number Theory

branch of mathematics → studied integers.

why it is important ?/
because many questions about integers are very difucult to solve even if seem sample

ex

$$x^3 + y^3 + z^3 = 33$$

let $x = 3$ $y = \sqrt[3]{3}$ $z = \sqrt[3]{3}$

[1] Prime and factors

- factor

a is divisor or factor of b if b divisble by a

if a is factor of b we write $a \mid b$

otherwise $a \nmid b$

- Prime n is prime if
  - $n > 1$
  - n has Two divisors only (1 and n)

assumption

:- for every number more than one can be re write as $n = P_1^{a_1} \cdot P_2^{a_2} \cdot P_3^{a_3} \cdot P_4^{a_4} \cdots P_k^{a_k}$

whe P_i are distinct prime and a_i integer and positive

→ The number of factors

$$\tau(n) = \prod_{i=1}^{k} (a_i+1) = (a_1+1)(a_2+1) \cdots (a_k+1)$$

[1]

(4)

- The Sum of factors of n

$$\sigma(n) = \prod_{i=1}^{k} (1+P_i+\cdots+P_i^{a_i}) = \prod_{i=1}^{k} \frac{P_i^{a_i+1}-1}{P_i-1}$$

$$= \frac{P_1^{a_1+1}-1}{P_1-1} * \frac{P_2^{a_2+1}-1}{P_2-1} * \frac{P_3^{a_3+1}-1}{P_3-1} * \cdots * \frac{P_k^{a_k+1}-1}{P_k-1},$$

- The product of factors

$$\mu(n) = n^{\tau(n)/2}$$

Assumption

n is perfect number if $n = \underbrace{\sigma(n) - n}_{}$ Sum of factors

in othe words $n =$ its factors between 1 and $n-1$.

⇒ number of Primes

The are infinite numbers of primes.

Set → $P = \{P_1, P_2, \cdots, P_n\}$

$P_{new} = P_1 . P_2 \cdots P_n + 1$ ⤸ we Can use it To form new Prime

- density of Primes

let $\pi(n)$ → The number of Prime between 1 and n

$$\pi(n) \approx \frac{n}{\ln n}$$

* Conjectures

There are many conjectures but no one prove it

famous of them for example:-

[1] Goldbach's Conjectures :-

any even integer more than one can divide to two primes number

[2] Twin prime Conjecture:-

The are infinite number of pairs like $\{P, P+2\}$ and both are prime.

[3] Legendre's Conjecture

always there are prime number between n^2 and $(n+1)^2$

Basic Algorithms :-

* if n is not prime it can be represent as a product of a.b where $\min(a,b) \leq \sqrt{n}$. #

So we can do it in Algorithm $O(\sqrt{n})$.

* Sieve of Eratosthenes

build a array where sieve [K] = 0 then K prime

if sieve[K] ≠ 0 so it's not prime and value of sieve[K] is prime factor for it.

big notation of Algorithm :- n/x

$\log n = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots + \frac{1}{n}$

$$\sum_{x=2}^{n} n/x = n/2 + n/3 + n/4 + \dots + n/n = O(n \log n)$$

[3]

Euclid's Algorithms:-

The greatest Common divisor of number a, b = gcd(a, b)
the least Common multiple of number a, b = LCm(a, b)

$$LCm(a, b) = \frac{a*b}{gcd(a,b)} \xrightarrow{or} \frac{a}{gcd(a,b)} * b.$$

Euclid's Algorithm.

formula $gcd(a,b) = \begin{cases} a & b = 0 \\ gcd(b, a \bmod b) & b \neq 0 \end{cases}$

$O(\log(n))$

$n = \min(a, b)$

The worest Case is $gcd(F_{n+1}, F_n)$

F_n is Fibonacci of n

Euler's Totient Function:-

a, b are Coprime if $gcd(a, b) = 1$

Euler's totient Function $\varphi(n)$
give no. of Coprime Functions between 1 and n.

$\varphi(n)$ Can Calulate from prime Factorization of n using formula.

$$\varphi(n) = \prod_{i=1}^{K} P_i^{a_i - 1}(P_i - 1)$$

ex) $\varphi(12) = 2^1(2-1) * 3^0(3-1) = 2 \times 2 = 4$
$\{2, 2, 3\}$

modular Ariethmetic

- if num mod m = ans
ans $\in [0, m-1]$

Some important formulas

- $(x+y) \bmod m = (x \bmod m + y \bmod m) \bmod m$.
- $(x-y) \bmod m = (x \bmod m - y \bmod m) \bmod m$
- $(xy) \bmod m = (x \bmod m \cdot y \bmod m) \bmod m$
- $x^n \bmod m = (x \bmod m)^n \bmod m$

- modular exponentiation :- aim. To claclute $\boxed{x^n \% m}$
in recursion $O(\log(n))$

$$x^n = \begin{cases} 1 & n = 0 \rightarrow \text{base case.} \\ x \cdot x^{n-1} & n \text{ odd} \\ (x^2)^{n/2} & n \text{ even} \end{cases}$$

Fermat's Theorem and Euler's Theorem.

