CP

Maths

* Big Integers

* GCD, LCM, Euclidean Algorithm,
  Extended Eculidean Algorithm

* Sieve of Eratosthenes and Segmented Sieve.

* Modular Arthmatic

*

Congruence Modulo m

Definition:- two integers a and b are Congruent modulo m if they have Same remainder when divided by m.

Denoted by $a \equiv b \pmod{m}$

reads as a is Congruent to b modulo m.

Note:-

$a \equiv b \pmod{m}$ means $a \bmod m = b \bmod m$. ✓

$a \equiv b \pmod{m}$ if m divides $a-b$.

* Fermat's little Theorem

Definition:- if P is a Prime number and 'a' is Positive integer not divisible by "p" Then

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

Example 1 :- Does format's theorem hold true for

P = 5 and a = 2 ?

Given $p = 5$ $a = 2$

$\uparrow$ prime $\uparrow$ not divisible by

Condition is ok

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

16%5 = 1%5

$$2^{5-1} \equiv 1 \pmod{5}$$

$$2^{4} \equiv 1 \pmod{5}$$

$$16 \equiv 1 \pmod{5} \Rightarrow$$ 16%5 = 1%5 ✓

Example 2 :- $P = 13$ $a = 11$

$\uparrow$ prime $\uparrow$ not Divisible by p

Codition ok

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

$$11^{13-1} \equiv 1 \pmod{13}$$

$$\underline{\underline{11^{12}}} \equiv 1 \pmod{13}$$

* Multiplicative Inverse

Basics of Multiplicative Inverse

$5 \times 5^{-1} = 1$

$5 \times \frac{1}{5} = 1$ ✓

$A \times A^{-1} = 1$

$A \times \frac{1}{A} = 1$

$\frac{1}{A}$ is the multiplicative Inverse of A

* But the Real challenge Comes Under mod n

$A \times A^{-1} \equiv \underline{1 \bmod} \ n$

$A \times A^{-1} = 1$

$\frac{1}{A}$

Example

$A = 2 \qquad n = 5$

$2 \times ? \equiv 1 \pmod{5}$

$2 \times 3 \equiv 1 \pmod{5}$

$6 \equiv 1 \pmod{5}$

$A = 3 \qquad n = 5$

$3 \times ? \equiv 1 \pmod{5}$

$3 \times \underline{2} \equiv 1 \pmod{5}$

$A = 2 \qquad n = 11$

$2 \times ? \equiv 1 \pmod{11}$

$2 \times \underline{6} \equiv 1 \pmod{11}$

$A = 5 \qquad n = 10$

$5 \times ? \equiv 1 \pmod{10}$

Does not have a multiplicative Invers since

They are not relatively primes.

$GCD(A, n) \,!= 1$

$a \quad , \quad p$ $\qquad p = 1e9+7$

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

$m = 1e9+7$ $\qquad \boxed{b^{p-1} = 1 \,\%\, m}$ ✓ $\qquad 1 \pmod{m}$

$(a/b) \,\%\, m$ $\qquad \boxed{b^{-1} \times b^{p-1}} = b^{-1} \,\%\, m$

b^{p-2}

$\boxed{a \,\%\, m * \boxed{b^{-1} \,\%\, m}}$ ✓

$b^{-1} \,\%\, m = b^{m-2}$

$b^{1e9+7-2}$

2^{13}

$$^{n}C_{r} = \left(\frac{n!}{r! * (n-r)!} \right) \% m$$

$$num = \left(n! * r!^{-1} * (n-r)!^{-1} \right) \% mod$$