CLASS- 39

Binary Exponentiation

Mod

pow → O(y) → power x^n

$2^4 = 2*2*2*2 = 16$

Binary Exponentiation → O(log(n)) → x^n

we can do Mod at intermediate steps

last 1 in binary representation is log(n)

7 → 111

2, 0

log(n)

Runtime error

overflow may be Possible

Modular arithmatic on division :

$(a/b) \% m \Rightarrow \left(\frac{a \% m}{b \% m}\right) \% m$ ✗

$\frac{a}{b} \rightarrow b^{-1} * \frac{1}{b}$

$(a * b^{-1}) \% m \Rightarrow (a \% m * (b^{-1}) \% m) \% m$

$\left(\frac{a}{b}\right) \% m \Rightarrow (a * b^{-1}) \% m$

Modular Multiplicative inverse (MMI)

Multiplicative Inverse ?

$A(x) = 1$

Multiplicative Inverse

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

$AX = 1$

— Multiplicative Inverse

MMI

(A * B) % M == 1

B is MMI of A

B value Range?

((A % M) * (B % M)) % M == 1

1 - M-1

M >

(A * B) % M == 1

B is MMI of A

B % M

B > M

((A % M) * (B % M)) % M == 1

1 - M-1

1 - (M-1)

A → 3 M=5

(3 * 4) % 5 == 1

M = 10^9+7

MMI

B > M

long long

Brute force!

3 * (7) % 5

⇒ MMI 1 - M-1

```
for ( i=1; i <= m-1; i++)
    if ( (a*i) % m == 1)
        cout << i is MMI of a
```

T.C = O(m)

MN 10^9+7 TLE

Fermat's little theorm

MMI isn't Possible for every value

MMI isn't possible for every value

a and M are coprime | gcd(a, M) = 1

→ if (M = Prime No) if (M ≠ Prime No)

Mod = Prime | Fermat's

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

a^{-1} * on both side

$[(a^{m-1}) \% m == 1 \% m]$

$(a^{m-1}) * a^{-1} \equiv a^{-1} \bmod m$

$a^{m-2} \equiv a^{-1} \bmod m$

MMI → a → a^{-1} ?

$(a^{-1}) \% m = (a^{m-2}) \% m$

$\left(\frac{a}{b}\right) \% M = (a * b^{-1}) \% M$ ⇒ $(a * (b^{m-2})) \% M$

$(b^{m-2}) \% m$

Binary Exponentiation ⇒ log(m)

$(b, m-2)$

inverse

→ a and M are coprime

→ Fermat's little Theorm
→ M is prime

Extended Euclidian Theorm

$ax + by = gcd(a,b)$ ⇒ $(b\%a, a)$

Hit and Trial — atleast 2 equation?

$gcd(b, a\%b)$

gcd(18, 12)
↓
gcd(12, 6)
↓
gcd(6, 0)

$ax + by = gcd(a,b)$
↓
$b \cdot x' + (a\%b) y' = gcd(b, a\%b)$
↓
$(a\%b) x'' + (b\%(a\%b)) y'' = gcd(a\%b, b\%(a\%b))$

if (b==0) return a

$a x'''' + 0 y'''' = gcd(a,0) = a$ ⇒ $x'''' = 1$, $y'''' = 0$

$ax + by = gcd(a,b)$
↓
→ $b x' + (a\%b) y' = gcd(b, a\%b)$

$a\%b = a - \lfloor \frac{a}{b} \rfloor * b$

$\frac{24}{5}$ ⇒ $24 - [4] * 5$
$= 24 - 20 = 4$

24 % 5 = 4

$24 - 10 \cdot r = 4$

$= 24 - 20 = 4$

$\rightarrow bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor * b\right) y' = g$

