- Sieve
  - prime no.
  - gcd
    - extended
    - linear diop.
    - modulo arithmetic
    - inverse modulo
      - fermat theorem
        - wilson theorem
        - CRT
        - mob. inv.
      - primality test
      - ⋮

↳ Prime no. → Numbers divisibly by 1 & itself

Given a number N, print all primes less than N.

Ex → N=10 → 2, 3, 5, 7

Brute force

$O(n^2)$

(2 → N) → ∀i if i is prime or not

(i → (2 → i-1)) → ∀j

Optimization → (2 — N) → ∀ i

i → is prime ??

↳ i = 36

↳ O(n√n)

↳ 1 x 36
2 x 18
3 x 12
4 x 9
→ 6 x 6 ← same
9 x 4
12 x 3
18 x 2
36 x 1

fundamental theorem of arithmetic

any number (+ve except 1) can be represented as product of power of primes:

$$X = p_1^a \times p_2^b \times p_3^c \ldots \ldots$$

$[p_i \in \{\text{prime no.}\}]$

$a, b, c \longrightarrow$ whole no.

$X = 6 \longrightarrow 2^1 \times 3^1$

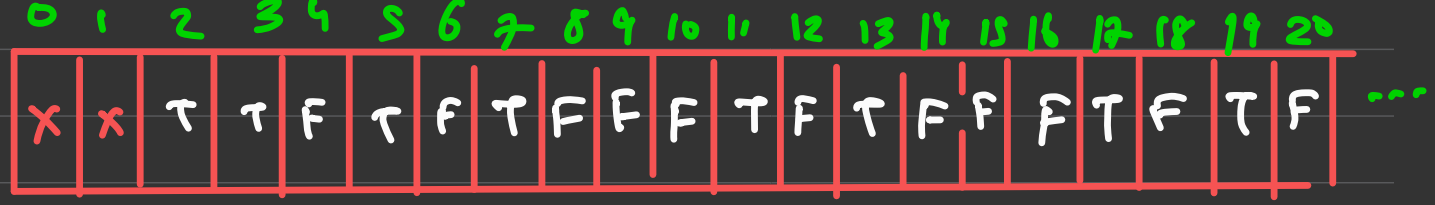
$X = 12 \longrightarrow 2^2 \times 3^1$

$X = 7 \longrightarrow 7^1$

Prime Sieve (ERATOSTHENES)

↳ Based on the fact that composite numbers are divisible by prime, we will filter them out.

↳ O(n) → space → bitset



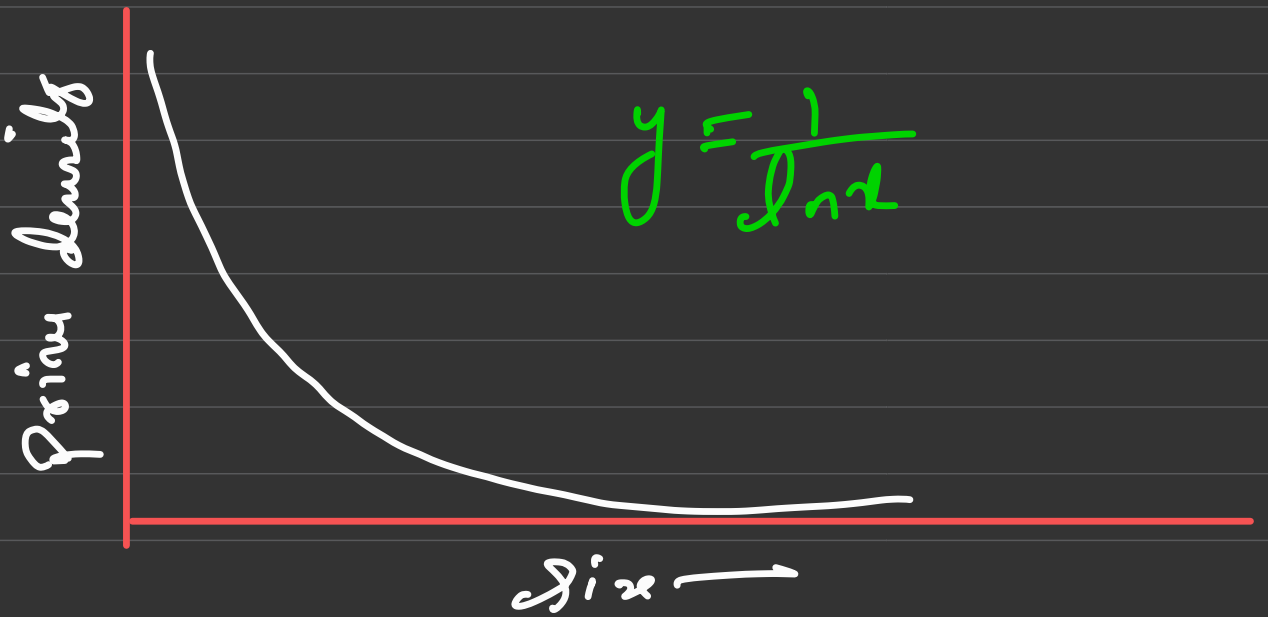
TC → $\frac{n}{2} + \frac{n}{3} + \frac{n}{5} + \frac{n}{7} \cdots\cdots$

