Prime Numbers

↳ fundamental concepts of prime no.

Agenda → Basics of prime sieve

Optimisation

Segmented Sieve

P.S

Fib

Q: You have a number N, print all the prime no.'s less than N.

N = 60 → [2, 3, 5, 7]

→ Brute force → Go from 2 → N & for every no. check if it is a prime or not: $O(N^2)$

→ Current, check if it is prime

2 → x-1 → $O(x)$

$O(N\sqrt{N})^2$

2 → $\sqrt{x}$

$n = 36$

$\sqrt{n}$

1×36

2×18

3×12

4×9

6×6

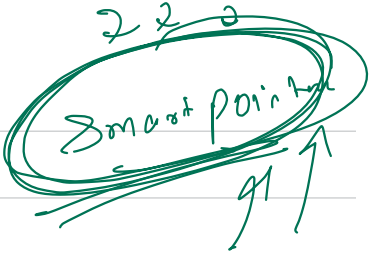
9×4

12×3

18×2

36×1

Sieve of eratosthenes



fundamental theorem of arithmetic

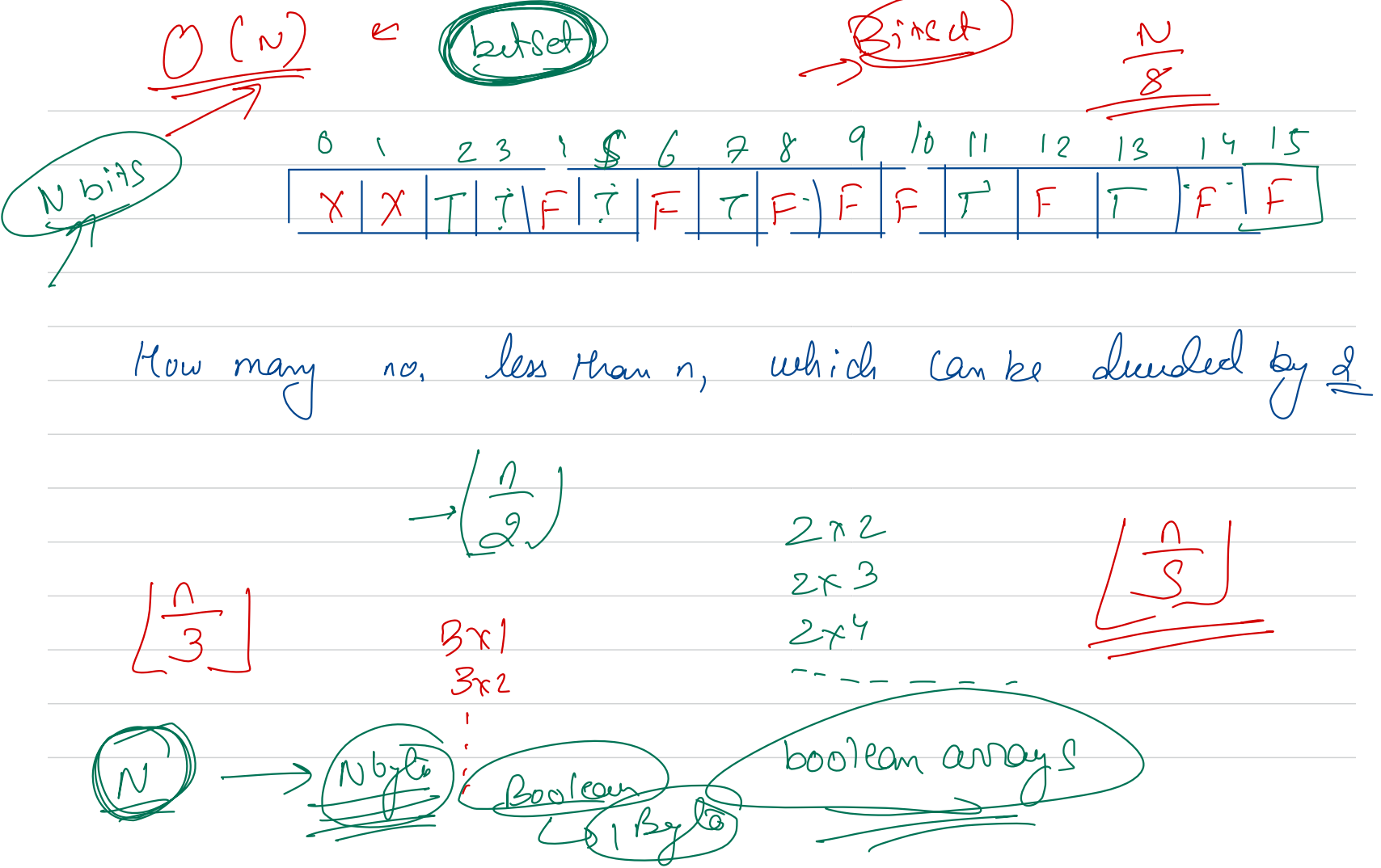
X = product of power of primes

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

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

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

any one prime no, can be a factor of multiple composites


O(N)
bitset
Bitset
N/8
N bits
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
X X T T F T F T F F F T F T F F
How many no. less than n, which can be divided by 2
n/2
n/3
n/5
2x2
2x3
2x4
3x1
3x2
N
N byte
Boolean
1 Byte
boolean arrays

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

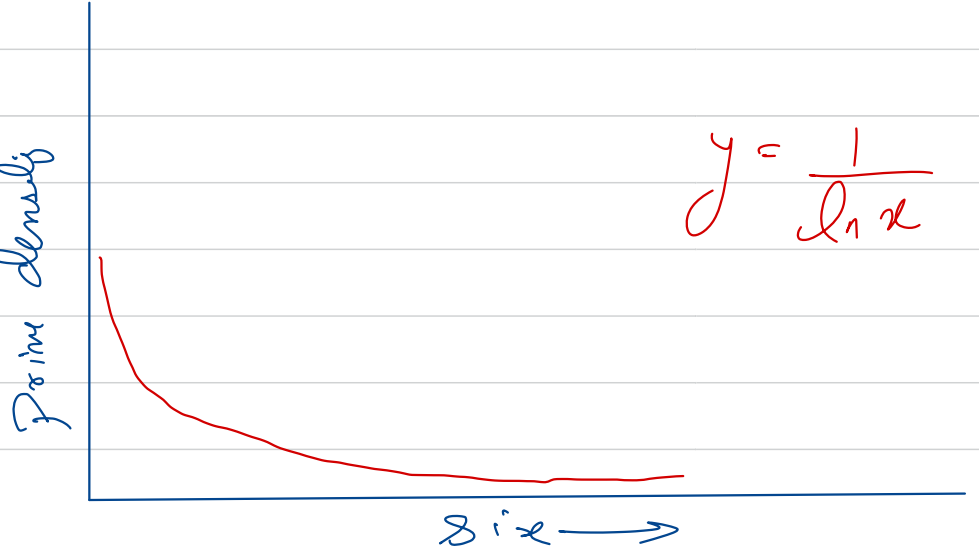
$\rightarrow$ $\sum_{p=2}^{\text{prime} \le n} \frac{n}{p}$

prime no. theorem $\rightarrow$ Ulam spiral

First n no.	# prime
10^2	25
10^3	168
10^4	1229
10^5	9592
i	?

Density of prime no. → # of prime / Total n no.

in the first 100 nos → 25 %



