Name: Md. Shahidul Islam

ID : IT-21024

Assignment: Bezout's Identity, Chinese Remainder Theorem, fermat's little theorem.

Number Theory Theorems - Part 1

1. Bazeout Theorem Proof and Example: Inverse of 101 mod 4620.

Sol^n:

Bézout's Identity states that if a and b are integers with a greatest common divisor $d = \gcd(a, b)$, then there exist integers x and y such that:

$$ax + by = d$$

Proof:

Consider the set S of all linear combinations of a and b that result in a positive integer:

$$S = \{ma + nb \mid m, n \in \mathbb{Z}, ma + nb > 0\}$$

Since at least one of a or b is non-zero, the set S is not empty. For example, if $a \neq 0$, then $|a| = (\pm 1)a + 0b$ will be in S.

By the Well-Ordering Principle, since S is a non-empty set of positive integers, it must have a smallest positive integer element. Let's call this smallest element d. Because d is in S, there exist integers x and y such that:

$$ax + by = d$$

Now, our goal is to show that this d is indeed the greatest common divisor of a and b. we need to show two things:

1. d is a common divisor of a and b:

Suppose d does not divide a. Then by the Division Algorithm, we can write $a = qd + r$, where q is the quotient and r is the reminder, with $0 < r < d$.

Substituting $d = ax + by$ into this equation, we get:

$$r = a - qd = a - q(ax+by) = a(1-qx) + b(-qy)$$

This shows that r is also a linear combination of a and b. Since $0 < r < d$; r is a positive integer that is smaller than the smallest positive integer in S, which is d. This is a contradiction. Therefore our initial assumption that d does not divide a must be false. Thus, d divides a.

Similarly, we can show that d divides b. Suppose d doesnot divide b. Then $b = q'd + r'$, where $0 < r' < d$. Substituting $d = ax + by$, we get:

$$r' = b - q'd = b - q'(ax+by) = a(-q'x) + b(1 - q'y)$$

Again; r' is positive linear combination of a and smaller than d, which is a contradiction.

Therefore, d must divide b.

Since d divides both a and b, it is a common divisor of a and b.

2. Any common divisor of a and b also divides d:

Let c be any common divisor of a and b.

This means that there exist integers K and l such that $a = Kc$ and $b = lc$. Substituting these into the equation $d = ax + by$, we get:

$$d = (Kc)x + (lc)y = c(Kx + ly)$$

Since $kx+ly$ is an integer, this equation shows that c divides d.

Since d is a common divisor of a and b, and any other common divisor c also divides d, d must be the greatest common divisor of a and b.

Therefore, $d = \gcd(a, b)$

This completes the proof of Bézout's Identity.

Find the inverse of 101 mod 4620

we want to find x such that:

$$101x \equiv 1 \pmod{4620}$$

This means we need to solve:

$$101x + 4620y = 1$$

Using Bezout Theorem

Step1: Apply the Euclidean Algorithm

we divide until the remainder is 0:

$$4620 = 45 \times 101 + 75 \longrightarrow 1$$

$101 = 1 \times 75 + 26 \longrightarrow (2)$

$75 = 1 \times 26 + 23 \longrightarrow (3)$

$26 = 1 \times 23 + 3 \longrightarrow (4)$

$23 = 7 \times 3 + 2 \longrightarrow (5)$

$3 = 1 \times 2 + 1 \longrightarrow (6)$

$2 = 2 \times 1 + 0 \longrightarrow$ (Done

So, $\gcd(101, 4620) = 1$, so inverse exists

Step 2: Back-substitute to express 1 as a combination of 101 and 4620

From step(6):

$$1 = 3 - 1 \cdot 2$$

From step(5): $2 = 23 - 7 \cdot 3$

$$1 = 3 - 1(23 - 7 \cdot 3) = 8 \cdot 3 - 1 \cdot 23$$

From step (4): $3 = 26 - 1 \cdot 23$

$$1 = 8(26 - 1 \cdot 23) - 1 \cdot 23 = 8 \cdot 26 - 9 \cdot 23$$

From step (3): $23 = 75 - 2 \cdot 26$

$$1 = 8 \cdot 26 - 9(75 - 2 \cdot 26) = 8 \cdot 26 - 9 \cdot 75 + 18 \cdot 26 \cancel{= (8+18) \cdot 26 \cdot 9}$$
$$= (8 + 18) \cdot 26 - 9 \cdot 75$$
$$= 26 \cdot 26 - 9 \cdot 75$$

