

Abdur Rahmon Bijoy  
ID: IT-21056

Q-1

Fermat's Little Theorem (FLT):

If  $p$  is a prime and  $a \neq 0 \pmod{p}$ , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof:

Let  $a \in \mathbb{Z} : p \text{ prime}, a \neq 0 \pmod{p}$

Consider the set  $\{a, 2a, 3a, \dots, (p-1)a\}$

all are distinct  $\pmod{p}$  so

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$$

Cancelling  $(p-1)!$  (invertible  $\pmod{p}$ )  $\rightarrow$

$$a^{p-1} \equiv 1 \pmod{p}$$

$a^{p-1} \pmod{p}$  for  $a = 2, p = 13$

$$\therefore 2^{12} \equiv 1 \pmod{13}$$

prove that  $13$  is prime and  $2$  is not divisible by  $13$ .

## Use in cryptography :

- \* FLT, Vmdurpms, modular inverse and modular exponentiation are crucial in RSA.
- \* RSA key generation relies on Euler's theorem.

## Question - 2

Compute  $\varphi(n)$ :

$$\varphi(n) = n \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

1.  $n = 35 = 5 \cdot 7$

$$\varphi(35) = 35 \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$$

2.  $n = 45 = 3^2 \cdot 5$

$$\varphi(45) = 45 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 24$$

3.  $n = 100 = 2^2 \cdot 5^2$

$$\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

## Euler's theorem

If  $\gcd(a, n) = 1$  then  $a^{\varphi(n)} \equiv 1 \pmod{n}$

### Proof sketch:

\*  $n$  has  $\varphi(n)$  elements

\*  $a$  acts as a permutation on this group

$$a^{\varphi(n)} \cdot (m_1 \cdot m_2 \cdots m_{\varphi(n)}) = (n_1 \cdot n_2 \cdots n_{\varphi(n)}) \pmod{n}$$

\* Cancelling the common product.

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

## Question-3

Step-1: Understand the process

$3, 4, 5$  are pairwise coprime, and their product is  $N = 3 \times 4 \times 5 = 60$

$$\text{Let, } m_1 = 3, a_1 = 2$$

$$m_2 = 4, a_2 = 3$$

$$m_3 = 5, a_3 = 1$$

Step2: Compute  $N_i = \frac{N}{m_i}$

$$N_1 = \frac{60}{3} = 20$$

$$N_2 = \frac{60}{4} = 15$$

$$N_3 = \frac{60}{5} = 12$$

Step 3: find  $M_i$

$$M_i \equiv N_i^{-1} \pmod{n_i}$$

$$\text{find } M_1 \equiv 20^{-1} \pmod{3}$$

$$\text{We want } 20M_1 \equiv 1 \pmod{3}$$

$$20 \equiv 2 \pmod{3}$$

$$2M_1 \equiv 1 \pmod{3} \Rightarrow M_1 = 2$$

$$\text{find } M_2 \equiv 15^{-1} \pmod{4}$$

$$15 \equiv 3 \pmod{4}$$

$$3M_2 \equiv 1 \pmod{4} \Rightarrow M_2 = 3$$

$$\text{Find } M_3 \equiv 12^{-1} \pmod{5}$$

$$12 \equiv 2 \pmod{5}$$

$$2M_3 \equiv 1 \pmod{5} \Rightarrow M_3 = 3$$

Step 4:

$$x \equiv a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \pmod{N}$$

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \pmod{60}$$

$$x \equiv 80 + 135 + 36 \equiv 251 \pmod{60}$$

$$x \equiv 251 \pmod{60} \Rightarrow x \equiv 11 \pmod{60}$$

$$x \equiv 11 \pmod{60}$$

#### Question - 4

$$a^{n-1} \equiv 1 \pmod{n}$$

it follows Fermat's Little Theorem.  $\gcd(a, n) = 1$ .

Check if 561 is composite

$$\text{factors of } 561 = 3 \times 11 \times 17$$

so 561 is a composite

Use Konstelt's Criterion

A number  $n$  is a Carmichael number if and only if

\*  $n$  is square free

\* For every prime divisor

$\therefore 561$  is a Carmichael number

Now,

$$a = 2$$

$$\text{compute } 2^{560} \pmod{561} \equiv 1$$

$$a^{2^5}$$

$$\gcd(5, 561) = 1 \rightarrow$$

$$a^{2 \cdot 10} \cdot \gcd(10, 561) = 1$$

$$a^{2 \cdot 5^2} \pmod{561} \equiv 1$$

### Question - 05

To find primitive root modulo 17,

$$\mathbb{Z}_{17} = \{1, 2, \dots, 16\}$$

Since 17 is prime the order of the group is  $\phi(17) = 16$

so we want  $g^k \not\equiv 1 \pmod{17}$  for any  $k < 16$  and  $g^{16} \equiv 1 \pmod{17}$ .

test small values of  $g$ .

Let's test  $g = 3$

Compute  $3^k \pmod{17}$  for  $k = 1$  to 16

$$3^1 = 3 \pmod{17}$$

$$3^2 = 9$$

$$3^3 = 10$$

$$3^4 = 13$$

$$3^5 = 5$$

$\vdots$

$$3^6 = 1$$

$3$

$\therefore 3$  is a primitive root modulo 17.