Bezout's Theoram : Proof and Example :

Theoram 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 :

$$a = bq_1 + r_1$$

$$b = r_1 q_2 + r_2$$

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

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

Chinese Remainder Theorem (CRT): Proof

Theorem statement:

Let $n_1, n_2, \ldots n_K$ be pairwise coprime integers.

For any integers $a_1, a_2, \ldots a_K$ the system:

$$
\begin{aligned}
x &\equiv a_1 \bmod n_1 \\
&\vdots \\
x &\equiv a_2 \bmod n_2 \\
x &\equiv a_K \bmod n_K
\end{aligned}
$$

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

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 $p-1$ element

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

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