$bx' + ay' - \left(\left\lfloor \frac{a}{b} \right\rfloor b\right) y' = g$

$ay' + b\left[x' - \left(\frac{a}{b}\right) y'\right] = g$

$ax + by = g$

$x = y' \qquad y = x' - \left(\frac{a}{b}\right) y'$

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

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

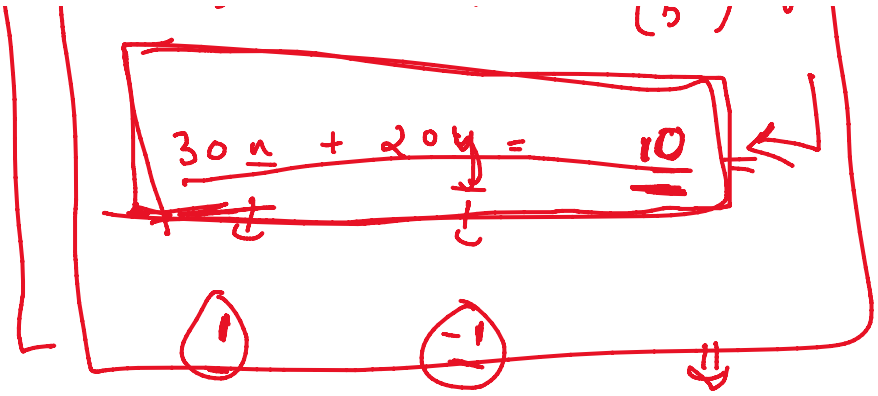
$bx' + (a \% b) y' = gcd(b, a \% b)$

$x = y', \quad y = x' - \left(\frac{a}{b}\right) y'$

Solve

Prime No

Eucledian



Euclidian

--gcd(a,b)

Application of Euclidian Algorithm

Linear Diophantine Equation

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

$a\left(\frac{x}{k}\right) + b\left(\frac{y}{k}\right) = gcd(a,b)$

$ax' + by' = gcd(a,b)$ → Extended Euclidean Algorithm

$\frac{x}{b} = x' * k$, $y = y' * k$

Euler Totient function

$\phi(n)$ = No of integers from 1 to n which are coprime with n

$\phi(5) = 4$ [1, 2, 3, 4]

$\phi(\text{Prime No}) = n - 1$

Ex: 1, Primes

$\phi(7) = 6$

$\phi(11) = 10$

$\phi(13) = 12$

ϕ(Prime NO) = ...

↳ 1, Prime NO

1 - Prime NO - 1

$\phi(p) = p - 1$ — gcd = 1

$\phi(p^k) = p^k - \frac{p^k}{p}$ ⇒ gcd ≠ 1

(3^7)

gcd( ) = 1

(3^7) ⇒ Factors

$1 - (3^7)$

①

gcd(3^7) ≠ 1

3^7

3^3 ⇒ 27

3, 9, 27

27 = 3 * 3 * 3

3, 33, 333

3^4 ⇒ 81

3^3 → 3, 9, 27

3 → multiple ⇒ 3 * n

$\frac{p^k}{p}$

$\frac{20}{2}$ 2

$\frac{27}{3}$

$\frac{27}{3} = 9$ (3 * n, 3 * 3 * 3) = atleast 3

3, 6, 9, 12, 15, 18, 21, 24, 27

$\frac{81}{3}$

$\phi(a * b) = \phi(a) * \phi(b)$

a and b are coprime

$\phi(n) = \phi(p_1^a * p_2^b * p_3^c * \cdots p_k^k)$

$\phi(n) = \psi($ [illegible]

$\Rightarrow \phi(p_1^a) * \phi(p_2^b) * \phi(p_3^c) -- \phi(p_k^k)$

$\Rightarrow \left(p_1^a - \frac{p_1^a}{p}\right) * \left(p_2^b - \frac{p_2^b}{p}\right) * -- - -$

$= p_1^a\left(1 - \frac{1}{p_1}\right) * p_2^b\left(1 - \frac{1}{p_2}\right) * p_3^b\left(1 - \frac{1}{p_3 b}\right) + --$

