Fermat's Theorem Applications:

Compute 6^{10} mod 11= 6^{11-1} mod 11=1

If a ≡ b mod n ,then a mod n=b

Find 3^{12} mod 11

Properties of Modular arithmetic:

(a+b) mod n= (a mod n +b mod n)mod n

(a-b) mod n= (a mod n -b mod n)mod n

(a*b) mod n= (a mod n * b mod n)mod n

3^{12} mod 11= (3^{11} * 3) mod 11=((3^{11} mod 11) * (3 mod 11)mod 11 =(3 *3)mod 11=9

Second application:

a^{-1} mod p= a^{p-2} mod p

8^{-1} mod 17 = 8^{17-2} mod 17= 8^{15} mod 17=15

Euler's Theorem:

First version: If a and n are coprime,then $a^{Ø(n)}$ ≡ 1 (mod n)

Second version:It removes the condition that a and n should be coprime.if n= P* q,a<n and k is an integer,then $a^{k * Ø(n)-1}$ ≡ a (mod n)

Ø(n) is euler's t function

Ø(n) =Z_n*

Properties:

1. **Ø(1) =0**
2. **Ø (p)=p-1 if p Is prime**
3. **Ø (m * n) = Ø (m) * Ø (n) if m and n are relatively prime**
4. **Ø (p^e) = P^e - P^{e-1} ,If p is prime**

Compute 6^{24} mod 35 using Euler's theorem ANS :1
Compute 8^{-1} mod 77 using Euler's theorem ANS :29

What is Ø(240), Ø(10)
6^{24} mod 35 =$6^{Ø(35)}$ mod 35

Ø(7 * 5)= Ø(7) * Ø(5) =6 *4 =24

$\text{Ø}(240)=\text{Ø}(2^4 * 3^1 * 5^1)$
$\text{Ø}(240)=(2^4 - 2^3) * (3^1 - 3^0) * (5^1 - 5^0)=64$