Mathematics 3.0

(Number Theory)

1) GCD (Greatest Common Divisor)

a, b

$$GCD(a,b) = GCD(b, a\%.b) \quad \text{— (1)}$$

Recursive definition of GCD

↳ Euclid's method

$$LCM(a,b) = \frac{a * b}{GCD(a,b)} \quad \text{— (2)}$$

↳ complexity $O(Log(max(a,b)))$

2 numbers

if $a > b$

$O(\log(A))$ ✓

$n_1, n_2 \ldots\ldots n_k$

⇓

Prime factorisation of each number.

(3) Computing Prime Numbers

Check if a no is Prime.

$i =$

$2 \ldots N-1$

N

$N \% i == 0$

↓

Not Prime

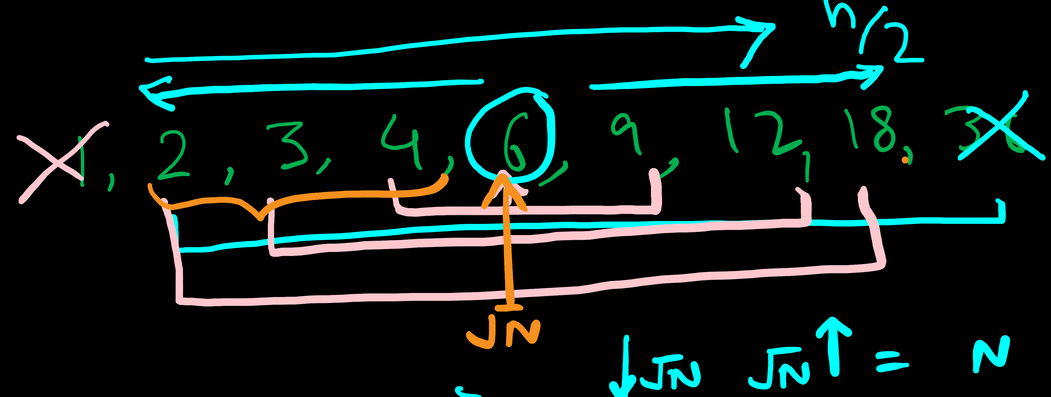
O(N) time to

Optimize

2 . . . . . $\sqrt{N}$

$i = \uparrow$

N



$\downarrow\sqrt{N}$ $\sqrt{N}\uparrow = N$

$O(n/2)$

2, 3, 4, 6

```
for(i=2 ; i*i <=N ; i++)
    if(N%i==0)
        {
        NOT PRIME
        }
```