Fermat's Theorem status that

$$x^{m-1} \bmod m = 1$$

when m is prime and m, x coprime.

also

$$x^k \bmod m = x^{k \bmod (m-1)} \bmod m$$

more general Euler's Theorem status that.

$$x^{\varphi(m)} \bmod m = 1$$

note $\varphi(m) = m-1$ (S) if m is prime

So

when m is prime so

$$\boxed{x^{m-1} \bmod m = 1}$$

$x^{\text{number of coprime of number } m} \bmod m = 1$

modular Inverse.

$$\boxed{x x^{-1} \bmod m = 1}$$

how To find inverse modular

$A \% C$

$(A * B) \% C = 1$ search from $0 \rightarrow C-1$

Condition To have inverse That A Coprime To C

or

$x^{-1} = x^{\varphi(m)-1}$ # Proof

if m prime

$x^{-1} = x^{m-2}$

Euler $x^{\varphi(m)} \bmod m = 1$

$x . x^{\varphi(m)-1} \bmod m = 1$

$x . x^{-1} \bmod m = 1$

So $x^{-1} = x^{\varphi(m)-1}$

Computer Arithmetic

hint to — unsigned number in data Type are represent modulo $2^k \rightarrow$ last bit capacity.

Like Integer represent To modulo 2^{32}

$$\boxed{X \bmod 2^{32}}$$

hint

$(1^n + 2^n + 3^n + 4^n) \bmod m$

$= (1^{n \bmod \varphi(m)} + 2^{n \bmod \varphi(m)} + 3^{n \bmod \varphi(m)} + 4^{n \bmod \varphi(m)}) \bmod m$

* note
* To get LCm we Take the Big power

LCm(12, 30)

$12 = 2^2 . 3^1$

$30 = 2^1 . 3^1 . 5^1$

$LCm(12,30) = 2^2 . 3^1 . 5^1 = 60$ #

* To get Gcd do apposite Take the small power

Gcd(12, 30)

$12 = 2^2 . 3^1 . 5^0$

$30 = 2^1 . 3^1 . 5^1$

$gcd(12,30) = 2^1 . 3^1 . 5^0 = 6$ #

Solving Equations

Diophantine equation

form :- $\boxed{ax + by = c}$

x, y unknowns.
a, b and c constants.

Every number in it should by integer.

We can solve it using Euclid's Algorithm

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

Can be solve if c divisible by gcd(a, b)
otherwise can't be solved.

ex: $ax + by = c$
$39x + 15y = 12$
$gcd(39, 15) = 3$ and $c | gcd(a, b)$

So it can be solved.

~~Solution (1, -2), ( ), ( )~~

note → Solution is not unique.

if solution is (x, y) so there are

$$\left(x + \frac{kb}{gcd(a,b)}, y - \frac{ka}{gcd(a,b)}\right)$$

where k is any integer.

Chinese remainder Theorem:-
Solve equations in forms:-

$x = a_1 \bmod m_1$
$x = a_2 \bmod m_2$
$\vdots$
$x = a_n \bmod m_n$

where all pairs of $m_1, m_2, \cdots, m_n$ are coprime.

let X^{-1}_m the inverse of X modulo m, and

$$X_k = \frac{m_1 m_2 \cdots m_n}{m_k} \quad . \#$$

$$X = a_1 X_1 X^{-1}_{1m_1} + a_2 X_2 X_{2m_2} + \cdots + a_n X_n X^{-1}_{nm_n}$$

ex)

$X \equiv 2 \pmod 3$

$X \equiv 2 \pmod 4$

$X \equiv 1 \pmod 5$

find x

Solution

$GCD(3,4) = 1$, $GCD(3,5) = 1$, $GCD(4,5) = 1$

So we can use Chinese remainder theorem.

$$X = \underset{\text{mod } 3}{4.5} + \underset{\text{mod } 4}{3.5.2} + \underset{\text{mod } 5}{3.4.3}$$

$$= 20 + 15 + 12$$

Take mod 3

$X = 20 \pmod 3 \cong 2 \pmod 3$

To res

Take mod 5

$X = 0 + 0 + 12 \pmod 5 = 2 \pmod 5$

note $2.3 = 6 = 1 \pmod 5$

$X = 15 \pmod 4 = 3 \pmod 4 = 2.3 \pmod 4 = 2 \pmod 4$

So final res $\boxed{X = 26 \text{ mod } 60}$

$X = 20 + 30 + 36 = 86$

$=$ ~~[illegible]~~ (6) solutions $= 26, 86, 146, 206, \cdots$

Other Results

[1] Lagrange's Theorem:-

Every positive integar can be represented as a sum of four squares i.e. $a^2+b^2+c^2+d^2$.

ex) $123 = 8^2+5^2+5^2+3^2$

[2] Zeckendorf's Theorem:-

Every positive integar has a unique representation as a sum of fibonacci numbers.

ex) $74 = 55+13+5+1$

[3] Pythagorean Triples

(a,b,c) $a^2+b^2=c^2$

right angle Triangle

ex) $(3,4,5)$ is a Pythagorean Triple

note (ka, kb, kc) also " "

* $k>1$

A Pythagorean triple is primitive if a, b, c are coprime.

use Euclid's formula

$(n^2-m^2, 2nm, n^2+m^2)$ ∀ $0<m<n$

where m, n are coprime

and at least one of them is even.

ex) $n=2$ $m=1$ $\rightarrow (3,4,5)$

Wilson's Theorem

n is prime when

$(n-1)! \bmod n = n-1$

الحمدلله

Testa