

Name: Minza Zisun

ID : IT-21020.

1. Base on theorem Proof

(and example) Inverse of

$101 \bmod 4620$

$$bp-a = n \in \mathbb{Z} \quad bp = a + b \cdot n$$

$$a + b \cdot n = b \cdot d + a \cdot x = b \cdot (d+x) = b$$

Theorem:

$$(bP-d) + (aP-1)a = (ad+bx)a = a$$

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

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

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 $S = \{an + by \mid n, y \in \mathbb{Z}; an + by > 0\}$

Since, a and b are not both zero, S is non-empty.

2. By the well-ordering principle, S contains a least element. Let $d = ax + by$ be the smallest positive

Value in s.

3. $d = \text{gcd}(a, b)$ first moment passed.

4. $d \div a = qd + r \Rightarrow r = a - qa$ first born to

5. $d = ax_0 + by_0$ plug this in; moment

$$r = a - q(a x_0 + b y_0) = a(1 - qx_0) + b(-qy_0)$$

implies, if a, sd d born to

if b divides B born x moment fails small

Example: Find Inverse of $f = 101$ modulo 4620.

$101n \equiv 1 \pmod{4620}$ or moment part

This means $101n + 4620y = 1$ because

$$4620 = 45 * 101 + 75$$

$$101 = 1 * 75 + 25$$

so, $75 = 2 * 26 + 23$ sd d born to

$$26 = 1 * 23 + 3$$

$$23 = 7 * 3 + 2$$

$$3 = 1 * 2 + 1$$

$$2 = 2 * 1 + 0$$

Sol: $1 = 101 * 101 - 35 * 4620$

The Modular inverse of $101 \pmod{4620}$ is 101 .

Chinese Remainder theorem (statement) and Proof;

Statement:

Let, m_1, m_2, \dots, m_k be ~~pairwise~~ prime integers such that

$\text{gcd}(m_i, m_j) = 1$ for all $i \neq j$.

Let, $M = m_1 \cdot m_2 \cdots m_k$ then $\text{bom} M \equiv 1$

$$\left\{ \begin{array}{l} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \end{array} \right. \text{But if this statement is}$$

$n \equiv a_k \pmod{m_k}$ then From statement

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

Step-1: $R_1 m_1 + R_2 m_2 = 1 \quad (\text{bom}) \quad 1 \equiv 1$

Step-2: $n = a_1 R_2 m_2 + a_2 R_1 m_1 \quad : \text{first solving}$

modulo m_1 : $(\text{bom}) \quad 0 \equiv 0$

$n \equiv a_1 R_2 m_2 + a_2 R_1 m_1 \equiv a_1 R_2 m_2 \pmod{m_1}$ Final

$m_2 \equiv 0 \pmod{m_1}$ is not true $\text{bom} \quad 0 \neq 0$

$n \equiv a_1 \pmod{m_1}$

$n \not\equiv a_1 \pmod{m_2}$ because $a_1 \neq a_2$ for S.T.

Given, m_1, m_2, \dots, m_k ~~pairwise~~ coprime.

$M = m_1 m_2 \cdots m_k$ ~~bom~~ to guess $n \equiv a_1 \pmod{m_1}$

$m_1 = \frac{m}{m_1}$ so $q = n \div m_1 \quad r = n \pmod{m_1}$

$\gcd(m_1, \dots, m_k) = 1$, let b_i be the inverse of $m_i \pmod{m_i}$

The solution is:

$$n = \sum_{i=1}^k a_i b_i m_i \pmod{M}$$

This construction ensures:

$$n \equiv a_i \pmod{m_i} \text{ for all } i$$

3. Fermat's Little Theorem Proof:

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

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

Equivalently:

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

Proof:

p be a prime, $a \not\equiv 0 \pmod{p}$

1. The set of non zero integers modulo p ,

denoted $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

2. In a finite group of order n , any element a satisfies $a^n = 1$. So in \mathbb{Z}_p^* for any $a \in \mathbb{Z}_p^*$,

mod with

0.505 - 11

Statement $a^{p-1} \equiv 1 \pmod{p}$ if and only if a is invertible mod p .

Example: Compute $7^{222} \pmod{11}$ $\rightarrow 185$

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

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

Now compute: $7 + 185 = 185 \leftarrow$

$$7^1 \equiv 49 \Rightarrow 49 \pmod{11} = 5$$

$$\therefore 7^{222} \equiv 5 \pmod{11}$$

See above note: $185 \rightarrow$ sum of digits of 185 is 18

$\Delta = (m, n)$ b/w 1 to $n-1$ \leftarrow invertible

(mod) $\Delta = k \cdot n \pmod{n}$ \leftarrow sum of digits

$$185 = 10 \pmod{9}$$

$$185 = 20$$

$$(mod) \Delta = n \cdot 185$$

Now, sum of digits of 185 is 18 \leftarrow invertible

$x = 185 \cdot 18 \pmod{11}$ \leftarrow sum of digits of 185 is 18 \leftarrow invertible

$x = 185 \cdot 18 \pmod{11}$ \leftarrow sum of digits of 185 is 18 \leftarrow invertible