- Calculation of greatest common divisor
- Euclids algo
- Proof of time complexity for euclid al
  - Binet's formula
  - Golden ratio
  - PMI
- Modular arithmetic
- Problem solving

GCD → greatest common divisor

HCF

→ we also know the elementary maths way to calc gcd. of two numbers

→ n = {prime factor of n}
m = {prime factor of m}
→ intersection of the prime factors

[Store the prime no. somewhere & the calculate one of on]

Prime Sieve → $O(n \log \log n)$

$a > b$ $\quad$ % $\rightarrow$ remainder

Euclid's algo $\longrightarrow$ $\underbrace{\gcd(a,b) = \gcd(b, a \% b)}$

Let's pick a number $a$ & $b$

$$\boxed{a = bq + r}$$

if a number k divides 'a' & k divides 'b' as well

then it will divide $a-b$ as well.

$a = bq + r$

$\boxed{r == 0}$

$\downarrow$

$\boxed{a = bq}$

$r \neq 0$ $r = a \% b$

gcd (a, b) → this gcd of a, b divide both a & b & a % b also

gcd (a, b) = gcd (b, a - b)

$a = bq + r$

$\underbrace{a - bq}_{LHS} = \boxed{r}$ → divide the RHS

r is also divisible i.e. a % b is also divisible by gcd.

$$gcd(a,b) = g(b, a-b) \;;\; \underline{\underline{gcd(b, a\%b)}}$$

TC

$$gcd(a,b) = gcd(b, a\%b)$$

Base Case $\rightarrow$ $b == 0$ $\longrightarrow$ ret $\underline{\underline{a}}$

$$x^2 - x - 1 = 0$$

roots $\rightarrow \dfrac{1 \pm \sqrt{5}}{2}$ $\qquad \dfrac{-b \pm \sqrt{D}}{2a}$

$$x^2 - x - 1 = 0$$

$$x^2 = x + 1$$

$$x^3 = x \times x^2 = x(x+1) = x^2 + x \rightarrow 2x + 1$$

$$x^4 = x^3 \times x = (2x+1)x = 2x^2 + x$$

$$= 2x + 2 + x$$

$$= 3x + 2$$

$$x^5 = x^4 \times x = (3x+2) \times x = 3x^2 + 2x$$

$$= 3(x+1) + 2x$$

$$\Rightarrow 5x + 3$$

0, 1, 1, 2, 3, 5, 8, 13 . . . .

0th 1st 2nd 3 4 5 6 7 - - - -

$$x = x$$
$$x^2 = x + 1$$
$$x^3 = 2x + 1$$
$$x^4 = 3x + 2$$
$$x^5 = 5x + 3$$
$$x^6 = 8x + 5$$

Coefficients are Fibonacci no.

$$\boxed{x^n = f_n \cdot x + f_{n-1}}$$

$$x^n = f_n x + f_{n-1} \qquad x = \frac{1 \pm \sqrt{5}}{2}$$

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \beta = \frac{1-\sqrt{5}}{2}$$

$$\alpha^n = f_n \alpha + f_{n-1} \quad \text{— } 1 \qquad \beta^n = f_n \beta + f_{n-1} \quad \text{— } 2$$

$$\alpha^n - \beta^n = f_n (\alpha - \beta)$$

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

Binet's formula

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

$$\alpha = \frac{1+\sqrt{5}}{2}$$

$$\beta = \frac{1-\sqrt{5}}{2}$$

$$\boxed{f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}}$$

$$f_n \approx \phi^n$$

$\phi \to$ golden ratio

$\to$ 1.61...

Euclid algo → [M]

TC depends on the no. of steps required to reduce b → 0

$$\underbrace{gcd(a,b)}_{} \longrightarrow n \text{ steps}$$

$a \geq f_{n+2}$ $b \geq f_{n+1}$

Base Case

$gcd(2,1) \longrightarrow 1$ step

$gcd(3,1) \longrightarrow 1$ step

$n=1$

$a = 2$

$2 \geq f_{n+2} \rightarrow f_{1+2} \rightarrow f_3$ True

$3 \geq f_{n+2} \rightarrow f_{1+2} \rightarrow f_3$

Proove

$gcd(a, b) \longrightarrow n$ steps

$a \geq f_{n+2}$

$b \geq f_{n+1}$

$gcd(b, a\%b) \longrightarrow$ n-1 steps

if we prove this.

$b \geq f_{n-1+2}$

$a\%b \geq f_{n-1+1}$

Holds true

$\geq 1$

floor func^n

$a = \left\lfloor \frac{a}{b} \right\rfloor \times b + a\%b$

$\boxed{a \geq a\%b + b}$

$a=7 \quad b=3$

$\left\lfloor \frac{7}{3} \right\rfloor \rightarrow \lfloor 2.... \rfloor = 2$

$2 \times 3 + 1 \rightarrow 7$

$b \geq f_{n-1+2} \longrightarrow \boxed{b \geq f_{n+1}}$

$a\%b \geq f_{n-1+1} \longrightarrow a\%b \geq f_n$

$$\boxed{a \geq a\%b + b}$$

$gcd(a,b) = gcd(b, a\%b)$

$a \geq f_{n+1} + f_n$

$$\boxed{a \geq f_{n+2}}$$

$f_n \approx \phi^n$

$n \approx \log_\phi f_n$

$f_n \approx \min(a, b)$

$n \approx \log_\phi \min(a,b)$

steps

$TC \longrightarrow \boxed{O(\log_\phi \min(a,b))}$

$G \rightarrow$ factors

$[a_1 \quad a_2 \quad a_3 \quad a_4 \quad \ldots\ldots\ldots \quad a_n]$

$d$

$a_j \rightarrow d$

$d \leq k$

$\leq k$

$> k$

whole array becomes co-prime

12

$2 \times 2 \times 3$

max element

$\gcd(a_1\, a_2\, a_3 \ldots\ldots\, a_n) \rightarrow G$

$[a_1\ a_2\ a_3\ \ldots\ldots\ a_n] / G$

$\Downarrow$

co-prime $\leftarrow [ag_1, ag_2, ag_3 \ldots\ldots\ ag_n, ]$

$1^{st}$ xx $L^{r}$

$[a_1\ a_2\ a_3\ a_4 \ldots\ldots a_n]$

$N \le 10^5$

$l, r \le N$

$\gcd(\gcd(a_1, a_2, a_3 \ldots a_{l-1}), \gcd(a_{r+1}, a_j, a_{j+1} \ldots a_n))$

$q \le 10^5$

$q$

$\boxed{O(n \log \min)}$

TLE

prefix

$a_1,\ \gcd(a_1, a_2),\ \gcd(a_1, a_2, a_3) \ldots$

$\ldots \gcd(a_{n-1}, a_n),\ \gcd(a_n)$

suffix