =$

$(2 \times 3 \times 5 + 1 = 31)$ It can't be prime

because It is larger than the largest prime

so it must be dividable by at least 1 prime

Say P_2 Then $P_2 P_1 P_2 \ldots$ and $P_k (P_1 P_2 \ldots P_n$

$\Rightarrow P_k (P_1 P_2 P_3 \ldots P_{n+1}) - (P_1 P_2 \ldots P_n) \Rightarrow P_k \} 1$

- so no prime can divide 1 so it means our assumption is false and statement is false

Q#33 a)

n & m are odd then n+m is also odd

Contradiction $n = 2a+1$, $m = 2b+1$

$n+m = 2a+1+2b+1 \Rightarrow 2a+2b+2$

$2(a+b+1) \Rightarrow 2q+2b+r$

$n+m$ 2q

Contradiction is false ∎

b) Proof By Contrapositive

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

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

$= 2k+2l+1 \Rightarrow 2(k+l)+1$ $R = k+l$

$= 2R+1$ is odd hence proved

Q#74 a)

Proof By Contradiction

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

$6-7\sqrt{2} = \frac{a}{b}$

$-7\sqrt{2} = a/b = -6$

$\sqrt{2} = \frac{6b-a}{7b} = \frac{A_1}{B_1} \Rightarrow A_1 = 6b-a$ $B_1 = 7b$

$\sqrt{2}$ is rational Hence our assumption is wrong statement is True

b)

Proof by Contradiction

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

$\sqrt{2}+\sqrt{3} = a/b$

Squaring on bth

$2+3+2\sqrt{6} = a^2b^2$

$5+2\sqrt{6} = a^2b^2$

$2\sqrt{6} = a^2/b^2 = -5$

$\sqrt{6} = \frac{a^2-5b^2}{2b^2}$

Hence our assumption is wrong ad statement is True

Q#35 a) $n=1$

(1) $= \frac{1(1+1)(2(1)+1)}{6} = \frac{6}{6} = 1 = L.H.S = R.H.S$

Put $n=k$

$P(k) = 1^2+2^2+3^2+\cdots k^2$

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

Now Put $k+1=n$

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

Add $(k+1)^2$ on b/s

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

$\Rightarrow \frac{k(k+1)(2k+1)+6(k+1)^2}{6} \Rightarrow (k+1)\left(\frac{2k^2+k+6k+6}{6}\right)$

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

$\Rightarrow \frac{(k+1)(2k(k+2)+3(k+2))}{6} \Rightarrow \frac{(k+1)(k+2)(2k+3)}{6}$

b) Put $n=0$

$a^0 = a^{0+1}-1$

$1 = 1$ ~~Addition~~ = RHS

Put $n=k$

$P(k) = 1+2+2^2+\cdots a^k = a^{k+1}$

add a^{k+1} on b/s

$a^k + a^{k+1} = a^{k+1}-1+a^{k+1}$

$\rightarrow a^{k+1}(1+1)-(1)$

$a^{k+2}-1$ proof

a

c) Put n=1

$(1)^3 = \frac{1(1)^2(1+1)^2}{4} \Rightarrow \frac{4}{4} = 1$ RHS proved LHS

Put n=k

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

let $n = k+1$

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

Add $(k+1)^3$ on b/s

$k^3+(k+1)^3 = \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \Rightarrow (k+1)^2\left(\frac{1}{4}k^2+(k+1)\right)$

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

$\frac{1}{4}(k+1)^2(k+2)^2$ proved!

(a) Combinations:

1. Password Generation :- In Cybersecurity, combinations are used to generate strong and unique passwords. By selecting combination of characters, including letters, numbers, and symbols, password generators create secure login credentials.
2. Team Formation :- When forming teams or committees combinations can be used to ensure diversity or specific skill sets. For example in a workplace a combination of employees with different expertise may be selected for a project team.

(b) Permutations

1. Algorithm Designer Permutation play a crucial role in algorithm for tasks like sorting and searching Algorithm like quick sort use permutations to efficiently reorder data.
2. Music Playlist Shuffle :- When you shuffle a playlist on a music app, it generates permutation of songs. This ensures that the order of song is random and enjoyable for the listener.

(c) Binomial Theorem :-

1. Statistics and Survey :- In survey sampling the binomial theorem can be used to estimate population parameters from a sample, it plays a role in calculating confidence interval and margin of error

2. Genetics and Biology:- The binomial theorem is applied in genetics to predict the likelihood of specific genetic traits being passed on from one generation to the next. It helps model inheritance pattern.

(d) Proof Methods

1. Cryptography:- Proof methods especially in number theory, are used to design and analyze cryptographic algorithm. Proofs are essential to ensure the security of encryption schemes.

2. Legal System:- Legal Proffessionals use proof method to establish evidence and argument in court cases, Rigrous proof techinique are employed to support claims and counter arguments.

(e) Mathematical Induction

1. Computer Science:- Mathematical Induction is used in computer science to prove properties of algorithms and data structure. It helps analyze the correctness and efficiency of algorithms

2. Education:- Mathematical Induction is often taught as a problem-solving techique in mathematical education. It helps students develop logical reasoning and proof-writing skills.