**NUMBER THEORY**

1. a^(b^c) mod m = a^((b^c) mod n) mod m, where n = φ(m) Euler's totient function.
2. Phi of n = n\*(Product of (1-(1/p))) where p is a prime factor of n which is considered only ONCE. ----> Eulers totient Function
3. ap  = a (mod p). ------> Fermats little theorum.(for any p that doesnot divide a)
4. Chinese Remainder Theorum :-

x % num[0] = rem[0],   
x % num[1] = rem[1],   
.......................  
x % num[k-1] = rem[k-1]

SMALLEST SUCH x = ( SUM OF (rem[i]\*pp[i]\*inv[i]) ) % prod  
Where 0 <= i <= n-1  
  
**rem[i]** is given array of remainders  
  
**prod** is product of all given numbers  
prod = num[0] \* num[1] \* ... \* num[k-1]  
 **pp[i]** is product of all divided by num[i]  
pp[i] = prod / num[i]  
 **inv[i]** = Modular Multiplicative Inverse of   
 pp[i] with respect to num[i]