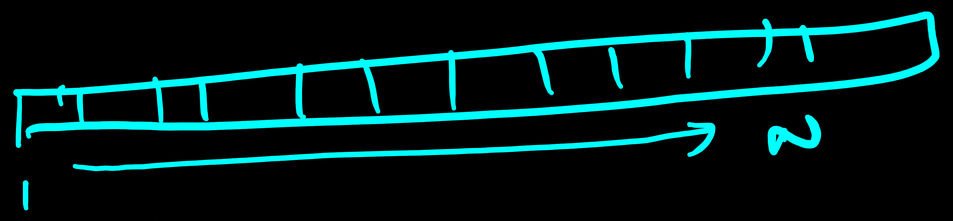
3

$\uparrow a \times b\downarrow = 36$

$\downarrow a \times b\uparrow = 36$

$O(\sqrt{N})$ for a single number

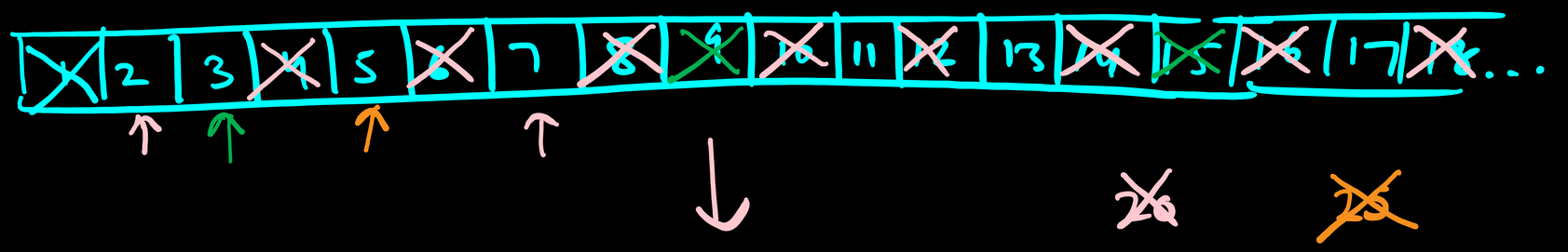
N - Prime Numbers



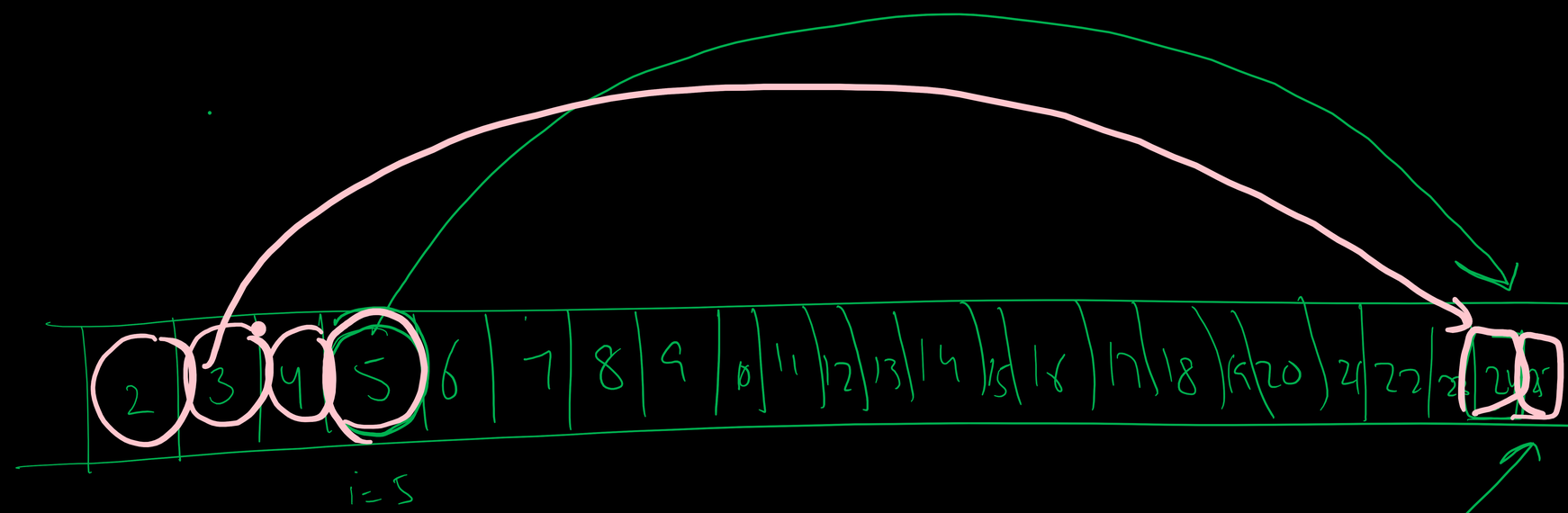
$O(N\sqrt{N})$ time.

$1s = 10^8$ computations ✓

Prime Sieve
(sieve of Eratosthenes)



We are left with only Prime numbers.



$// \; 3 \; // \leq \sqrt{24} > 8$

24

$j = i \times i$

2,3,5 $\sqrt{N}$ ← X ← 36

b

$\sqrt{b}$

2 | 3 | 5

$\sqrt{b}$

$O(\frac{N}{\sim}$

sieve $O(\sqrt{b}\ \log\log b)$

a = 25

b = 36

Visualise 25 26 27 28 29 30 31 32 33 34 35 36

X X X X 1 X 1 X X X X X

0 1 2 3 4 5 6 7 8 9 10

a

j-a

a = 25

28 - 25 ⇒ (3)

b

Shifting

for (i=a .... b)

count += 1

(2) Primes b/w a & b.

Linear Diophantine Equation

$ax + by = c$

- 2 variables
- a, b, c are constants

c is a multiple of $\gcd(a,b)$.

→ No of integral ?

Integral solution?

- Yes
- No

let $\gcd(a,b) = g$.

$a = K_1 g$

$b = K_2 g$

$+ K_2 g\, y = c$

$(K_1 x + K_2 x) = \frac{c}{g} \Rightarrow$ must be an integer.

($K_1 x + K_2 x$: integers)

$c \% g == 0$

$c \mid g$ ✓

x_0, y_0

$ax_0 + by_0 = c$

Generalised soln → family of solutions

$$\{x, y\} = \left\{ x_0 + \frac{b}{g} * t \;,\; y_0 - \frac{a}{g} * t \right\}$$

g = GCD

t = Parameter .....

$a\left(x_0 + \frac{b}{g}t\right) + b\left(y_0 - \frac{a}{g}t\right)$

$= ax_0 + \frac{ab}{g}t + by_0 - \frac{ab}{g}t$

$= ax_0 + by_0$

$= c$

$a = s \cdot K_1$

$b = s \cdot K_2$

→ Extended Euclidean Algorithm.
(later)

Properties of Modulo

① $(a+b) \% m = (a \% m + b \% m) \% m$

② $(a-b) \% m = (a \% m - b \% m + m) \% m$

eg $a = 8$, $b = 3$, $m = 7$

$(a \% m - b \% m + m) \% m$

$= 1 - 3 = (-2 + 7) \% 7$

$= 5$ ✓ (+ve)

③ $(a * b) \,\%\, m = ((a \,\%\, m) * (b \,\%\, m)) \,\%\, m.$

④ $\left(\frac{a}{b}\right) \,\%\, m = ((a \,\%\, m) * (b^{-1} \,\%\, m)) \,\%\, m$

$\left[\frac{1}{b} = b^{-1}\right] \Rightarrow$ Inverse of denominator

Linear Congruence

$x \,\%\, 2 = 1$ . .

$\hookrightarrow x \equiv 1 \pmod 2$

Chinese Remainder Thm

(CRT)

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 5 \pmod 7$$

Possible value(s) of x.

Brute Force ⇒

↓ inefficient

$i = 1 \ldots\ldots\ldots$ first Possible soln.

CRT

num[ ] = { 2, 3, 7, }

rem [ ] = { 1, 2, 5, }

↓

values of x.

$x \% num[0] = rem[0]$

$x \% num[1] = rem[1]$

$x \% num[2] = rem[2]$

⋮ ⋮

$x \% num[k] = rem[k]$

} value of x ?

Solution :

Formula

$$x = \sum_{0 \le i < k} (rem[i] * pp[i] * inv[i]) \% prod$$

rem[i] = Given ✓

prod = is product of num[i]

pp[i] = $\frac{\text{prod}}{\text{num[i]}}$ ✓

inv = $\frac{\text{Modular Multiplicative}}{\text{Inverse of pp[i] wrt num[i]}}$

$$(a * y) \;\%\; K = 1$$

$$(6 * y) \;\%\; 7 = 1$$

eg $y = 6$ is the modular multiplicative inv of 6 wrt. 7.

$$\boxed{y = 6}$$

Intution Behind CRT

$X \% 2 = 1$

$X \% 3 = 2$

$X \% 7 = 5$

] value of x ?

prod / num[i]

X = 7.3. + 7.2. + 2.3

7.3. → %.2 → Remainder

7.2. → %.3 → Remainder

2.3 → %.7 → Remainder

Rem = 5

$(6 * y) \% 7 = 5$

$$\sum PP[i] * inV[i] * rem[i]$$

Getting now :)

↓ Algorithm.

first make remainder 1,
then multiply it by 5.

