Afsana Akter Mim
IT-21004

Assignment-2: Number Theory Theorems Part 1

1. Bazeout Theorem Proof and Example [inverse of 101 mod 4620]

Statement:- If a and b are integers with $\gcd(a,b) = d$ then there exist integers x and y such that:

$$ax + by = d.$$

In particular, if $\gcd(a,b) = 1$ then $ax + by = 1$.

This is used to find the modular inverse of a modulo b.

Example: Find the inverse of 101 mod 4620

We need to find x such that:

$$101x \equiv 1 \mod 4620$$

This means we need:

$$101x + 4620y = 1$$

we will use the extented Euclidean Algorithm:

Step 1: Apply Euclidean Algorithm to find gcd (4620, 101)

$4620 = 45 \times 101 + 75$

$101 = 1 \times 75 \times 5$

$75 = 2 \times 26 + 23$

$26 = 1 \times 23 + 3$

$23 = 7 \times 3 + 2$

$3 = 1 \times 2 + 1$

$2 = 2 \times 1 + 0 \longrightarrow$ Done.

So, $\gcd(101, 4620) = 1$

Step 2: Work backward to express 1 as a linear combination

$1 = (26 \times 1575) \times 101 - 35 \times 4620 = 1601 \times 101$

$= 35 \times \cdot 4620$

So, $1601 \times 101 - 35 \times 4620 = 1$

∴ Modular inverse of ~~100~~ 101 mod 4620 is

$\boxed{1601}$

2. Chinese Remainder Theorem (Prove)

Statement:-

If we have a system of congruences:

$$x \equiv a_1 \mod m_1$$
$$x \equiv a_2 \mod m_2$$
$$\vdots$$
$$x_k \equiv a_k \mod m_k$$

and all moduli $m_1, m_2 \dots m_k$ are pairwise coprime, then there is a unique solution modulo $M = m_1, m_2, \dots m_k$

Proof:

Let, $M = m_1 m_2 \dots m_k$ Define

$$M_i = \frac{M}{m_i}$$

For each i, find the modular inverse y_i of M_i mod m_i i.e.

$$m_i y_i \equiv 1 \mod m_i$$

Then, the solution is:

$$x = \sum_{i=1}^{k} a_i M_i y_i \mod M$$

This works because each term $a_i M_i y_i \equiv a_i \mod m_i$ and $\equiv 0 \mod m_j$ for $j \neq i$ hence satisfies all the congruences.

3. Fermat's Little Theorem – Proof and Example.

Statement: If p is a prime and a is not divisible by p, then:

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

Proof: The numbers $1, 2, \ldots, p-1$ from a complete residue system mod p. Multiply each by a (since a is not divisible by p) the set:

$$a \times 1,\ a \times 2, \ldots, a \times (p-1)$$

Hence:

$$a^{p-1}(1\times2\times\cdots\times(p-1)) \equiv 1\times2\times\cdots\times(p-1) \bmod p$$

Cancelling $(p-1)!$

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

Example : compute $7^{222} \bmod 11$

Here, $p=11$, $a=7$

By Fermats Little Theorem

$$7^{10} \equiv 1 \bmod 11$$

break 222: $222 = 10\times22+2$

So,

$$7^{222} = (7^{10})^{22} \times 7^{2}$$

$$\equiv 1^{22} \times 7^{2} \bmod 11$$

$$= 49 \bmod 11$$

Now,

$$49 \bmod 11 = 5$$