$y = \frac{1}{\ln x}$

How many prime no. are there which are less than n, Approx

$\longrightarrow$ # prime less than $x \approx \frac{x}{\ln x}$

k^{th} prime $\longrightarrow$ $k \ln k$

$$\sum_{k=2}^{n/\ln n} \times \frac{n}{k \ln k} \longrightarrow n \times \sum_{k=2}^{n/\ln n} \frac{1}{k \ln k}$$

$$\simeq n \times \int_{2}^{\frac{n}{\ln n}} \frac{1}{k \ln k} \, dk$$

$$n \times \left[\ln(\ln(k)) \right]_{2}^{\frac{n}{\ln n}}$$

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

$\ln \ln 2 \hookrightarrow$ constant

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

$$\rightarrow O(n \ln \ln(n))$$

Q: Divisor of factorial

N! → # the divisors

$x \rightarrow p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \cdots \rightarrow \{ p_1, p_1, p_1, \ldots, p_2, p_2, p_2 \}$

(a_1 times, a_2 times)

$n! \rightarrow x \rightarrow 6 \rightarrow 2^1 \times 3^1 \rightarrow \{2, 3\}$

$12 \rightarrow 2^2 \times 3^1 \rightarrow \{2, 2, 3\}$ → subset → well divide

$x = (a_1+1)(a_2+1)(a_3+1)\ \cdots\cdots$

Prime sieve

$a_1 \rightarrow$ highest power of p_1 that divides $n!$

p_1

$(1 \times 2 \times 3 \cdots\cdots \times n)$ [$n!$ comprises of $(1-n)$]

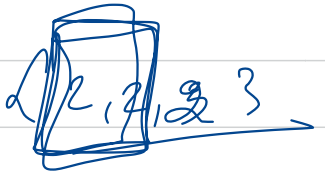
$\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_1^2} \right\rfloor + \left\lfloor \frac{n}{p_1^3} \right\rfloor \cdots\cdots$ 24 $\rightarrow 4!$

$\hookrightarrow$ Legendre's formulae

4!