$$TC \rightarrow \sum_{p=2}^{K} \frac{n}{p}$$

K is the prime just less than n

first n no.'s	# primes
100	25
10^3	168
10^4	1229
10^5	9592
⋮	⋮

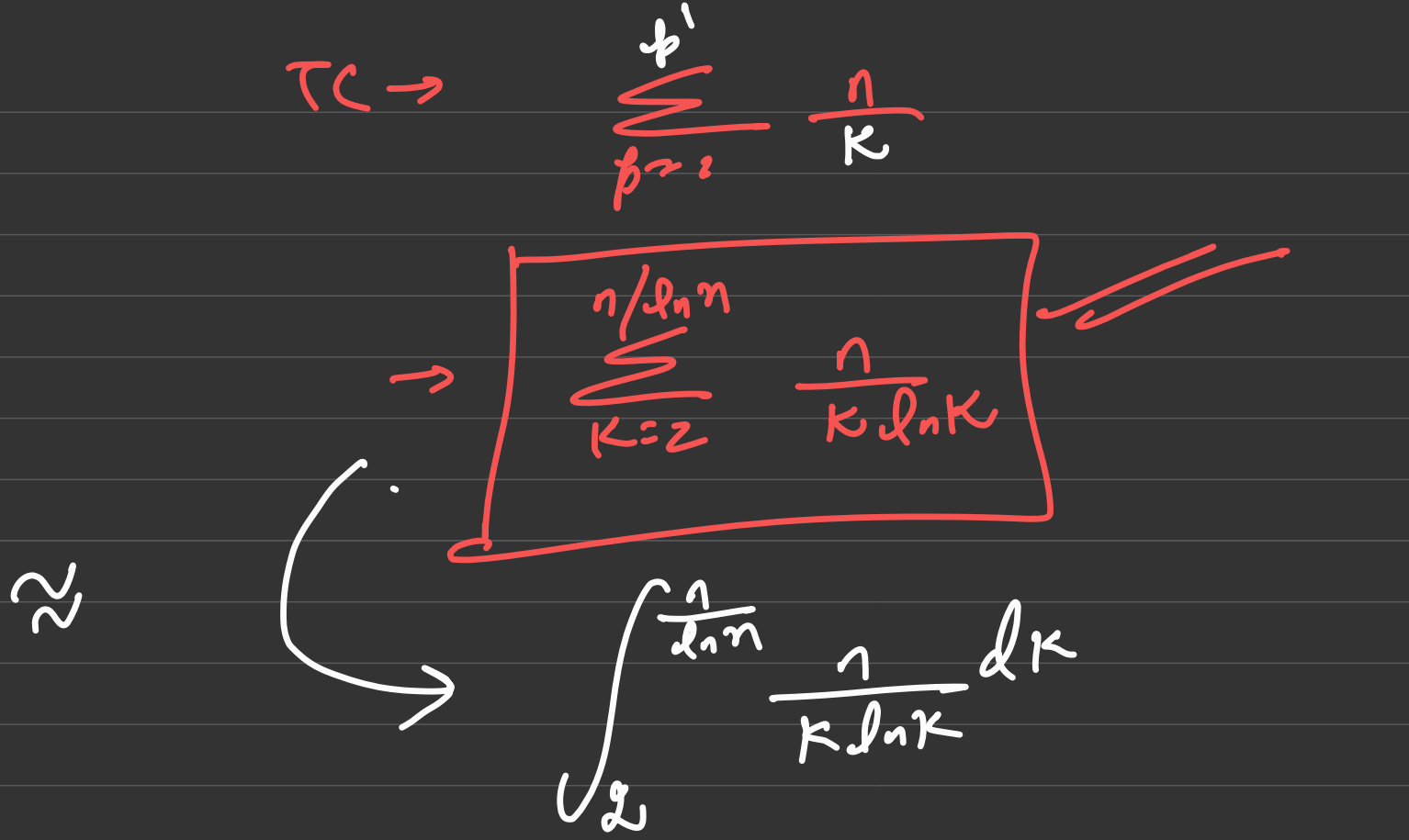
Density of prime no. → $\frac{\#\text{ of prime}}{\text{Total no.'s.}}$



