# Number Theory Theorem - Part 1

① Bazeout theorem proof and Example :

Inverse of 101 mod 4620.

Soln.

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.

Let's call this smallest element d. Because d is in S, there exist integers $x$ and $y$ such that,

$ax+by=d$.

Tanzina Fatema, IT21005

Tanzina Fatema, IT21005

Now, our goal is to show that 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 doesnot 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,

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

r is positive linear combination of a and smaller than d, which is a cotradiction

2. Any common divisor of a and b also divised d:

Let c be any common divisor of a and b. This means that there exist integers k and

Such that $a = kc$ and $b = lc$. Substituting these into the equation, $d = ax + by$, we get:

$d = (kc)x + (lc)y = c(kx + y)$.

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

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

This completes the proof of Bézout's identity:

Find the inverse of 101 ~~a~~ 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,

Apply the euclidean Algorithm,

step 1: We divide until the remainder is 0:

$4620 = 45 \times 101 + 75$ —— (1)

Tanzina Fatema, IT21005

Tanzina Fatema, IT21005

$101 = 1 \times 75 + 26 \longrightarrow (2)$

$75 = 1 \times 26 + 23 \longrightarrow (3)$

$26 = 1 \times 23 + 3 \longrightarrow (4)$

$23 = 7 \times 3 + 2 \longrightarrow (5)$

$3 = 1 \times 2 + 1 \longrightarrow (6)$

$2 = 2 \times 1 + 0 \longrightarrow$ 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):

$$1 = 3 - 1.2$$

from step(5):

$$2 = 23 - 7.3$$

$$1 = 3 - 1(23 - 7.3) = 8.3 - 1.23$$

from step(4): $3 = 26 - 1.23$

$$1 = 8(26 - 1.23) - 1.23$$

$$= 8.26 - 9.23$$

Tanzina fatema, IT21005

from, step(3):

$$23 = 75 - 2.26$$

$$1 = 8.26 - 9(75 - 2.26)$$
$$= 8.26 - 9.75 + 18.26$$
$$= (8+18).26 - 9.75$$
$$= 26.26 - 9.75$$

from, step(2):

$$26 = 101 - 1.75$$

$$1 = 26(101 - 1.75) - 9.75$$
$$= 26.101 - 26.75 - 9.75$$
$$= 26.101 - (26+9).75$$
$$= 26.101 - 35.75$$

from step(1): $75 = 4620 - 45.101$

$$1 = 26.101 - 35(4620 - 45.101) = 26.101 - 35.4620 + 1575.101$$
$$= (26+1575).101 - 35.4620$$
$$= 1601.101 - 35.4620$$

final result:

$$1 = 1601.101 - 35.4620$$

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,

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

Proof sketch :

Let, $N = n_1 n_2 \ldots n_k$, for each $i$, define:

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

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

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 $j \neq i$.

Tanzina fatema, IT21005

Tanzina Fatema, IT21005

# ③ Fermat's little 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 $\{1, 2, \cdots p-1\}$ forms a multiplicative group modulo $p$.

Then, multiplication by $a$ permutes this set:

$$a_1, a_2, \cdots a_{(p-1)}$$

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

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

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

Use fermat's little theorem,

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

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

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

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

$$= 49 - 4 \cdot 11$$

$$= 49 - 44$$

$$= 5$$

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