Fermat's Little Theorem:

Statement:

If 'p' is a prime and $a \not\equiv 0 \bmod p$. then

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

Proof Idea (using group theory):

i. The multiplicative group Z_p^* has $p-1$ elements

ii. Since it's a finite group the order of any element divides $p-1$

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

Chinese Remainders Theorem (CRT): Proof

Theorem statement:

Let $n_1, n_2, \dots, n_k$ be pairwise co-prime integers.

For any integers $a_1, a_2, \dots, a_k$ the system:

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$x \equiv a_k \bmod n_k$$

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

Bezout's Theorem: Proof and Example:

Theorem statement:

For any integers 'a' and 'b' There exist integers x and y such that:

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

This is Bezout Identity.

when $\gcd(a,b) = 1$, the Identity used to find the modular inverse of 'a' mod 'b'

Proof:

Let 'a' and 'b' be integers, and apply

Euclidean Algorithm: $a = bq_1 + r_1$

$$b = r_1 q_2 + r_2$$

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_{n-1} = r_n q_{n+1} + 0$$