$(6 * y) \% 7 = 1$

↓

modular multiplicative inverse of 6 wrt 7.

$((6 \cdot 6) \% 7 = 1) * 5$

↓

$((6 \cdot (6)) \% 7) * 5$

$= 5$

Euler Phi Fn (ϕ)

Number of given numbers $\leq N$ and coprime with N.

$$n = 25 = 5^2$$

$$\Rightarrow \quad \phi(25) = 25\left(1 - \frac{1}{5}\right)$$

$= 25 - \frac{25}{5}$

$= 20$

$25 - \frac{25}{5}$

$= 20$

e.g. $N = 50 = 5^2 \cdot 2$

$\phi(n) = 50\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{2}\right)$

$= \left(50 - \frac{50}{5}\right)$

$\phi(50) = 20$

$= 40\left(1 - \frac{1}{2}\right) = \frac{40}{2} = 20$

Euler Totient Fn

Property

$$\therefore a^{\phi(m)} \equiv 1 \pmod{m}$$

if m is prime

$$\phi(m) = m-1$$

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

Fermat's Lil Thm

$$\Rightarrow a \cdot a^{p-2} \equiv 1 \pmod{p}$$

↓

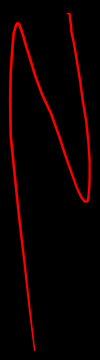
Multiplicate Modulo Inverse of a wrt p.

(Inverse Modulo)

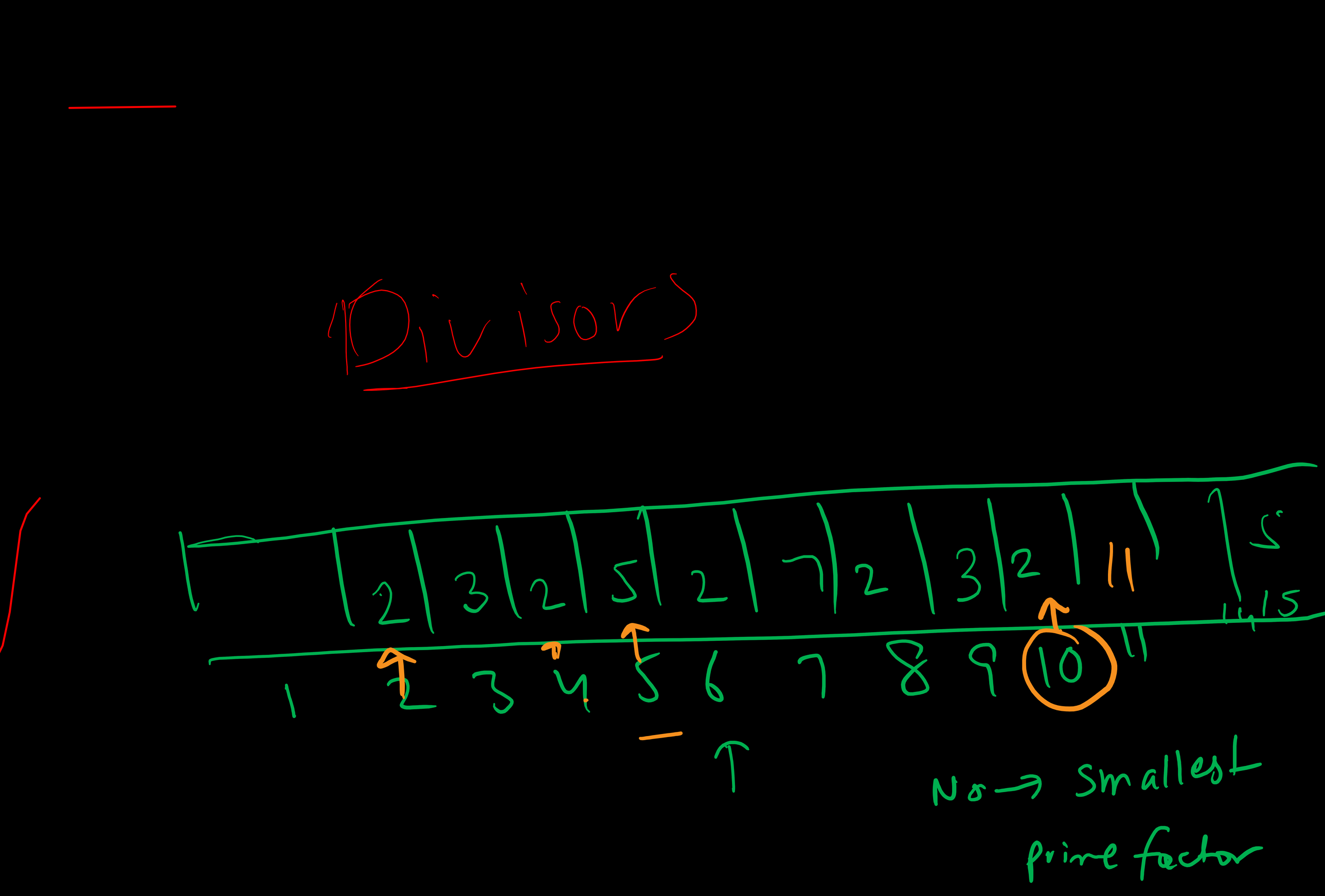
$$(a \cdot y) \,\%\, p \equiv 1$$

↓

a^{p-2} if p is prime



Divisors


1 2 3 4 5 6 7 8 9 10 11
1 2 3 2 5 2 7 2 3 2 11 5
14 15
No → Smallest
prime factor