$\Rightarrow p_1^a * p_2^b * p_3^c --- p_k^k * \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) -- \left(1 - \frac{1}{p_k}\right)$

$\Rightarrow \boxed{n\left[1 - \frac{1}{p_1}\right]\left[1 - \frac{1}{p_2}\right]\left[1 - \frac{1}{p_3}\right] - - \left(1 - \frac{1}{p_k}\right)}$

$\frac{1}{2} = 0$

$\left(n - \frac{n}{p_1}\right) \Rightarrow n'\left[1 - \frac{1}{p_2}\right]\left[1 - \frac{1}{p_3}\right] - - -$

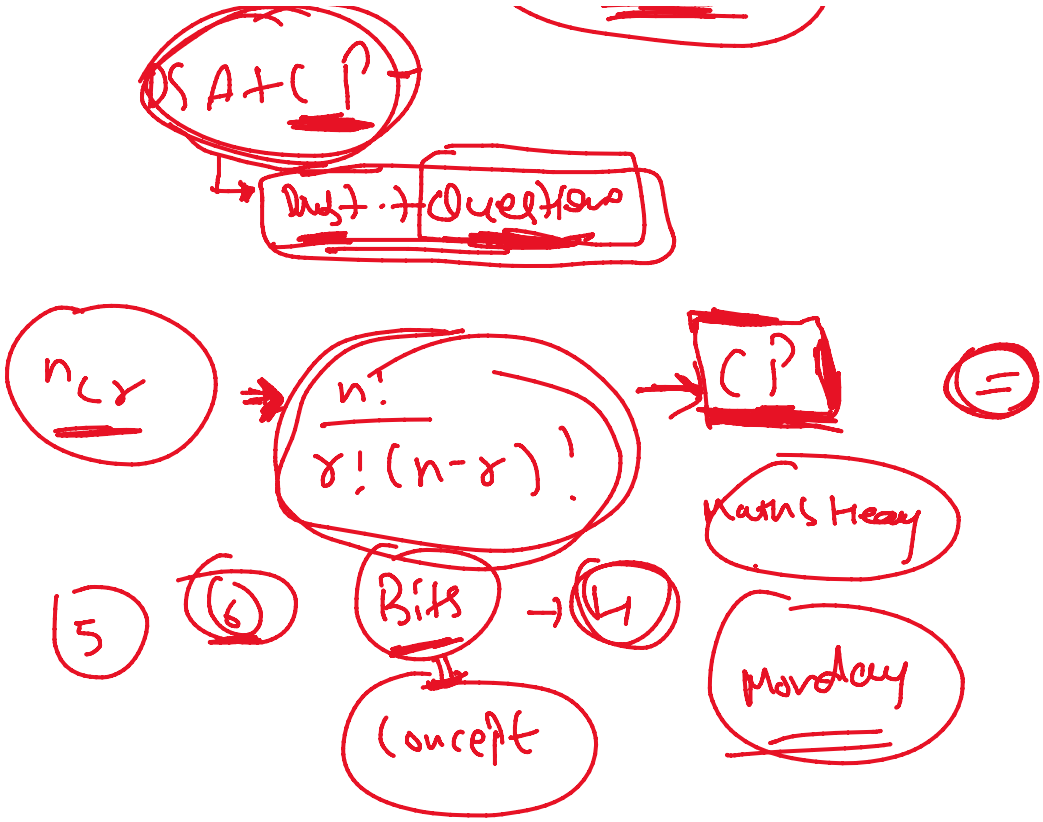
Integer

$\Rightarrow n\phi\left(n' - \frac{n'}{p_2}\right)\left[1 - \frac{1}{p_3}\right] - -$

$= n''\left[1 - \frac{1}{p_3}\right] - - -$

Reiterate

$\Rightarrow A + C$ [illegible]


SAtC P
Must. to Overthink
nCr
n!
r!(n-r)!
CP
=
Maths Heavy
5
6
Bits
4
Monday
Concept