Number Theory Theorems - Part 1

1. Bazeout Theorem Proof and Example: Inverse of 101 mod 4620.

Sol^n:

Bézout's Identity states that if a and b are integers with a greatest common divisor $d = \gcd(a, b)$, then there exist integers x and y such that:

$$ax + by = d$$

Proof:

Consider the set S of all linear combinations of a and b that result in a positive integer:

$$S = \{ma + nb \mid m, n \in \mathbb{Z}, ma + nb > 0\}$$

Since at least one of a or b is non-zero, the set S is not empty. For example, if $a \neq 0$, then $|a| = (\pm 1)a + 0b$ will be in S.

By the Well-Ordering Principle, since S is a non-empty set of positive integers, it must have a smallest positive integer element. Let's call this smallest element d. Because d is in S, there exist integers x and y such that:

$$ax+by=d$$

Now, our goal is to show that this d is indeed the greatest common divisor of a and b. We need to show two things:

1. d is a common divisor of a and b:

Suppose d does not divide a. Then by the Division Algorithm, we can write $a=qd+r$, where q is the quotient and r is the reminder, with $0<r<d$. Substituting $d=ax+by$ into this equation, we get:

$$r=a-qd=a-q(ax+by)=a(1-qx)+b(-qy)$$

This shows that r is also a linear combination of a and b. Since $0<r<d$, r is a positive integer that is smaller than the smallest positive integer in S, which is d. This is a contradiction. Therefore our initial assumption that d does not divide a

must be false. Thus, d divides a.

Similarly, we can show that d divides b. Suppose d doesnot divide b. Then $b = q'd + r'$, where $0 < r' < d$. Substituting $d = ax + by$, we get:

$$r' = b - q'd = b - q'(ax+by) = a(-q'x) + b(1 - q'y)$$

Again; r' is positive linear combination of a and smaller than d, which is a contradiction,

Therefore, d must divide b.

Since d divides both a and b, it is a common divisor of a and b.

(B) 2. Any common divisor of a and b also divides d:

Let c be any common divisor of a and b. This means that there exist integers K and l such that $a = Kc$ and $b = lc$. Substituting these into the equation $d = ax + by$, we get:

$$d = (Kc)x + (lc)y = c(Kx + ly)$$

Since $kx+ly$ is an integer, this equation shows that c divides d.

Since d is a common divisor of a and b, and any other common divisor c also divides d, d must be the greatest common divisor of a and b.

Therefore, $d = \gcd(a, b)$

This completes the proof of Bézout's Identity.

Find the inverse of 101 mod 4620

we want to find x such that:

$$101x \equiv 1 \pmod{4620}$$

This means we need to solve:

$$101x + 4620y = 1$$

Using Bezout Theorem

Step1: Apply the Euclidean Algorithm

we divide until the remainder is 0:

$$4620 = 45 \times 101 + 75 \longrightarrow 1$$

$101 = 1\times75+26 \longrightarrow (2)$

$75 = 1\times26+23 \longrightarrow (3)$

$26 = 1\times23+3 \longrightarrow (4)$

$23 = 7\times3+2 \longrightarrow (5)$

$3 = 1\times2+1 \longrightarrow (6)$

$2 = 2\times1+0 \longrightarrow$ (Done)

So, $\gcd(101, 4620) = 1$, so inverse exists

Step 2: Back-substitute to express 1 as a combination of 101 and 4620

From step(6):

$$1 = 3 - 1\cdot2$$

From step(5): $2 = 23 - 7\cdot3$

$$1 = 3 - 1(23 - 7\cdot3) = 8\cdot3 - 1\cdot23$$

From step (4): $3 = 26 - 1\cdot23$

$$1 = 8(26 - 1\cdot23) - 1\cdot23 = 8\cdot26 - 9\cdot23$$

From step (3) :- $23 = 75 - 2 \cdot 26$

$$1 = 8 \cdot 26 - 9(75 - 2 \cdot 26) = 8 \cdot 26 - 9 \cdot 75 + 18 \cdot 26 \; \cancel{= (8+18) \cdot 26 = 97}$$

$$= (8+18) \cdot 26 - 9 \cdot 75$$

$$= 26 \cdot 26 - 9 \cdot 75$$

From step(2) :

$$26 = 101 - 1 \cdot 75$$

$$1 = 26(101 - 1 \cdot 75) - 9 \cdot 75 = 26 \cdot 101 - 26 \cdot 75 - 9 \cdot 75$$

$$= 26 \cdot 101 - (26+9) \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot 75$$

From step (1) : $75 = 4620 - 45 \cdot 101$

$$1 = 26 \cdot 101 - 35(4620 - 45 \cdot 101) = 26 \cdot 101 - 35 \cdot 4620 + 1575 \cdot 101$$

$$= (26 + 1575) \cdot 101 - 35 \cdot 4620$$

$$= 1601 \cdot 101 - 35 \cdot 4620$$

Final result :

$$1 = 1601 \cdot 101 - 35 \cdot 4620$$

So the inverse of 101 mod 4620 is :

$$101^{-1} \equiv 1601 \pmod{4620}$$

Answer : 1601

2. Chinese Remainder Theorem (CRT) - Proof

Statement:

Let $n_1, n_2, \ldots n_K$ be pairwise coprime integers and $a_1, a_2 \ldots a_K \in \mathbb{Z}$. Then the system:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_K \pmod{n_K}$$

has a unique solution modulo $N = n_1 n_2 \cdots n_K$

Proof Sketch:

Let $N = n_1 n_2 \cdots n_K$. For each i, define:

$$N_i = \frac{N}{n_i},$$ and find M_i such that

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

Then, define the solution:

$$x = \sum_{i=1}^{K} a_i N_i M_i \pmod{N}$$

Each term $a_i N_i M_i \equiv a_i \pmod{n_i}$ and $\equiv 0 \pmod{n_j}$ for $j \neq i$

3. Fermat's Little Theorem - Proof and Example:

Theorem:

If p is a prime number and $a \not\equiv 0 \pmod{p}$ then:

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

Proof:

Let $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. The set $\{1, 2, \ldots, p-1\}$ forms a multiplicative group modulo p.

Then multiplication by a permutes this set:

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

All values are distinct modulo p. So the product of the original and the permuted set are congruent modulo p:

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

(After canceling $(p-1)!$, which is nonzero mod p)

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

Use Fermat's Little Theorem:

$7^{10} \equiv 1 \bmod 11$ (since 11 is prime)

Now:

$$222 = 10 \cdot 22 + 2$$

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

$$\Rightarrow 7^{222} = 1^{22} \cdot 7^{2} = 49 \bmod 11$$

$$= 49 - 4 \cdot 11$$

$$= 49 - 44$$

$$= 5$$

Answer: $7^{222} \equiv 5 \pmod{11}$