8/2 → 10 → 2

a[i] ↑

=4/2 → 10/2 = 5. ∴ 10 = 2 × 5

=2/2

=1

14 = 2 × 7

14/2 = 7 ⇒ 7/7 ⇒ 1

8 = 2.2.2 = 2^3

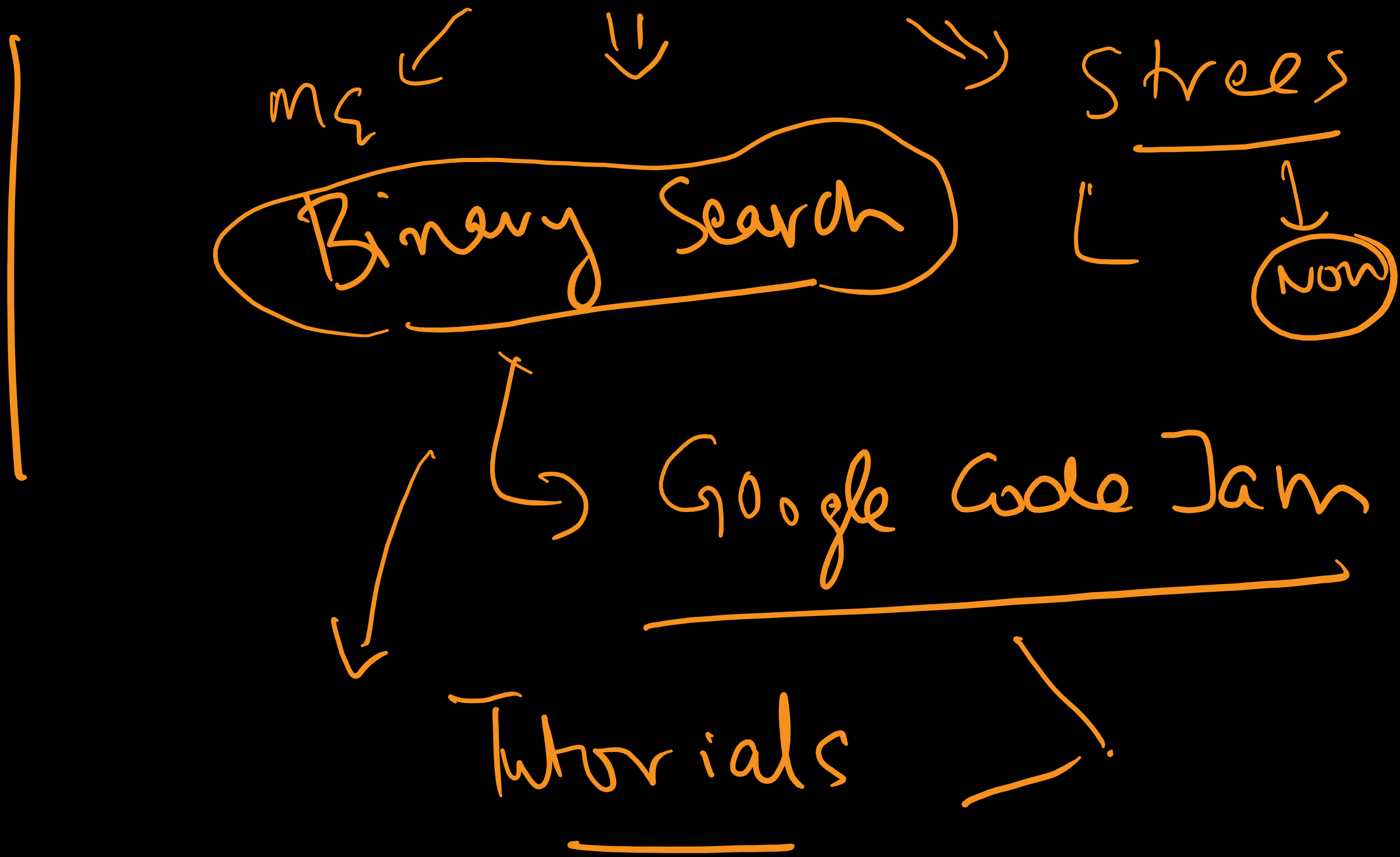
O(N log log N)

