

1.) Given  $a \in \mathbb{Z}_p$

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

$$= \left( nC_0 a^n + nC_1 a^{n-1} p + nC_2 a^{n-2} p^2 + \dots + nC_n a^0 p^n \right) \bmod p$$

$$= (0 + 0 + 0 + \dots + a^n) \bmod p$$

$$= a^n \bmod p$$

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

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

3.) Euclidean Algorithm to find GCD  
 $\gcd(56245, 43159) = ?$

$$56245 = 1 \times 43159 + 13086$$

$$43159 = 3 \times 13086 + 3901$$

$$13086 = 3 \times 3901 + 1883$$

$$3901 = 2 \times 1383 + 1135$$

$$1383 = 1 \times 1135 + 248$$

$$1135 = 4 \times 248 + 143$$

$$248 = 1 \times 143 + 105$$

$$143 = 1 \times 105 + 38$$

$$105 = 2 \times 38 + 29$$

$$38 = 1 \times 29 + 9$$

$$29 = 3 \times 9 + 2$$

$$9 = 4 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$\gcd(56245, 43159) = 1$$

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

$\because 3$  is a prime w.r.t  $\phi(p^k) = p^k - p^{k-1}$

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

$$= 3^4 - 3^3 = 3^3(3-1)$$

$$= 27 \times 2 = 54$$

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

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

$$100 = 1100100$$

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

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

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

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

$$3^2 \bmod 31319 = 9$$

$$3^4 \bmod 31319 = 81$$

$$3^{2^3} \bmod 31319 = 6561$$

$$3^{2^4} \bmod 31319 = 14415$$

$$3^{2^5} = (14415)^2 \bmod 31319 = 21979$$

$$3^{2^6} = (21979)^2 \bmod 31319 = 12185$$

$$3^{100} \bmod 31319 = 25879 \bmod 31319$$