# of primes less than x

$$\pi(x) \simeq \frac{x}{\ln x}$$

↳ k^{th} prime $\simeq k \ln k$


TC →
$\sum_{p=1}^{n}$
$\frac{n}{k}$
$\sum_{k=2}^{n/\ln n}$
$\frac{n}{k \ln k}$
$\approx$
$\int_2^{\frac{n}{\ln n}} \frac{n}{k \ln k}\, dk$

$$n \int_2^{\frac{n}{\ln n}} \frac{1}{k \ln k} \, dk$$

$$\hookrightarrow \quad n \times \left[\ln(\ln k) \right]_2^{n/\ln n}$$

$$n \left[\ln \ln \left(\frac{n}{\ln n} \right) - \ln(\ln 2) \right]$$

$\ln(\ln 2)$ is a constant

$$n \times \left(\ln \ln(n) - \ln \ln \ln n \right)$$

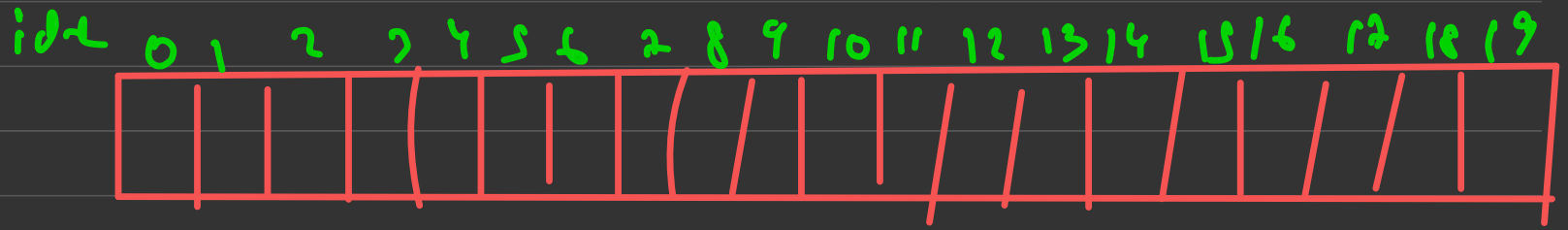
$\ln \ln \ln n$ → lower order

TC → $O(n \ln(\ln(n))) \rightarrow O(n \log\log(n))$

Q.

→ potential → 10^8

Sieve → [6, 17]



6 7 8 9 10 11 12 13 14 15 16 17 18

(2, 3, 5, 7, 11, 13, 17, 19)

→ $\min < 1e^9$

$\lceil 1e^9 \rceil$

p - 5 Prime no.

we want first multiple $\geq a$

$$x \Rightarrow \left(\frac{a}{p}\right) \times p$$

$x < a$

↳ $x += a$

$a = 13$

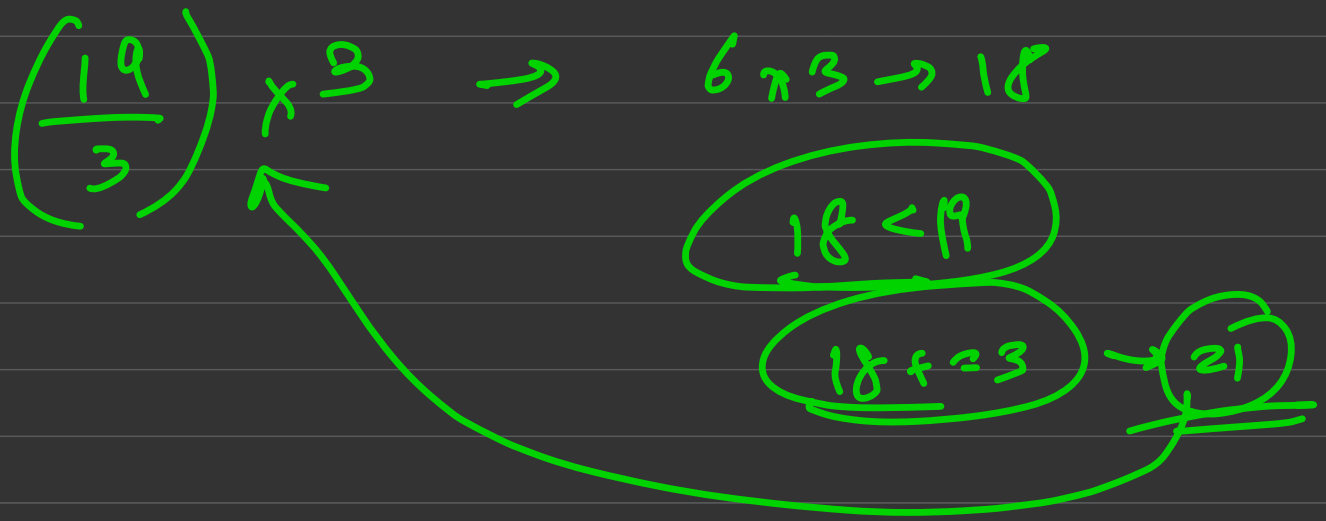
$p = 2$

$\left(\frac{13}{2}\right) \times 2$

$6 \times 2 \rightarrow 12 \rightarrow 14$

$\left(\frac{16}{2}\right) \times 2$

↳ $8 \times 2 \rightarrow 16$


19/3
x3
6x3 → 18
18 < 19
18 + 3
21