$1 \times 2 \times 3 \times 4$

24



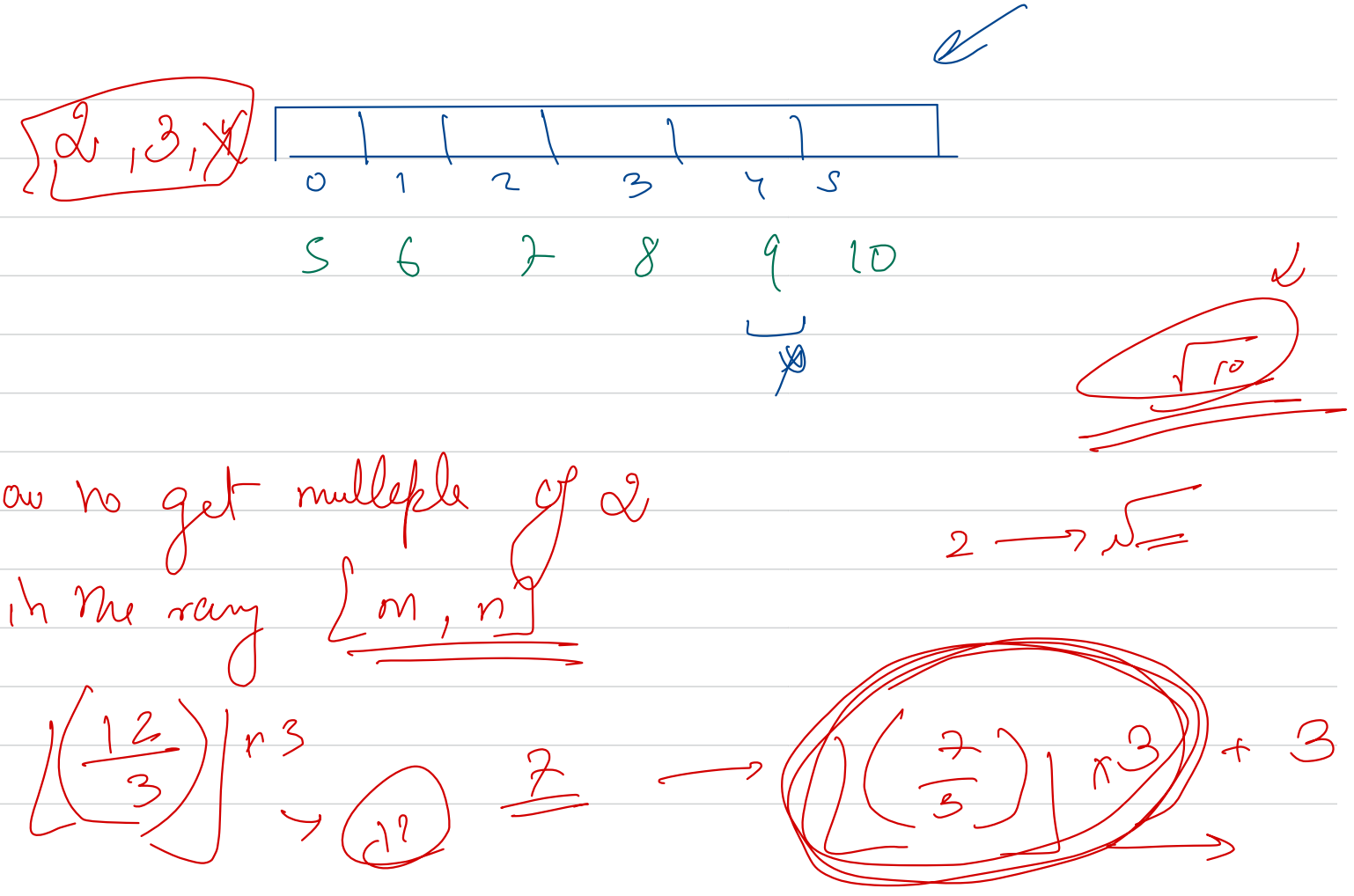
$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2^2} \right\rfloor$$

2 1

Segmented Sieve →

# of factors → $\sqrt{n}$

# of prime → $\frac{n}{\ln n}$


2, 3, 4
0 1 2 3 4 5
5 6 7 8 9 10
√10
How to get multiple of 2
in the range [m, n]
2 → √
[(12/3)] * 3
12
2
[(7/3)] * 3 + 3