Introduction To Number Theory

Agenda →

→ GCD
→ Euclidean formula ← proof

TC ← proof &

→ applications
→ Binet's formula
→ Problem solving

Prerequisite

→ Basic loops
→ Elementary Maths
→ Basic Recursion

GCD → greatest common divisor / HCF

VVI

we all know in elementary maths how we calc gcd

$n = \{\text{powers of prime}\}$

$m = \{\ \}$ → common

gcd → Time Complexity

$\sqrt{n} + \sqrt{m} + \longleftrightarrow$

for(i=2; i*i <= n ; i++)

gcd → lcm

$$lcm = \left(\frac{ab}{gcd}\right)$$

$A_1 \quad A_2 \quad A_3 \; - - - - - - - \; A_n$

→ the whole array been

→ co-prime

j → factors $\le K$

$a[j]$ / factors

factors ??

operation → we don't

perform

$T \le 10^5$

$N \le 10^5$

$A_i \le 10^9$

$K \le 10^9$

cc-point

$gcd(a, b, c) = gcd(a, gcd(b, c))$

$gcd(a[1], a[2], a[3] \ldots a[n-1]) = T$

T → this is the largest number that divides all elements

factor of T → $c_1 \; c_2 \; c_3 \ldots c_x$

$max(c_1, c_2, c_3 \ldots c_x) \leq K$ Yes

else NO

gcd(2, 3, 6) = 1

co-prime

$\sqrt{n}$

2 2 2

10, 15, 30 → 2, 3, 6 → 1

k = 6

gcd(10, 15, 30) ← 5 →

5 → 5, 4c

c_1 c_2 c_3 →

5, 10, 20

k = 4

gcd → 5 → 5

False

10^{6} 10^{7} 10^{9}

$\sum M_i \le 10^{6}$

10^{9}

This Solution optimal

1, 2, 3, 4 → 24

36 → 36

6, 5 → 30

gcd → 6

all fact. of 24 → $1 \times 2 \times 3 \times 2 \times 2$

all fact. of 36 → $1 \times 2 \times 2 \times 3 \times 3$

all fact. of 30 → $3 \times 2 \times 5$

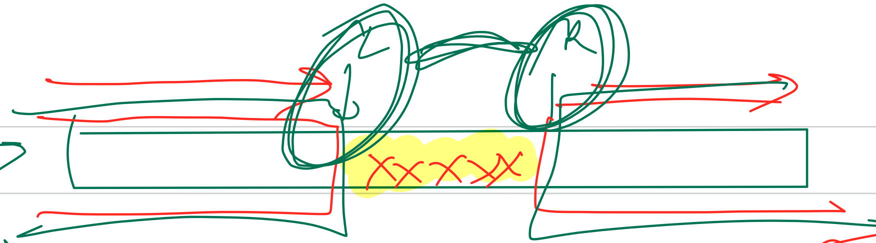
common factor → gcd

1 . . . .

$2 \times 2 \times 3$

gcd ← 3×2 → prime

gcd queries



$T \le 10^5$

$N \le 10^5$

$Q \le 10^5$

$A_i \le 10^5$

$O(\log(\min()))$

$a_1 \quad a_2 \quad a_3 \quad a_4$

$P \to a_1 \quad a_2, a_1 \quad a_3, a_2, a_1 \quad a_4, a_3, a_2$

$S \quad a_1, a_2 \quad a_2, a_3, a_4 \quad a_3, a_4 \quad a_4$

$N \log \min()$

prefix gcd array $p(i)$

suffix gcd array $s(i)$

Thm

Extended → modular inverse

Modular arithmetic

Linear diophantine

prime factorsin $\rightarrow$ sieve $\rightarrow$ $O(n \log \log n)$

$\sqrt{n}$

prim factr

any suggestions $gcd(a, b)$

Can we write any relation between a & b

$a > b$

if we divide them

$$\boxed{a = \underbrace{b \times q} + r}$$

$r = 0$

$(a) = (bq)$

$a \% b = 0$

$$\boxed{(6) = (3 \times 2)}$$

$6 \% 3 = 0$

$(7 = 3 \times 2 + 1)$

$r \neq 0$

gcd

any no. K divides

a and b

a − b

a > b

remainder

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

recursive relation

what does a % b represents ?? → remainder ??

