1. Bazeout Theorem Proof and Example [inverse of $101 \mod 6120$]

⇒ Bézout's Identity:

For any integers a and b, not both zero, there ex integers x, y such that:

$$ax + by = \gcd(a, b)$$

Proof using well-ordering principle:

Step 1: Define a set

Let's define a set:

$$S = \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$

That is, S is the set of all positive integers that can be written as a linear combination of a and b

Step 2: Show that S is Non-Empty

Since a and b are not both zero, some combin $ax + by$ must be non-zero. We can always choose su x, y to make it positive (e.g., try $x = 1, y = 0$ or $x = 0, y = 1$).

So, S is a non-empty subset of N.

Step 3: Use well-ordering principle

Since $S \subseteq \mathbb{N}$ and is non-empty, it has a smallest element, say:

$$d = ax_0 + by_0 \text{ for some } x_0, y_0 \in \mathbb{N}$$

Step 4: Show that d Divides Both a and b

Now we show that $d \mid a$ and $d \mid b$

Let's divide a by d:

$$a = dq + r \quad \text{where } 0 \leq r < d$$

So, $r = a - dq = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$

But notice that $r \in S$ (it is a linear combination).

* If $r > 0$, then $r \in S$ and $r < d$, contradicting the minimality of d.
* So the only possibility is:

$$r = 0 \Rightarrow d \mid a$$

Similarly, we show $d \mid b$ by the same argument

Step 5: d is the Greatest Common Divisor:

So, d is a common divisor of a and b.

Now, suppose c is any common divisor of a and b, then

$$c \mid ax_0 + by_0 \Rightarrow c \mid d$$

So, d is divisible by every other common divisor

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

Therefore,

we have shown that,

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

$$d = ax_0 + by_0$$

$$\therefore \gcd(a, b) = ax_0 + by_0$$

So, the integers x_0, y_0 exists - this completes the proof.

Example:

Given that,

modular inverse of

$101 \mod 4620$

That is means: find x an integer x such that,

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

Or, in Bézout Identity form: $101x + 4620y = 1$

Step 1: Use the Euclidean Algorithm we compute gcd(4620, 101) first,

$4620 \div 101 = 45$ remainder $75 \rightarrow 4620 = 101 \times 45 + 75$
$101 \div 75 = 1$ remainder $26 \rightarrow 101 = 75 \times 1 + 26$
$75 \div 26 = 2$ remainder $23 \rightarrow 75 = 26 \times 2 + 23$
$26 \div 23 = 1$ remainder $3 \rightarrow 26 = 23 \times 1 + 3$
$23 \div 3 = 7$ remainder $2 \rightarrow 23 = 3 \times 7 + 2$
$3 \div 2 = 1$ remainder $1 \rightarrow 3 = 2 \times 1 + 1$
$2 \div 1 = 2$ remainder $0 \rightarrow 2 = 1 \times 2 + 0$

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

Step 2: Back-substitute

* $1 = 3 - 2 \times 1$
* $2 = 23 - 3 \times 7$

So, $1 = 3 - (23 - 3 \times 7) = 3 \times 8 - 23$

* $3 = 26 - 23 \times 1$

$1 = (26 - 23) \times 8 - 23 = 26 \times 8 - 23 \times 9$

* $23 = 75 - 26 \times 2$

$1 = 26 \times 8 - (75 - 26 \times 2) \times 9 = 26 \times 8 - 75 \times 9 + 26 \times 18 = 26 \times 26 - 75 \times 9$

* $26 = 101 - 75 \times 1$

$1 = (101 - 75) \times 26 - 75 \times 9 = 101 \times 26 - 75 \times 35$

* $75 = 4620 - 101 \times 45$

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

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

∴ Final result: $1 = 101 \times 1601 - 4620 \times 35$

so, the modular inverse of 101 mod 4620 is

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

2. Chinese Remainder Theorem - proof:

⇒ Theorem:

Let, $m_1, m_2, \ldots, m_k$ be pairwise coprime integers. Then the system:

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_k$.

Proof:

1. Define $M = m_1 m_2 \ldots m_k$
   For each i, define $M_i = \frac{M}{m_i}$
2. Since, $\gcd(M_i, m_i) = 1$, there exists a modular inverse y_i such that:
   $$M_i y_i \equiv 1 \bmod m_i$$
3. Define the solution:
   $$x = \sum_{i=1}^{k} a_i M_i y_i$$
4. Then for each i:
   * $M_j \equiv 0 \bmod m_i$ for $j \neq i$
   * $M_i y_i \equiv 1 \bmod m_i$

   So, $x \equiv a_i \bmod m_i$.

Hence, x satisfies all congruences.

5. If x' is another solution, then $x \equiv x' \bmod m_i \ \forall i$
   $\Rightarrow x \equiv x' \bmod M$
   So, the solution is unique modulo M.

So, $x \equiv \sum_{i=1}^{k} a_i M_i y_i \bmod M$

2. Fermat's Little Theorem - Proof - Example

$7^{222} \bmod 11$.

⇒ Fermat's Little Theorem:

Let p be a prime, and let a be any integer such that $\gcd(a,p) = 1$. Then:

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

Proof:

Step 1: Consider the set

$$S = \{1, 2, 3, 4, \ldots, p-1\}$$

These are the nonzero elements of $\mathbb{Z}_p$, the integers modulo p.

Step 2: Multiply each element of S by a

Create a new set:

$$aS = \{a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\} \bmod p$$

Step 3: Claim All elements in aS are distinct mod

Because $\gcd(a,p) = 1$, multiplication by a is a bijection (1-to-1 mapping) in $\mathbb{Z}_p^*$, the multiplicative group.

So:

$\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \equiv \{1, 2, \ldots, p-1\} \bmod p$ Just are rearranged.

Step 4: Multiply all elements of both sets

$$a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv a^{p-1} \cdot (p-1)!$$

So, $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

Step 5: Cancel $(p-1)!$

Because p is prime, and $(p-1)! \not\equiv 0 \bmod p$, we can cancel it (modulo a prime allows cancellation).

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

(proved)

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

⇒ 11 is a prime

∴ gcd (7, 11) = 1

So, Fermat's Little Theorem applies.

Fermat's Little Theorem says

$$7^{10} \equiv 1 \bmod 11 \quad \boxed{\text{Since } 11-1=10}$$

Now, Reduce the exponent mod 10

We want,

$$7^{222} \bmod 11$$

Break 222 as a multiple of 10

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

Now, $7^{10} \equiv 1 \bmod 11 \Rightarrow (7^{10})^{22} \equiv 1^{22} = 1 \bmod 11$

So, $7^{222} \equiv 1 \cdot 7^2 \equiv 49 \bmod 11$

Reduce $49 \bmod 11$

$49 \div 11 = 4$ remainder $5 \Rightarrow 7^{222} \equiv 5 \bmod 11$

$\therefore 7^{222} \bmod 11 = 5$