Bezeout Theorem

For any integers a and b, there exist integers x and y such that

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

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

1. Since, $S \subset \mathbb{Z}_{>0}$ and is non-empty, by the
2. well ordering Principle, it has a smallest element d.
3. Then $d = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$
4. For any common divisor c of a and b, $c|d$, so d is a common divisor
5. We prove $d|a$ and $d|b$ using the division algorithm and contradiction
6. Thus, $d = \gcd(a,b)$

Find the inverse 101 mod 4620

$$101x \equiv 1 \bmod 4620$$

$$\therefore 101x + 4620y = 1$$

1. Apply Euclidean algorithm

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

$$101 = 1 \times 75 + 26$$

$$75 = 2 \times 26 + 23$$

$$26 = 1 \times 23 + 3$$

$$23 = 7 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

working Backwards

$1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$1 = 8 \cdot 26 - 9(75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$

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

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

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

∴ The Inverse of 101 mod 4620 is

1601

Chinese Remainder Theorem

Let $n_1, n_2 \cdots n_k$ be pairwise coprime integers ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) and let $a_1, a_2, \cdots a_k$ be any integers. Then, the system of simultaneous congruences:

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ \vdots \\ x \equiv a_k \bmod n_k \end{cases}$$

2 moduto case

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{cases}$$

Step 1: use Bezout's Identity

Since, $\gcd(n_1, n_2) = 1$, there exist integers m_1 and m_2 such that

$$m_1 n_1 + m_2 n_2 = 1$$

Step-02 Construct sol^n.

$$x = a_1 m_2 n_2 + a_2 m_1 n_1$$

modulo n_1

$$x \equiv a_1 m_2 n_2 + a_2 m_1 n_1$$
$$\equiv a_1 \cdot 1 + a_2 \cdot 0 = a_1 \bmod n_1$$

Because $n_1 | n_2$ so $m_1 n_1 = 0 \mod n_1$ and

$m_2 n_2 = 1 \mod n_1$

modulo n_2

$x \equiv a_1 \cdot 0 + a_2 \cdot 1 \equiv a_2 \mod n_2$

Step - 3 Uniqueness.

modulo $N = n_1 n_2$

Eupt.

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 1 \mod 5 \end{cases}$$

Here, $n_1 = 3, n_2 = 4, n_3 = 5$

let $N = 3 \cdot 4 \cdot 5 = 60$

Now, for each i:

- $N_1 = 60/3 = 20$
- $N_2 = 60/40 = 15$
- $N_3 = 60/5 = 12$

Now compute modular inverse

$20^{-1} \mod 3 = 2$ because $20 \cdot 2 = 40 \equiv 1 \mod 3$

$15^{-1} \mod 4 = 3$

$12^{-1} \mod 5 = 3$.

$\therefore$

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3$$

$$x = 80 + 135 + 36 = 251$$

$$x \equiv 251 \pmod{60}$$

$$x \equiv 11 \pmod{60}$$

Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have

$$a^p = a \pmod{p}$$

~~Proof~~

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Eg. Find $7222 \bmod 11$

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$.

$$(7^{10})^k \equiv 1 \pmod{11}$$

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

$$\equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}$$

$\therefore (722 \bmod 11 = 5)$ Ans.