1. Bezout Theorem Proof:

If $\gcd(a,m)=1$, then there exist integers s and t such that,

$$sa + tm = 1$$

Taking modulo m:

$sa \equiv 1 \pmod{m} \Rightarrow s$ is the mod inverse of ~~a mod~~ $a \pmod{m}$

This gives a constructive proof for existence of modular inverse using the Extended Euclidean Algorithm.

Example: Inverse of 101 mod 4620

Using the Euclidean Algorithm:

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

Now back-substitute to express 1 as a linear combination of 101 and 4620:

$1 = 3 - 1 \times 2$

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

$= 8 \cdot 3 - 1 \cdot 23$

$= \cdots$

= Eventually ... $1837 \cdot 101 - 4 \cdot 4620$

∴ Inverse of 101 mod 4620 is 1837

because $101 \cdot 1837 \equiv 1 \mod 4620$

2 Chinese Remainder Theorem (CRT)

Let,

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Assume all m_i are pairwise coprime. Define:

$$M = m_1 \cdot m_2 \cdots m_n$$

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

Let, $y_i = M_i^{-1} \bmod m_i$

Then the solution is:

$$x \equiv \sum_{i=1}^{n} a_i \cdot M_i \cdot y_i \pmod{M}$$

This ensures:

→ $x \equiv a_i \mod m_i$

→ $x \mod M$ is unique solution modulo M

3 Fermat's Little Theorem:

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

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

Proof Idea:

- Consider the set $\{a, 2a, 3a, \cdots (p-1)a\} \bmod p$
- All are distict modulo p, so product of the set modulo p is same as $a^{p-1}(p-1)!$
- since $(p-1)! \not\equiv 0 \bmod p$, we can divide both sides to conclude:

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

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

Use Fermat's Little Theorem:

- Since 11 is prime and $\gcd(7, 11) = 1$
- $7^{10} \equiv 1 \bmod 11$

Break 222 as:

- $222 = 10 \cdot 22 + 2$
- So,

$$7^{222} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 49 \bmod 11$$

$$49 \bmod 11 = 49 - 4 \cdot 11 = 49 - 44 = 5$$

Ans: $7^{222} \bmod 11 = 5$.