$(3)^{2^0} \pmod{31319} = 3$

$(3)^{2^1} = ((3)^{2^0})^2$

$\Rightarrow 9 \cancel{(\bmod 31319)}$

$(3)^{2^2} = (3^{2^1})^2$

$\Rightarrow 9^2 \pmod{31319}$

$\Rightarrow 81 \cancel{(\bmod 31319)}$

$(3)^{2^3} \Rightarrow (81)^2 \bmod (31319)$

$\Rightarrow 6561 \cancel{(\bmod 31319)}$

$(3)^{2^4} \Rightarrow (3^{2^3})^2$

$\Rightarrow (6561)^2 \pmod{31319}$

$\Rightarrow 14415 \cancel{(\bmod 3131)}$

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

$\Rightarrow 207792225 \pmod{31319}$

$\Rightarrow 21979$

$(3^{2^6}) = (3^{2^5})^2 \Rightarrow (21979)^2 \pmod{31319}$

$\Rightarrow 12185$

$\Rightarrow (3)^{100} \pmod{31319} \Rightarrow (12185 \times 21979 \times 81) \bmod 31319$

$\Rightarrow 25829$

~~Check~~ ~~the~~ ~~Primitive~~
~~Roots~~ ~~of~~ $\cancel{Z_{19}}$

ASSIGNMENT

PART A

1A) Given,

$a \in Z_p$

$(a+p)^n \pmod p = a^n \pmod p$

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

$\Rightarrow (0+0+0 \cdots + 0 + a^n) \bmod p$

$\Rightarrow a^n \pmod p$

2A) Z_5 :-

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

$a^{-1} = \{1, 2, 3, 4\}$

Z_{11} :-

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

~~$a^{-1} = \{1, 6, 4, 3, 9, 2, 8, 7\}$~~

$a^{-1} = \{1, 6, 4, 3, 9, 2, 8, 7, 5, 10\}$

3A) Euclidean algorithm to find gcd

gcd (56245, 43159) :

56245 = 1 × 43159 + 13086

43159 = 3 × 13086 + 3901

13086 = 3 × 3901 + 1383

3901 = 2 × 1383 + 1135

1383 = 1 × 1135 + 248

1135 = 4 × 248 + 143

248 = 1 × 143 + 105

143 = 1 × 105 + 38

105 = 2 × 38 + 29

38 = 1 × 29 + 9

29 = 3 × 9 + 2

9 = 4 × 2 + 1

2 = 2 × 1 + 0

gcd = 1

4A) $\phi(3^4)$

$\because$ 3 is a prime, wkt $\phi(p^e) = p^e - p^{e-1}$

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

$\Rightarrow 3^3(3-1)$

$\Rightarrow 27 \times 2$

$\Rightarrow 54$

$\phi(2^{10}) \Rightarrow 2^{10} - 2^9$

$\Rightarrow 1024 - 512$

$\Rightarrow 512$

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

100 = 1100100

$\Rightarrow 2^6 + 2^5 + 2^2$

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

$\Rightarrow (3)^{2^6} * (3)^{2^5} * (3)^{2^2}$

$3^{100} \bmod (31319) \Rightarrow ((3)^{2^6} \cdot (3)^{2^5} \cdot (3)^{2^2}) \bmod (31319)$