= O(N) ✓

Query $O(\log N)$

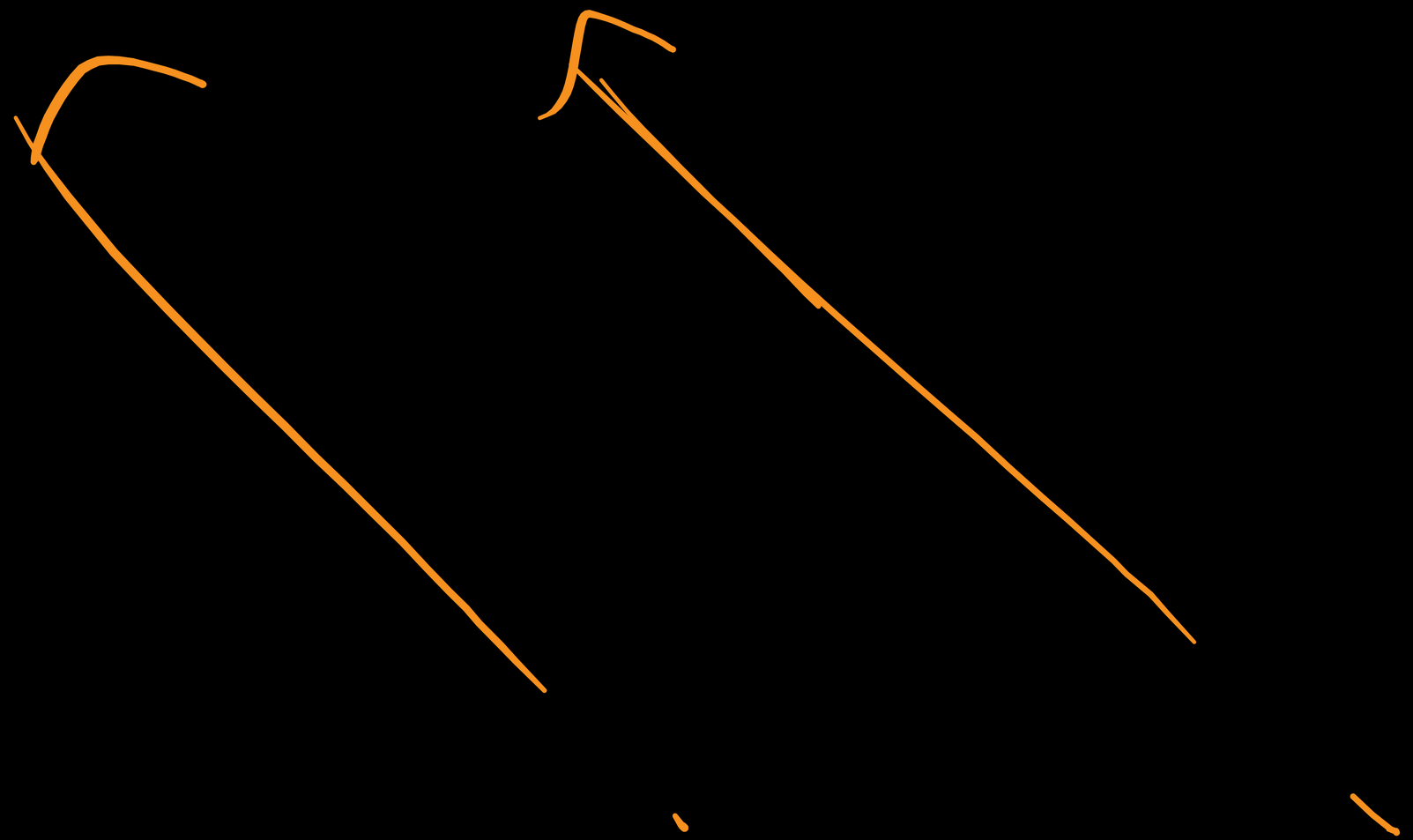
SUNDAY

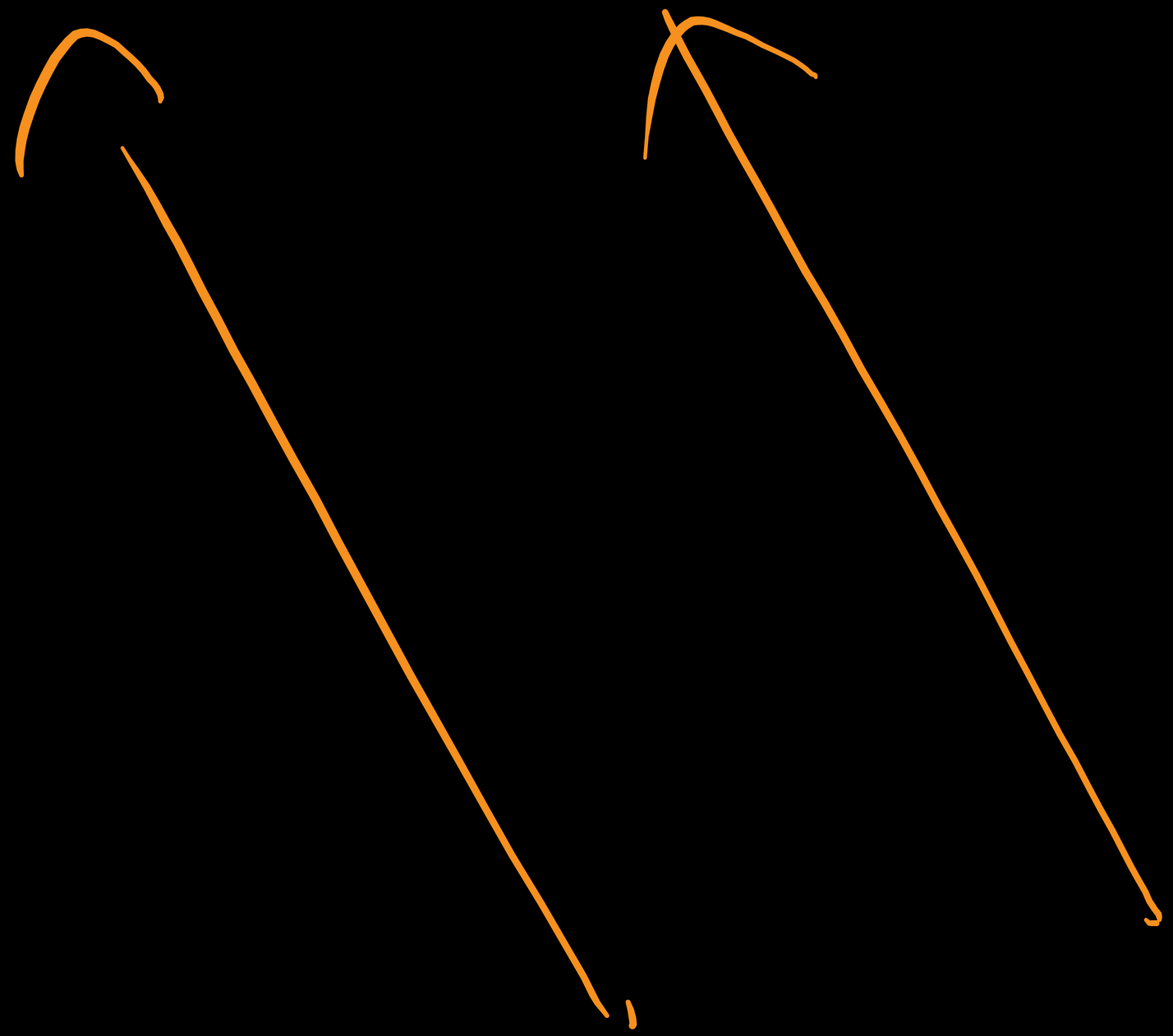
Divide & Conquer