From step (2):

$$26 = 101 - 1 \cdot 75$$

$$1 = 26(101 - 1 \cdot 75) - 9 \cdot 75 = 26 \cdot 101 - 26 \cdot 75 - 9 \cdot 75$$
$$= 26 \cdot 101 - (26 + 9) \cdot 75$$
$$= 26 \cdot 101 - 35 \cdot 75$$

From step (1): $75 = 4620 - 45 \cdot 101$

$$1 = 26 \cdot 101 - 35(4620 - 45 \cdot 101) = 26 \cdot 101 - 35 \cdot 4620 + 1575 \cdot 1$$
$$= (26 + 1575) \cdot 101 - 35 \cdot 4620$$
$$= 1601 \cdot 101 - 35 \cdot 4620$$

Final result:

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

So the inverse of 101 mod 4620 is:

$$101^{-1} \equiv 1601 \pmod{4620}$$

Answer: 1601

2. Chinese Remainder Theorem (CRT) - Proof

Statement:

Let $n_1, n_2, \ldots n_k$ be pairwise coprime integers and $a_1, a_2, \ldots a_k \in \mathbb{Z}$. Then the system:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x = a_k \pmod{n_k}$$

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

Proof Sketch:

Let $N = n_1 n_2 \cdots n_k$. For each i, define:

$$N_i = \frac{N}{n_i},$$ and find M_i such that

$N_i M_i \equiv 1 \pmod{n_i}$

Then, define the solution:

$$x = \sum_{i=1}^{k} a_i N_i M_i \pmod{N}$$

Each term $a_i N_i M_i \equiv a_i \pmod{n_i}$ and $\equiv 0 \pmod{n_j}$ for $j \neq i$

3. Fermat's Little Theorem - Proof and Example.

Theorem:

If p is a prime number and $a \not\equiv 0 \pmod{p}$ then:

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

Proof:

Let $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{p}$. The set $\{1, 2, \ldots, p-1\}$ forms a multiplicative group modulo p.

Then multiplication by a permutes this set:

$$a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$$

All values are distinct modulo p. So the product of the original and the permuted set are congruent modulo p:

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

(After canceling $(p-1)!$, which is nonzero mod p)

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

use Fermat's little Theorem:

$7^{10} \equiv 1 \bmod 11$ (since 11 is prime)

Now:

$222 = 10 \cdot 22 + 2$

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

$\Rightarrow 7^{222} = 1^{22} \cdot 7^{2} = 49 \bmod 11$

$= 49 - 4 \cdot 11$

$= 49 - 44$

$= 5$

Answer: $7^{222} \equiv 5 \pmod{11}$

CamScanner

* Inverse modulo:

* Fermatts Little theorem:

$$\boxed{a^{m-1} \% m = 1} \; ; \; m \text{ is prime}$$

$$\therefore \frac{1}{a} \% m = a^{m-2} \% m$$

* Euler's theorem:

$$\boxed{a^{\varphi(m)} \% m = 1 \; ;} \; \gcd(a,m) \text{ is } 1.$$

$$\therefore \frac{1}{a} \% m = a^{\varphi(m)-1} \% m \; , \; \boxed{\begin{array}{c} a^{b} \% m = a^{b \% \varphi(m)} \% m \\ \hline \varphi(\varphi(m)) \le \frac{n}{2} \end{array}}$$

* Diofantine equation:

$$\boxed{\begin{array}{l} ax + by = c \; ; \\ \gcd(a,b) \mid c \end{array}}$$

$$\frac{1}{a} \% m = x \quad ; m = b$$

$$\Rightarrow ax \% m = 1 \% m$$

$$\Rightarrow ax \% m + my \% m = 1 \% m$$

$$\Rightarrow ax + by = 1$$

$$\boxed{\therefore \frac{1}{a} \% b = x}$$

$$\boxed{\begin{array}{l} x = y_1 \\ y = x_1 - \lfloor \frac{a}{b} \rfloor y_1 \end{array}}$$

