Assignment : 1

Part - A

1. SOLUTION -

$a \in Z_p$ (given)

$(a+p)^n (\bmod p) = ({}^nC_0 a^0 p^n + {}^nC_1 a^1 p^{n-1} + \dots + {}^nC_n a^n)$ (mod p)

$= a^n \bmod p$

Since , $p^r \pmod p = 0$

Hence, proved .

2.

$Z_5 = \{1, 2, 3, 4\}$

a	1	2	3	4
a^{-1}	1	3	2	4

such that $aa^{-1} = 1 \pmod 5$

where $a \in Z_5$

$Z_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

Such that $aa^{-1} = 1 \pmod{11}$

where $a \in Z_{11}$

Scanned by CamScanner

2)

i) $n = 3^4$

$$\phi(p^k) = p^{k-1}(p-1)$$

$$= 3^3(3-1) = 27 \times 2 = 54$$

ii) 2^{10}

$$\phi(2^{10}) = 2^9(2-1) = 524$$

3) $\gcd(56245, 43159)$

$56245 = 43159 * 1 + 13086$

$43159 = 13086 * 3 + 3901$

$13086 = 3901 * 3 + 1383$

$3901 = 1383 * 2 + 1135$

$1383 = 1135 * 1 + 248$

$1135 = 248 * 4 + 143$

$248 = 143 * 1 + 105$

$143 = 105 * 1 + 38$

$105 = 38 * 3 + 29$

$38 = 29 * 1 + 9$

$29 = 9 * 3 + 2$

$9 = 2 * 4 + 1$

$2 = 1 * 2 + 0$

Scanned by CamScanner

$\therefore \gcd = 1$

5) $3^{100} \pmod{31319}$

$100 = 1100100$

$= 2^6 + 2^5 + 2^2$

$3^{100} = 3^{2^6 + 2^5 + 2^2} \pmod{31319}$

$= (12185 \times 21979 \times 14415) \pmod{31319}$

$= \cancel{17850}\ 25879$