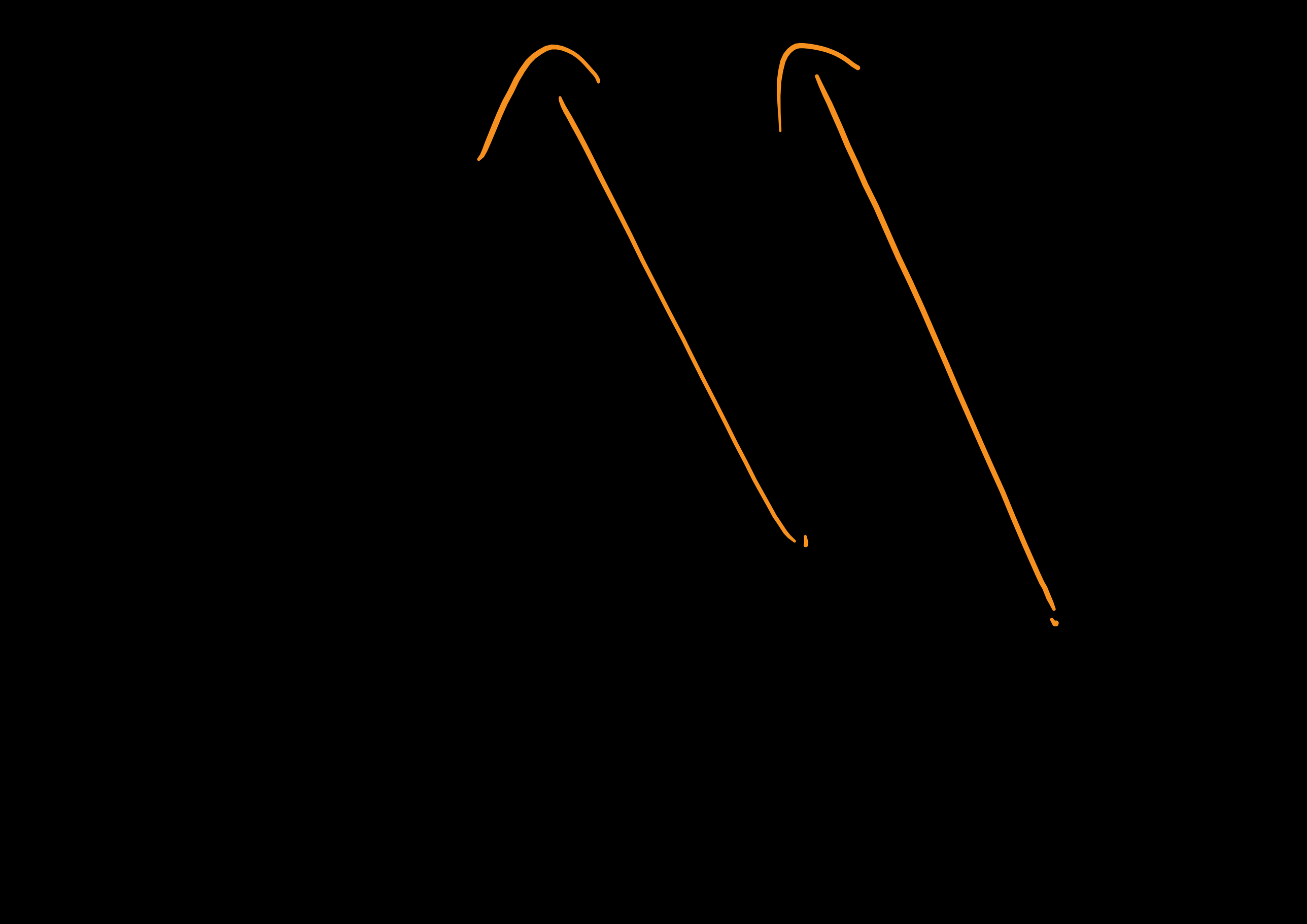

Binary Search
Google Code Jam
Tutorials
Now

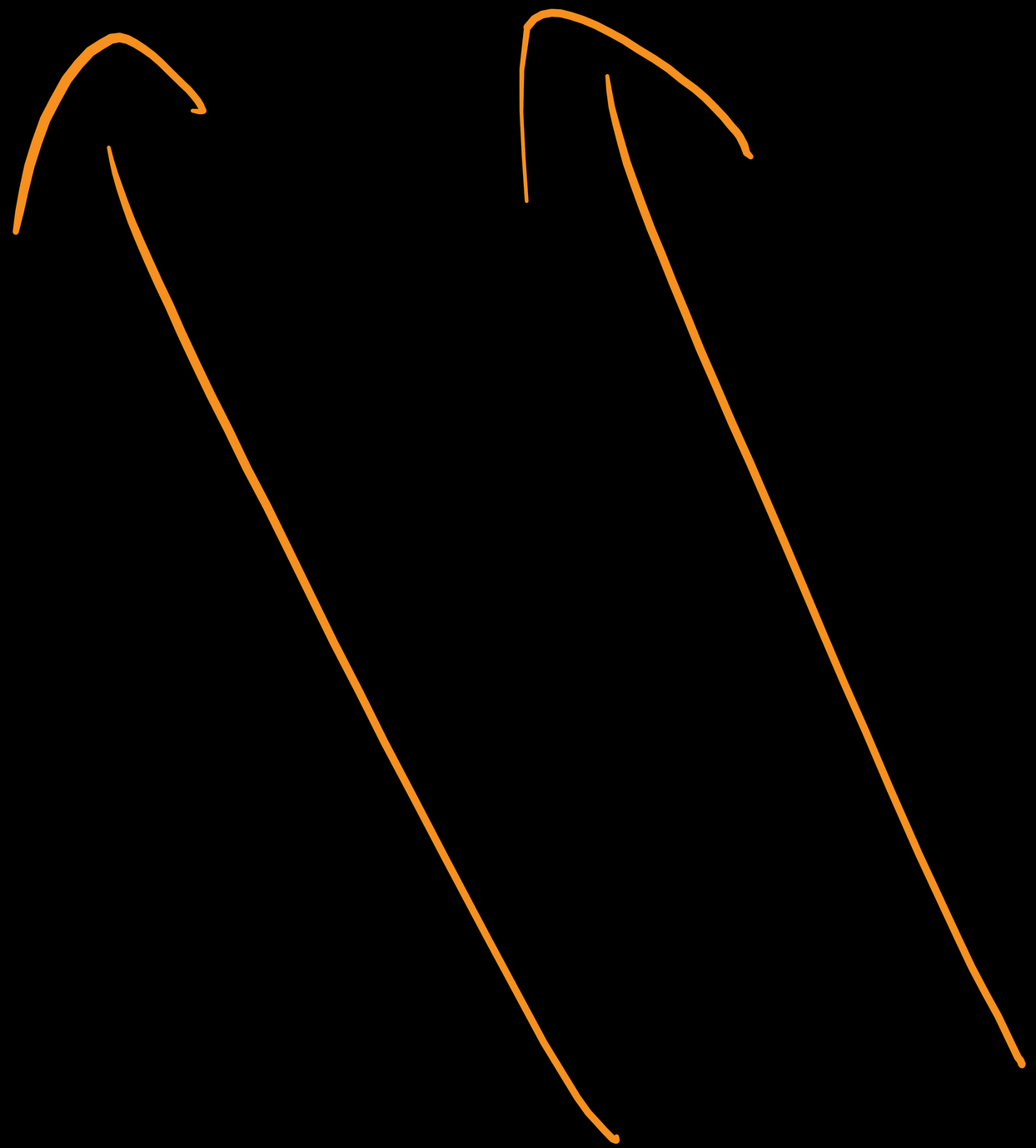
Graphs after Dinal:

