19MA20059

Discrete Mathematics | Keerti P. Charantimath

Test 4

2) $a_n = 6a_{n-1} - 8a_{n-2} + n4^n$, $n \geq 2$, $a_0 = 8$, $a_1 = 22$

Homogeneous part

$a_n = 6a_{n-1} - 8a_{n-2}$

Substituting $a_n = x^n$

$x^n = 6x^{n-1} - 8x^{n-2}$

$x^2 = 6x - 8$

$x^2 - 6x + 8 = 0 \implies x = 2, 4$

$a_n^{(h)} = A_1(2)^n + A_2(4)^n$

Particular part

$a_n - 6a_{n-1} + 8a_{n-2} = n4^n$

$f(r) = r4^r \implies$ 4 is a characteristic root of multiplicity 1

19MA20059

General form $\Rightarrow$ $a_n = (P_1 n + P_2) 4^n . n^1$

Substituting general form in the given $eq^{\underline{n}}$

$$(P_1 n + P_2) n 4^n = 6(P_1(n-1)+P_2) 4^{n-1} (n-1)$$
$$- 8(P_1(n-2)+P_2) 4^{n-2} (n-2)$$
$$+ n 4^n$$

$$P_1 n^2 4^n + P_2 n 4^n = (6P_1 n - 6P_1 + 6P_2)(n-1) 4^{n-1}$$
$$- (8P_1 n - 16P_1 + 8P_2)(n-2) 4^{n-2}$$
$$+ n 4^n$$

$$\cancel{P_1 n^2 4^n} + \cancel{P_2 n 4^n} = \cancel{4^{n-1} n^2 . 6P_1} - \cancel{4^{n-1} P_1 6n} + \cancel{6n P_2 4^{n-1}}$$

$$16 P_1 n^2 + 16 P_2 n = 4(n-1)(6P_1 n - 6P_1 + 6P_2)$$
$$- (n-2)(8P_1 n - 16P_1 + 8P_2)$$
$$+ 16n$$

$$16P_1 n^2 + 16P_2 n = 24n^2 P_1 - 24P_1 n + 24P_2 n$$
$$- 24P_1 n + 24P_1 - 24P_2$$
$$- 8P_1 n^2 + 16P_1 n - 8P_2 n$$
$$+ 16P_1 n - 32P_1 + 16P_2 + 16n$$

Equating coefficients of n^2, n & 1

for $n^2 \Rightarrow$ $16P_1 = 24P_1 - 8P_1 \longrightarrow 16P_1 = 16P_1$

for $n \Rightarrow$ $16P_2 = -24P_1 + 24P_2 - 24P_1 + 16P_1 - 8P_2$
$+ 16P_1 + 16$

19MA20059

$\cancel{16P_2} = -16P_1 + \cancel{16P_2} + 16$

$\boxed{P_1 = 1}$

for 1 $\Rightarrow$ $0 = 24P_1 - 24P_2 - 32P_1 + 16P_2$

$0 = -8P_1 - 8P_2$

$P_1 + P_2 = 0$

$1 + P_2 = 0$

$\boxed{P_2 = -1}$

$\therefore a_n^{(P)} = (n-1)n\,4^n = (n^2-n)4^n$

$\therefore$

$a_n = a_n^{(h)} + a_n^{(P)}$

$a_n = A_1 2^n + A_2 4^n + (n^2-n)4^n$

now, $a_0 = 8$ | $a_1 = 22$

$8 = A_1 + A_2$ | $\cancel{22} = \cancel{2}A_1 + \cancel{4}A_2 + 0$

$8 = A_1 + A_2$ | $11 = A_1 + 2A_2$

$A_2 = 3$, $A_1 = 5$

$\boxed{\therefore a_n = (5 \times 2^n) + (3 \times 4^n) + (n^2-n)4^n}$

Page No.:

19MA20059

4) Let $a, b \in G$

$n, n+1, n+2 \rightarrow$ 3 consecutive integers

Let

$(ab)^n = a^n b^n \longrightarrow (1)$

$(ab)^{n+1} = a^{n+1} . b^{n+1} \longrightarrow (2)$

$(ab)^{n+2} = a^{n+2} b^{n+2} \longrightarrow (3)$

$(2) \rightarrow (ab)(ab)^n = a.a^n.b.b^n$

$a.b.a^n.b^n = a.a^n.b.b^n$

$b.a^n = a^n.b$ [cancellation law]

$(3) \rightarrow (ab)(ab)^{n+1} = a.a^{n+1}.b.b^{n+1}$

$a.b.a^{n+1}.b^{n+1} = a.a^{n+1}.b.b^{n+1}$

$b.a^{n+1} = a^{n+1}b$ (cancellation law)

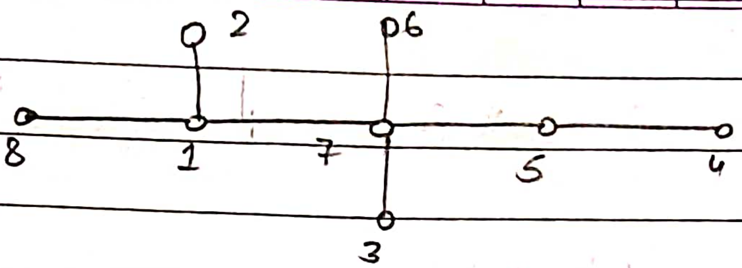
$b.a^n.a = a^n.a.b$

$a^n.b.a = a^n.a.b$

$ba = ab$ (left cancellation law)

Hence, G is an abelian group.