$a = b \times q + r$

$a - bq = r$

remainder

for any K

a/b

$a = bq + a\%b$ r

$a\%b$ → remainder

if a & b has a gcd k

$\gcd(a,b) = \gcd(b, a\%b)$ ← Euclid algo

recursive relation

→ modular inverse

→ Extended euclid

& linear diophantine eqn

⋮

$gcd(a, b)$ $\xrightarrow{h}$ recursion

$gcd(b, a \% b)$

$a = \underline{36}$ $b = \underline{16}$ $\rightarrow gcd \rightarrow \underline{4}$

$gcd(36, 16) = gcd(16, 4) = gcd(4, 0)$

Base case

if $b == 0$ return $\underline{a}$

2 euclid algo

TC $\rightarrow \log_{\phi}(\min(a, b))$

golden ratio

$\phi \rightarrow$? ?

$\phi \rightarrow$ golden ratio

$\rightarrow f_n \approx \phi^n$

n^{th} fibonacci

$\phi = 1.6 \ldots$

$f_0 = 0$ $f_1 = 1$ $f_2 = 1$ $f_3 = 2$

$f_n \to$ fibonacci

Derive any relation btw a, b & fibonacci

TC gcd(a, b) $\to$ n steps

a > b

↳ statement

$a \geq f_{n+2}$

$b \geq f_{n+1}$

$\to$ Induction

↳ Base Case

gcd(3, 1)

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

gcd(4, 1)

b = 1

n = 1

$a \geq f_{n+2}$

$a \geq f_{1+2}$

$a \geq f_3$

$b \geq f_{n+1}$

$b \geq f_2$

$1 \geq 1$

$a > b$

Induction assume

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

2 ≥ 1

$\left\lfloor \frac{a}{b} \right\rfloor \geq 1$ $a \geq b + a \% b$

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

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

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

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

$\hookrightarrow a \geq a \% b + b$

Clear?.?

$a \geq a \% b + b$ $\quad (\sim) O(\log_{\phi} \min(a, b))$

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

$a \geq f_{n+2}$

$\gcd(a, b) =$

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

$a \geq f_{n+2}$

$b \geq f_{n+1}$

$f_n \approx \phi^n$

$n \approx \log_{\phi} f_n$

steps

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

quadratic

$x^2 - x - 1 = 0$

roots $\Rightarrow \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$

$=$

roots $= \dfrac{1 \pm \sqrt{5}}{2}$

$x^2 - x - 1 = 0$

$x^2 = x + 1$

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

$x^3 = x^2 + x$

$x^3 = 2x + 1$

$$x^3 = 2x + 1$$

$$x^4 = x \times x^3$$

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

$$= 2x^2 + x$$

$$= 3x + 2$$

$\vdots$

$$x^5 = 5x + 3$$

$$x^6 = 8x + 5$$

$\vdots$

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

$$\rightarrow \quad x^n = f_n x + f_{n-1} \quad \text{--- } (1)$$

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

$$\alpha^n = f_n \alpha + f_{n-1}$$

$$\beta^n = f_n \beta + f_{n-1}$$

$$\frac{\cancel{1} + \sqrt{5} - \cancel{1} + \sqrt{5}}{2} = \sqrt{5}$$

$$\alpha^n - \beta^n = f_n(\alpha - \beta) + \cancel{f_{n-1}} - \cancel{f_{n-1}}$$

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

$$= \sqrt{5}$$

$$f_n = \frac{\overset{1}{\alpha^n} - \beta^n}{\sqrt{5}}$$

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

$$\rightarrow \underline{f_n \approx \phi^n} \leftarrow$$

Binets formula