Thank You!









$(a * y) \% p = 1$ ← Fermat's Li'l Thm.

$\hookrightarrow y = a^{p-2}$

fast exponentiation ✓

$inv(a) = a^{\phi(m)-1}$

$= a^{m-2}$ if m is prime.

Most challenging
hardest Problem
on Number Theory -

⇒ POWPOW2

↳ Read 2 mins

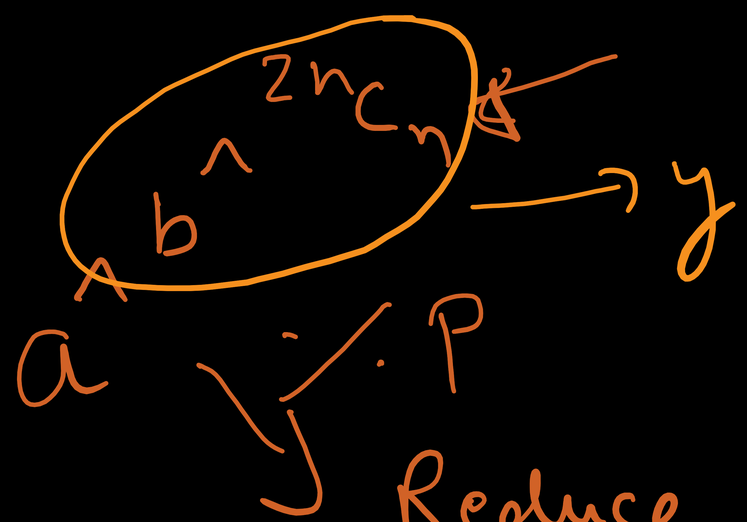
$a^{b^{exp}} \% P$

$P = 10^9 + 7$

$exp = {}^{n}C_0 + ({}^{n}C_1)^2 + ({}^{n}C_2)^2 + \cdots ({}^{n}C_n)^2$

$= {}^{2n}C_n$

$a, b, n \leq 10^5$



$n = 10^5$

Reduce to Smaller Problem.

$a^y \;\%\; P$

$P = 10^9 + 7$

↳ Prime No

$a^{\phi(m)+\phi(m)+\ldots\phi(m)+rem} \;\%\; m$

$\left(a^{P-1} \;\%\; P = 1\right) \rightarrow$ Fermats Thm.

$y = k\phi(m) + y \,\%\, \phi(m)$

$$\because \; a \equiv a^{k\cdot\phi(m)+1} \pmod{p}$$

$$\Rightarrow a^{y\cdot\phi(m)+1} \equiv a \pmod{p}$$

$$\Rightarrow a^{y(p-1)+1} \equiv a \pmod{p} \qquad p = 10^9+7$$

$$\Rightarrow a^{y(10^9+6)} \equiv a \pmod{(10^9+7)}$$

$$b = {}^{2n}C_n$$

Not coprime

$$\because b \equiv 0 \pmod{(10^9+6)}$$

Not Prime

(Composite No)

b is odd

b is even

Break down into Coprimes

$$b^{2nC_n} \mod 2 \times (5 \times 10^8 \div 3)$$

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

↳ a, b coprime

$$b^{2nC_n} \mod 2$$

↳ 0

$$b^{{}^{2n}C_n} \bmod (5\times10^8+3)$$

$b \le 10^5$

$(5\times10^8+3)$

$\phi(2\cdot(5\times10^8+3))$

$\phi = \phi(2)(5000003)$ — Prime.

$= 1(5000002)$

$= 5000002$

$= 5\times10^8+2$

$b^{{}^{2n}C_n} \,\%\, (5\times10^8+3)$

$(5\times10^8+3)$ → Prime NO

$b^{2n}C_n \;\%\; \phi(p')$

$\%\;(5\times10^8+3)$

$p' = (5\times10^8+2)$

$\Rightarrow b^{2n}C_n \;\%\; (5\times10^8+2)$

Not Prime

$^{2n}C_n$ = Big NO

Big NO %o Composite NO

$^{2n}C_n$ %. $(5\times10^8+2)$

X

$^{2n}C_n$ → $^{2n}C_n$ mod 2 = R1

$^{2n}C_n$ mod 1681 = R2

$^{2n}C_n$ mod 148721 = R3

Prime → Fermat $(n-1)^{p-2} = 1$

⇒ Remainder

⇒ BRUTE force

⇒ Prime $n!^{p-2}$

p = 148721

R1, R2, R3 unif incr. (BF similar modulo)

$$nC_r = \frac{(n-r+1)(n-r+2)\cdots n}{1\,2\,\cdots\,r}$$

$$= \frac{(n-r+1)(n-r+2)(n-r+3)\cdots(n)}{r!}$$

$r!$ ↓

${}^{n}C_r \;\%\; m$

$m = 2,$ ⇐ ✓

1681.