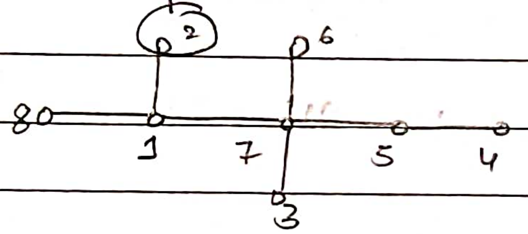
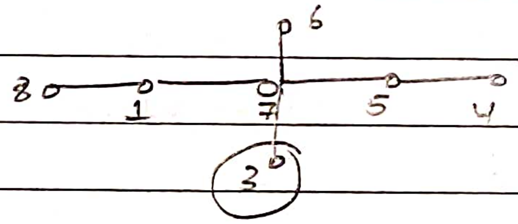
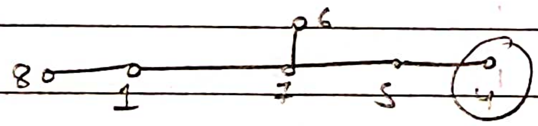
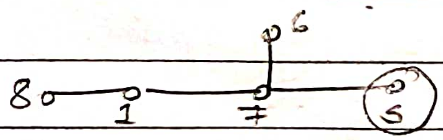
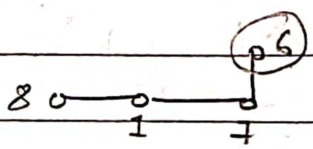
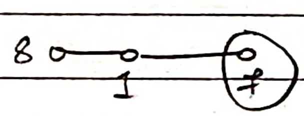
19 MA 20059

1) 

Algorithm (for Prüfer code) :-

→ Choose vertex with smallest label and degree=1. Delete it from tree and note down the neighour.

→ Repeat this until the tree is exhausted

	vertices with degree = 1	sequence
	{8, 2, 6, 3, 4}	—
	{8, 6, 3, 4}	1
	{8, 6, 4}	1, 7
	{8, 6, 5}	1, 7, 5
	{8, 6}	1, 7, 5, 7
	{8, 7}	1, 7, 5, 7, 7

19MA20059

 $\{8, 1\}$ | 1, 7, 5, 7, 7, 1

Tree exhausted.

Prüfer code for the given tree is
$\{1, 7, 5, 7, 7, 1\}$

6) Given :- E is ~~a~~ the modular elliptic curve defined by
$$y^2 = x^3 + 6x \pmod{13}$$

i)

x	$x^3+6x \pmod{13}$	in QR(13)	y
0	0		
1	7	no	
2	7	no	
3	6	no	
4	10	yes	$6, 13-6=7$
5	12	yes	$5, 13-5=8$
6	5	no	
7	8	no	
8	1	yes	$1, 13-1=12$
9	3	yes	$4, 13-4=9$
10	7	no	
11	6	no	
12	6	no	

19MA20059

$QR(13) = \{1, 4, 9, 3, 12, 10\}$

$E = \{(0,0), (4,6), (4,7), (5,5), (5,8),$
$(8,1), (8,12), (9,4), (9,9), O\}$

no. of points in $E = 10$

ii) Let $P = (4,7) = (x_1, y_1) = (x_2, y_2)$

$P + P = 2P = (x_3, y_3) = (4,7) + (4,7)$

$x_3 = m^2 - x_1 - x_2$ $\qquad m = \frac{3x^2 + 7}{2y'}$

$y_3 = m(x_1 - x_3) - y'$

$m = \frac{3(4)^2 + 7}{2(7)} \mod (13)$

$= 55 \times 14^{-1} (\mod (13))$

$= 55 \mod (13)$

$= 3 \mod (13)$

$m = 3$

Now, $x_3 = 3^2 - 4 - 4 \ (\mod (13))$

$= 1 \mod 13$

$\boxed{x_3 = 1}$

$y_3 = 3(4-1) - 7 \ (\mod (13))$

$\boxed{y_3 = 2}$

$\boxed{\therefore (4,7) + (4,7) = (1,2)}$

19MA20059

iii) Let $P = (4,7) = (x_1, y_1)$

$Q = (5,5) = (x_2, y_2)$

$R = (x_3, y_3) = P + Q$

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-7}{4-7} \bmod (13) = -2 \times (-1)^{-1} \bmod (13)$

