1) Bezout's Theorem:

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

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

This is often used to find modular inverse when $\gcd(a, m) = 1$

example:

find inverse of 101 mod 4620

using extended Euclidean algorithm

$4620 = 45 \times 101 + 75$

$101 = 1 \times 75 + 26$

$75 = 2 \times 26 + 23$

$26 = 1 \times 23 + 3$

$23 = 7 \times 3 + 2$

$3 = 1 \times 2 + 1$

Back-substitute →

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

∴ So, inverse of 101 mod 4620 is 16

② chinese remainder theorem

statement:

If $n_1, n_2 \cdots n_k$ are pairwise coprime positive integers and $a_1, a_2 \cdots a_k$ are any integers then the system:

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

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

proof:

Let $N = n_1 n_2 \cdots n_k$.

$$N_i = \frac{N}{n_i} \text{ then } \gcd(N_i, n_i) = 1$$

By Bezout's theorem, there exists an inverse

$M_i \equiv N_i^{-1} \mod n_i$ such that:

$$N_i M_i \equiv 1 \mod n_i$$

Construct: $x = \sum_{i=1}^{k} a_i N_i M_i \mod N$

Each term $a_iN_iM_i$ satisfies:

$$a_iN_iM_i \equiv a_i \bmod n_i \text{ and } \equiv 0 \bmod n_j \text{ for } j \neq i$$

Thus $x \equiv a_i \bmod n_i$ for each i, ant the solution is unique module N

③ Fermat's Little theorem:

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

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

proof:

Let $a \not\equiv 0 \bmod p$ consider the set:

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

Each element in $S \bmod p$ is distinct and nonzero (since a is invertible mod p).

so:

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \bmod p$$

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

Since $(p-1)! \not\equiv 0 \bmod p$, we can cancel $(p-1)!$ on both sides:

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

Example:

Compute $7^{222} \bmod 11$

$p = 11$ (prime), $a = 7$ so

$7^{10} \equiv 1 \bmod 11$ (Fermat's Little Theorem)

Now,

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

$\Rightarrow (1)^{22} \cdot 49 = 49 \bmod 11$

$\Rightarrow 49 \bmod 11 = 5$