148721 ⇐ ✓

$\Rightarrow$

$\left((n-r+1) \;\%\; m \times (n-r+2) \;\%\; m \cdots \right) \%\, m$

$$\left(\frac{1}{n!}\right) \% m$$

$m = 2$ prime

using

$$\underbrace{a \cdot a^{p-2}}_{\uparrow \quad \uparrow} \% \underline{p} = 1$$

$$(n!)^{p-2}$$

$p = 2$

$$(n!)^{2-2} = 1$$

$^{n}C_{r} \;\%\; P$

↳ Lucas Thm

$$x = \binom{2n}{n} \% (500000002)$$

$$= \sum pp(i) * rem(i) * inv(i)$$

$n = 10^5$

$^{2n}C_n$ ⇓ very big

$(10, 17,) \% 7$

$= (3)$ ⇓ (3)

$(100.000000-0-0000)\ \%.\ 5\times10^{8}$

$\ldots)$

$+2$

Smaller No

b

Even

$b^{2n}C_n \ \%.\ (10^9+6)$

$b^{2n}C_n$

$$D \mod (2)(5.10^8 + 3)$$

coprimes

$$\text{even} \leftarrow \underline{b}^{2n C_n} \mod 2 = 0$$

$$b^{2n C_n \cdot P - 1} \mod (5.10^8 + 3) \rightarrow \text{add}$$

Prim. Case

$$2n C_n \mod (5.10^8 + 2)$$

$$2 \cdot 41^2 \cdot 148$$

$^{2n}C_n \;\%\; 2 = R1$

$^{2n}C_n \;\%\; 1681 = R2$

$^{2n}C_n \;\%\; 148721 = R3$

num

rem.

$^{2r}C_K \rightarrow X$

CRT

Let $X = {}^{2r}C_n$

$$X = \sum rem(i) * pp(i) * inv(i)$$

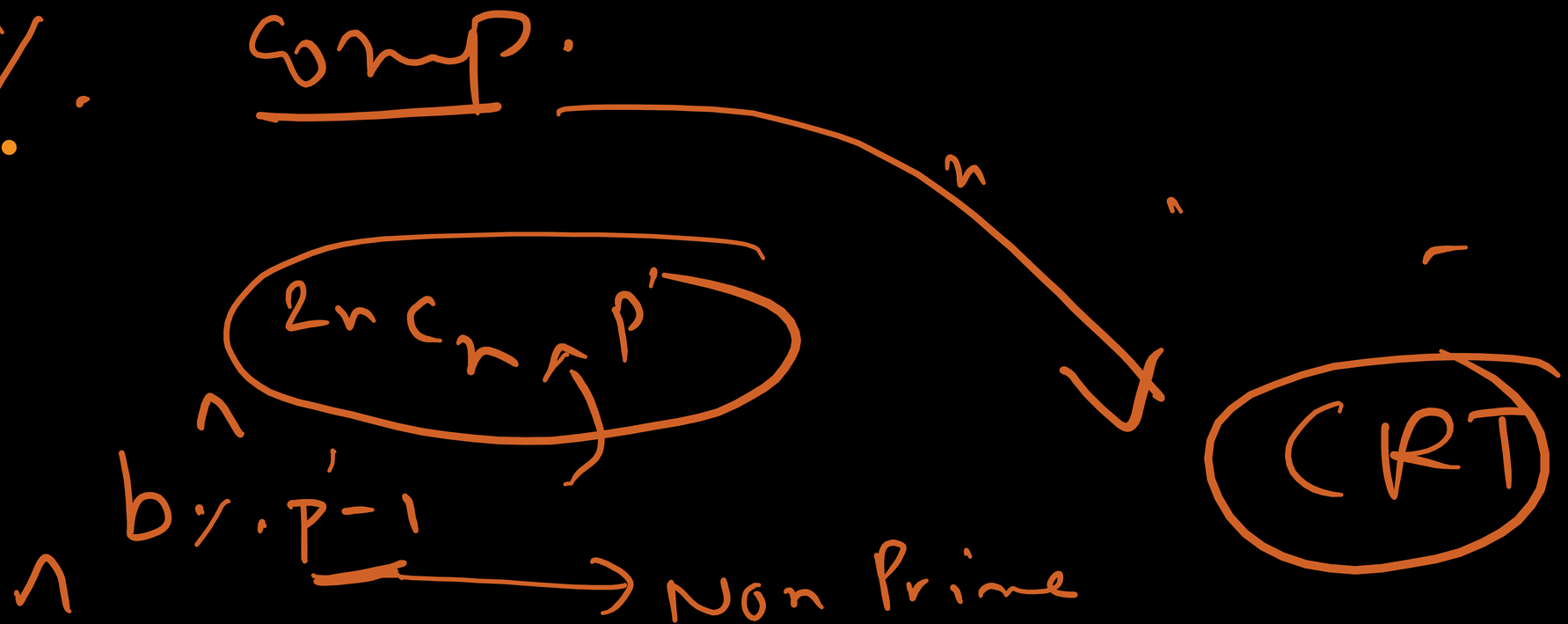
$inv(n!)$ wrt Σ $\rightsquigarrow$ -

$inv(n!)$ wrt 1681 $\times$ Bruteforce

$in(4!)$ wrt 148721 $\Rightarrow$ formula

Lucas. ${}^{n}C_{r} \% p$ $\downarrow$ inv

Big NO :/. comp.



a :/. p

ϕ(2 ≠ Prime.)

= ϕ(2) ϕ (Prime

= 1 . ϕ(1-