$m = 11 \bmod (13)$

$\boxed{m = 11}$

$x_3 = (11)^2 - 4 - 5 \bmod (13) = 112 \bmod (13)$

$\boxed{x_3 = 8}$

$y_3 = 11(4-8) - 7 \bmod (13) = -51 \bmod (13)$

$\boxed{y_3 = 1}$

$\therefore \boxed{(4,7) + (5,5) = (8,1)}$

19MA20059

3) i) Let : p = probability that a person has disease

q = " " " doesn't have disease

given :- $p = 1/50$

$q = 1 - p = 49/50$

Given :-

P_n = Probability that the n^{th} studies person has disease & no one else before this person has the disease

$P_n = q^{n-1} p$ (q fairlures + 1 success)

$= \frac{49^{n-1}}{50^n}$, $n \geq 1$

Probability generating function

$$\boxed{G(x) = \sum_{n=1}^{\infty} \frac{49^{(n-1)}}{50^n} x^n = \sum_{n=1}^{\infty} q^{n-1} p x^n}$$

$$G(x) = xp \sum_{n=1}^{\infty} (qx)^{n-1} = \frac{px}{1-qx} = \frac{x}{50-49x}$$

Page No.:

19MA20059

ii) $G'(x) = \sum_{n=1}^{\infty} n q^{n-1} p x^{n-1}$ ($G'(1) \rightarrow$ expectation)

$G'(1) = \sum_{n=1}^{\infty} n q^{n-1} p$

Expectation $= p \sum_{n=1}^{\infty} n q^{n-1}$

Let $G'(1) =$ Expectation $= E(X)$

$E(X) = p(1 + 2q + 3q^2 + 4q^3 + \dots) \rightarrow (1)$

$q(E(X)) = p(q + 2q^2 + 3q^3 + 4q^4 + \dots) \rightarrow (2)$

(1) − (2)

$E(x)(1-q) = p(1 + q + q^2 + \dots)$

$= \frac{p}{1-q}$

$\therefore E(x) = \frac{\cancel{p}}{\cancel{p}} \cdot 1$

$E(x) = \frac{1}{p} = \frac{1}{1/50} = 50$

$\Rightarrow$ Expected no. of persons to be examined including the person with disease $= \boxed{50}$

$\Rightarrow \therefore$ Expected no. of persons to be examined before finding a person with disease $= 50 - 1 = \boxed{49}$

19MA20059

Variance $= G''(1) + G'(1) - (G'(1))^2$

$G''(x) = \dfrac{50(-2) \times (-49)}{(50-49x)^3} = \dfrac{4900}{(50-49x)^3}$

$G''(1) = 4900$

Variance $= 4900 + 50 - (50)^2 = 2450$

19MA20059

Page No.:

5)

i) $GF(2^3) = GF(8) \quad \bmod (x^3+x+1)$

$111 = x^2+x+1$

if we consider $\langle x \rangle$, then $GF/\{0\}$ forms a cyclic group of order 7

$x^0 = 1$; $x^3 = x+1$; $x^6 = x^2+1$

$x^1 = x$; $x^4 = x^2+x$; $x^7 = 1 = x^0$

$x^2 = x^2$; $x^5 = x^2+x+1$

so we can write 111 as x^5

For inverse, let it be 'a'

$(x^2+x+1)(a) \equiv 1 \bmod (x^3+x+1)$

$x^5 . a \equiv 1$

$a = x^{-5}$

$a . x^7 = x^{-5} . x^7$

$a = x^2$

$\boxed{\text{Inverse} = x^2 \quad (100)}$

since $111 = x^5$, to find square root we can express it as

$x^5 = x^5(1) = x^5 x^7 = x^{12}$

19MA20059

and $(x^6)^2 = (x^{6\times 2}) = x^{12}$

$x^5 \cdot x^7 = (x^6)^2$

$x^5 = (x^6)^2$

$\boxed{\therefore \text{square root of } 111 = x^6 = x^2+1 \quad (101)}$

Inverse of 111 = 100
square root of 111 = 101

ii) Quadratic residues means it is a perfect square and every element is a perfect square

Quadratic residue of

$0 \Rightarrow 0 = 000$

$x^0 \Rightarrow 1 = 001$

$x^1 \Rightarrow x^2 = 100$

$x^2 \Rightarrow x^4 = x^2+x = 110$

$x^3 \Rightarrow x^6 = x^2+1 = 101$

$x^4 \Rightarrow x^8 = x = 010$

$x^5 \Rightarrow x^{10} = x^3 = x+1 = 011$

$x^6 \Rightarrow x^{12} = x^5 = x^2+x+1 = 111$