* Divide and conquer:

* Big mod:

$$\rightarrow x^{n} \% m = ?$$

$\checkmark$ $f(n) = f(\frac{n}{2}) * f(\frac{n}{2})$; n is even

$\checkmark$ $f(n) = f(n-1) * x$; n is odd

* Modular multiplication via addition:

→ $(a \times n) \% m = ?$

$$\boxed{\begin{array}{ll} \checkmark\ f(n) = f(\frac{n}{2}) + f(\frac{n}{2}) & ;\ n \text{ is even} \\ \checkmark\ f(n) = f(n-1) \cancel{\times} + a & ;\ n \text{ is odd} \end{array}}$$

* Sum of Geometric series:

→ $(x^1 + x^2 + x^3 + \dots\dots + x^n) \% m = ?$

$$\boxed{\begin{array}{ll} \checkmark\ f(n) = f(\frac{n}{2}) \cancel{\times} + x^{\frac{n}{2}} \times f(\frac{n}{2}) & ;\ n \text{ is even} \\ \checkmark\ f(n) = f(n-1) + x^n & ;\ n \text{ is odd} \end{array}}$$

✓ complexity : $\log^2 n$

→ $(x^0 + x^1 + x^2 + \dots + x^n) \% m = ?$

$$\boxed{\begin{array}{ll} \checkmark\ f(n) = (1+x) \times f(x^2, \frac{n}{2}) & ;\ n \text{ is even} \\ \checkmark\ f(n) = 1 + x \times f(x, n-1) & ;\ n \text{ is odd} \end{array}}$$

✓ complexity : $\log n$

→ $(1x^1 + 2x^2 + 3x^3 + \dots + nx^n) \% m = ?$

$$\boxed{\begin{array}{ll} \checkmark\ f(n) = f(\frac{n}{2}) + x^{\frac{n}{2}} \times f(\frac{n}{2}) + \frac{n}{2} \times x^{\frac{n}{2}} \times g(\frac{n}{2}) & ;\ n \text{ is even} \\ \checkmark\ f(n) = f(n-1) + n \times x^n & ;\ n \text{ is odd} \end{array}}$$

* Chinese Remainder Theorem (CRT):

$x \% m_1 = a_1$

$x \% m_2 = a_2$

$\vdots$

$x \% m_n = a_n$ হলে (যেখানে $\gcd(m_i, m_j) = 1 ; 1 \le i < j < n$)

দুটি equation এর ক্ষেত্রে,

$$\boxed{x = (a_1 m_2 q + a_2 m_1 p) \% m_1 m_2}$$

n টি equation এর ক্ষেত্রে,

$$\boxed{x \mathrel{+}= a_i \frac{prod}{m_i} q \ \% \ prod} \ ; prod = m_1 m_2 m_3 \cdots m_n$$

* ^nC_r calculation: $^nC_r \% m = ?$

1. $O(r)$ approach (without mod → exact value)
2. $O(n)$ approach → Precalculation (prime mod)
3. Lucas theorem (prime mod) → big n, r and small m.
4. $O(n^2)$ approach (non-prime mod)
5. $O(m)$ approach → CRT (non-prime mod)

* Lucas theorem: $\boxed{^nC_r \% m = ?}$

→ n, r বড় হলে এবং m ছোট হলে : $1 \le r \le n \le 10^{18}$, $1 \le m \le 10^6$

m ↓ always prime

→ complexity : $O(m)$

→ m square free হলে CRT use করে $^nC_r \% m$ বের করা যাবে।

→ number of elements are not divisible by p in n_{th} row of pascal triangle $= \boxed{\prod_{i=0}^{k} (n_i + 1)}$

$\therefore$ divisible by p $= \boxed{(n+1) - \prod_{i=0}^{k} (n_i + 1)}$ → proof : combinatorics