Assignment - 1

Part-A.

1.) $(a+p)^n \pmod p = {}^nC_0\, a^n p^n + {}^nC_1\, a^1 p^{n-1} + \dots + {}^nC_n\, a^n \pmod p$

$= a^n \bmod p$

since $p^n \pmod p = 0$

Hence proved.

2.) $\mathbb{Z}_5 = \{1, 2, 3, 4\}$

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

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

where $a \in \mathbb{Z}_5$

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

$a =$	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 $a \in \mathbb{Z}$

4.) d) $n = 3^4$

$\therefore$ 3 is a prime wrt $\phi(p^e) = p^e - p^{e-1}$.

$\Rightarrow \phi(3^4) = 3^4 - 3^{4-1}$

$= 3^4 - 3^3 = 54$

$\phi(2^{10}) = 2^{10} - 2^9 = 1024 - 512 = 512$ //

3.) Euclidean algorithm to find GCD.

gcd (56,245, 43,159)

56 245 = 43159 × 1 + 13056

43159 = 13086 × 3 + 3901

13086 = 3901 × 3 + 1383

3901 = 13853 × 2 + 1155

13853 = 1 × 1135 + 248

1135 = 248 × 4 + 143

248 = 1 × 143 + 105

143 = 1 × 105 + 38

105 = 38 × 2 + 24

38 = 29 × 1 + 9

29 = ~~9×3+2~~ 4 × 3 + 2

9 = 2 × 4 + 1

2 = 1 * 2 + 0

∴ gcd = 1.

5.) $3^{100} \bmod (31319)$

100 = 1100100

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

$(3)^{100} = (3)^{2^6 + 2^5 + 2^2}$

$3^{100} \bmod (31319) = \left((3)^{2^6} \times (3)^{2^5} \times (3)^{2^2}\right)$
$(\bmod 31319)$

$(3)^{24} \pmod{31319} = ?$

$(3)^{2^5} = \left((3)^2\right)^2 = 9 = 9 \pmod{31319}$

$(3)^{2^2} = \left(3^{2^1}\right)^2 = 9^2 \pmod{31319}$

$= 81 \pmod{31319}$

~~= 81 (mo~~

$(3)^{2^4} = \left(3^{2^3}\right)^4$

$= (6261)^2 \pmod{31319}$

$= 14415.$

$(3)^{2^5} = \left(3^{2^4}\right)^2 = (14415)^2 \bmod (31319)$

$= 21979$

$(3)^{2^6} = \left(3^{2^3}\right)^2 = 12185$

$3^{100} \pmod{31319} = 25829 \pmod{31319}$