Abdur Rahman Bijoy
ID: IT-21056

Q-1

Fermat's Little theorem (FLT):

If p is a prime and $a \neq 0 \mod p$, then

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

proof:

Let $a \in Z$ · p prime · $a \neq 0 \mod p$

consider the set: $\{a, 2a, 3a, \ldots (p-1)a\} \mod p$

all are distinct mod p so,

$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \mod p$

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

cancel $(p-1)!$ (invertible mod p) →

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

$a^{p-1} \mod p$ for $a = 7, p = 13$

$\therefore 7^{12} \equiv 1 \mod 13$

prove that 13 is prime and 7 is not divisible by 13.

Use in cryptography:

* FLT underpins modular inverse and modular exponentiation, crucial in RSA.
* RSA key generation relies on Eulers theorem.

Question - 2

Compute $\varphi(n)$:

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

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

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

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

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

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

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

Eulers theorem

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

proof sketch:

* n has $\varphi(n)$ elements
* a acts as a permutation on this group

$$a^{\varphi(n)} \cdot (m \cdot m_2 \cdots m_{\varphi(n)}) = (n_1 m_2 \cdots m_{\varphi(n)}) \bmod n$$

* cancelling the common product.

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

Question-3

Step-1: Understand the process

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

Let, $n_1 = 3 \cdot a_1 = 2$

$n_2 = 4, a_2 = 3$

$n_3 = 5, a_3 = 1$

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

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

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

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

Step 3: find M_i

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

Find $M_1 = 20^{-1} \bmod 3$

We want $20M_1 \equiv 1 \bmod 3$

$20 \equiv 2 \bmod 3$

$2M_1 \equiv 1 \bmod 3 \Rightarrow M_1 \equiv 2$

Find $M_2 = 15^{-1} \bmod 4$

$15 \equiv 3 \bmod 4$

$3M_2 \equiv 1 \bmod 4 \Rightarrow M_2 = 3$

Find $M_3 = 12^{-1} \bmod 5$

$12 \equiv 2 \bmod 5$

$2M_3 \equiv 1 \bmod 5 \Rightarrow M_3 = 3$

Step: 4

$x = a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \bmod N$

$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \bmod 60$

$x \equiv 80 + 135 + 36 \equiv 251 \bmod 60$

$x \equiv 251 \bmod 60 \Rightarrow x \equiv 11 \bmod 60$

$x \equiv 11 \pmod{60}$

Question-4

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

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

check if 561 is composite

factor $561 = 3 \times 11 \times 17$

So 561 is a composite

Use Korselt'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,

$a = 2$

compute $2^{560} \bmod 561 \equiv 1$

$a \geq 5$

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

$a \geq 10 \cdot \gcd(10, 561) = 1$

$10^{560} \bmod 561 = 1$

Question - 05

To find primitive root modulo 17.

$Z_{17} = \{1, 2, \ldots, 16\}$

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

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

test small values of g

Let's test $g = 3$

Compute $3^k \bmod 17$ for $k = 1$ to 16

$3^1 = 3 \bmod 17$.

$3^2 = 9$

$3^3 = 10$

$3^4 = 13$

$3^5 = 5$

$\vdots$

$3^{16} = 1$

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