Name: Mirza Zisun
ID : IT-21020.

1. Bazeout theorem Proof (and example [Inverse of 101 mod 4620]

Theorem:

Let, a and b be integers, not both zero, then there exist integers x and y such as that:

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

the integers x and y can be found using the extended Euclidean Algorithm.

Proof of Bezout's identity:

Let, a and b be integers, not both zero.

1. Define the set $S = \{an + bx \mid n, y \in Z;\ an + by > 0\}$

Since, a and b are not both zero, s in non-empty.

2. By the well-ordering principle, s contains a least element. Let $d = ax_0 + by_0$ be the smallest positive

Value in s.

3. $d = \gcd(a,b)$

4. $d \div a = qd + r \Rightarrow r = a - qd$

5. $d = ax_0 + by_0$ · plug this in;

$r = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$

$r = 0$ implying $d|a$.

6. $d|b$

Example: Find Inverse of 101 modulo 4620.

$101n \equiv 1 \bmod 4620$

This means $101n + 4620y = 1$

$4620 = 45 * 101 + 75$

$101 = 1 * 75 + 25$

$75 = 2 * 26 + 23$

$26 = 1 * 23 + 3$

$23 = 7 * 3 + 2$

$3 = 1 * 2 + 1$

$2 = 2 * 1 + 0$

Sol: $1 = 1601 \cdot 101 - 35 \cdot 4620$

The Modular inverse of 101 mod 4620 is 1601.

Chinese Remainder theorem state and Proof:

Statement:

Let, $m_1, m_2 \dots m_k$ are Pairwise Prime integers,

$\gcd(m_i, m_j) = 1$

Let, $M = m_1 \cdot m_2 \dots m_k$

$$\begin{cases} x = a_1 \pmod{m_1} \\ x = a_2 \pmod{m_2} \\ \vdots \\ x = a_k \pmod{m_k} \end{cases}$$

Let, $m_1, m_2 \in \mathbb{Z}$ with $\gcd(m_1, m_2) = 1$

Step-1: $R_1 m_1 + R_2 m_2 = 1$

Step-2: $x = a_1 R_2 m_2 + a_2 R_1 m_1$

modulo m_1:

$x \equiv a_1 R_2 m_2 + a_2 R_1 m_1 \equiv a_1 R_2 m_2 \pmod{m}$

$m_2 \equiv 0 \bmod m_1$ is not true

$x \equiv a_1 \pmod{m_1}$

$x \equiv a \bmod m_2$

Given, $m_1, m_2 \dots m_k$ Pairwise coprime.

$M = m_1 m_2 \dots m_k$

$m_1 = \frac{M}{m_i}$

$\gcd(m_i, m_j) = 1$, be the inverse of $M_i \bmod m_i$

The solution is:

$$x = \sum_{i=1}^{k} a_i y_i m_i \bmod M.$$

this construction ensures:

$x \equiv a_i \bmod m_i$ for all

3. fermat's Little theorem Proof:

Statement: If p is a prime number and a is an integer not divisible by p, then

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

Equivalently:

$$a^p \equiv a \pmod p$$

Proof:

p be a Prime, $a \not\equiv 0 \bmod p$.

1. The set of non zero integers modulo p, denoted $Z_p^* = \{1, 2, \ldots, p-1\}$

2. In a finite group of order n, any element a statistics $a^n = 1$. So in Z_p for any $a \in Z_p$;

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

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

Since, 11 is Prime and gcd $(7, 11) = 7^{10} \equiv (\text{mod } 11)$

$7^{222} = 7^{220} \cdot 7^2 = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 7^2 \pmod{11}$

Now compute;

$7^2 \equiv 49 \Rightarrow 49 \bmod 11 = 5$

$\therefore 7^{222} \equiv 5 \mod 11.$