10/02/21

Lecture 10

Topic : Modular Arithmetic & Number Theory

1. Fermat's Theorem
2. Euler's Theorem
3. Chinese Remainder Theorem
4. Steganography

1.

FERMAT'S THEOREM

Fermat's Theorem plays an important role in Cryptography. To understand this theorem, one needs to have basic knowledge of GCD, Prime numbers & Prime Factorisation.

Theorem: For any prime number p, 'a' is the integer which is not divisible by p, then

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

A variant of this theorem is :-

If p is a prime no. & a is a coprime to p (i.e gcd (a,p) = 1), then

$$a^p \equiv a \pmod p \longrightarrow (2)$$

Basically this theorem is useful in public key cryptography such as RSA.

2.

Examples on Fermat's Theorem

(1) Let's have $a = 3$, $p = 5$

Eq. 1 & 2, both are satisfied. So we will test both the equations with these values.

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

$\Rightarrow 3^4 \Rightarrow 81$

$\therefore 81 \bmod 5 \Rightarrow 1$

Hence $a^{p-1} \equiv 1 \bmod p$

$\because a^p \equiv a \pmod p$

$\therefore 3^5 \Rightarrow 243$

Also $3 \pmod 5 = 3$

Now, if we take 243 mod 5, it will give same result

$\because 243 \equiv 3 \pmod 5$

$\therefore (243) \bmod 5 \equiv (3 \bmod 5) \bmod 5$

$\Rightarrow 3 = 3 \quad \therefore$ LHS = RHS

(2) Solve : $6^{10} \bmod 11$

Sol: Acc. to Fermat's Theorem

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

Hence $p - 1 = 10$, $a = 6$

$\therefore p = 11$

Hence $6^{10} = 1 \bmod 11$

Now, $6^{10} \Rightarrow (6^8 \bmod 11)\ (6^2 \bmod 11) \bmod 11$

$\Rightarrow (4 \times 3) \bmod 11$

$\Rightarrow 1$

$\therefore 6^{10} \bmod 11 = 1$

Q.3 Solve $3^{10} \bmod 11$

Homework Question

3.

EULER'S TOTIENT FUNCTION

$\phi(n)$ is called as Euler's Totient Function which states that how many numbers are between 1 and $n-1$ that are relatively prime to n.

For example, if $n = 4$, $\phi(4) = 1, 3 = 2$ because they are relatively prime to 4.

Euler's Theorem:

It states that for every a & n that are relatively prime:

$$a^{\phi(n)} = 1 \pmod n$$

For example : Prove using Euler's Theorem,

$a = 3$, $n = 10$, $\phi(10) = ?$

Sol: $\phi(n) = \phi(10) = \{1, 3, 7, 9\} = 4$

Then according to Euler's Theorem:

$3^4 = 1 \pmod{10}$

$\therefore 3^4 = 81$

$\therefore 81 \bmod 10 = 1$ As LHS = RHS

Hence Proved.

CHINESE REMAINDER THEOREM

A famous problem was presented as : There are certain numbers repeatedly divided by 3 and remainder is 2, repeatedly divided by 5 and remainder is 3 and repeatedly divided by 7 and remainder is 2.

What will be that number??

$$\left.\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ x &\equiv a_3 \bmod m_3 \end{aligned}\right\} \text{Find the value of } x$$

Where m_1, m_2 & m_3 are relatively prime

$\therefore \gcd(m_1, m_2) = \gcd(m_1, m_3) = \gcd(m_2, m_3) = 1$

Also, $M = m_1 \times m_2 \times m_3 \cdots m_r$

$\therefore x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 \cdots + M_r X_r a_r) \bmod M$

where, $M_i = \frac{M}{m_i}$, &

$1 . a_1 \bmod m_1$

$M_i X_i \equiv 1 \pmod{m_i}$

Example

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 3 \pmod{11}$

Find x

Sol Here $a_1 = 1$, $a_2 = 1$, $a_3 = 3$

$m_1 = 5$, $m_2 = 7$, $m_3 = 11$

$\therefore x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3)$

$\because M = 5 \times 7 \times 11 = 385$

$M_1 = \frac{385}{5} = 77$

$M_2 = \frac{385}{7} = 55$

$M_3 = \frac{385}{11} = 35$

$\therefore 77 X_1 \equiv 1 \pmod 5$

$55 X_2 \equiv 1 \pmod 7$

$35 X_3 \equiv 1 \pmod{11}$

Congruence means mod on either side should give same result. We can take mod n. no. of times.

i.e $77 X_1 \equiv 1 \pmod 5$

$\Rightarrow 77 \bmod 5 . X_1 \equiv 1 \pmod 5 \pmod 5$

$\Rightarrow 2 X_1 \equiv 1 \pmod 5$ Multiply by 3

$\Rightarrow 6 X_1 \equiv 3 \pmod 5$

$\Rightarrow 1 . X_1 \equiv 3$

$\Rightarrow \boxed{X_1 = 3}$

Now, $55 X_2 \equiv 1 \pmod 7$

$55 \pmod 7) X_2 \equiv 1 \pmod 7 \pmod 7$

$[6 X_2 \equiv 1 \pmod 7] \times 6$

$36 X_2 \equiv 6 \pmod 7$

$36 \pmod 7)\ X_2 \equiv 6$

$\boxed{X_2 = 6}$

Similarly,

$35 X_3 \equiv 1 \pmod{11}$

$\Rightarrow 35 \pmod{11}\ X_3 \equiv 1 \pmod{11} \pmod{11}$

$\Rightarrow [2 X_3 \equiv 1 \bmod 11] \times 6$

$\Rightarrow 12 X_3 \equiv 6 \bmod 11$

$\Rightarrow 12 \pmod{11}\ X_3 \equiv 6$

$\Rightarrow 1 . X_3 \equiv 6$

$\Rightarrow \boxed{X_3 = 6}$

$\therefore x = [(77 \times 3 \times 1) + (55 \times 6 \times 1) + (35 \times 6 \times 3)] \bmod M$

$= (1191) \bmod 385$

$= 36$