

## CLASS-38

## Number Theory

## Sieve of Erathonesis

(@) I - n

$$n \log(\log(n))$$

For (i = 0;  $i < n$ ;  $i++$ )

For ( $j = 0$ ;  $j < n$ ;  $j++$ )

$$\text{Ex} \quad \underbrace{n + n + n + \dots}_{n} \Rightarrow n \times n = n^2$$

## Highest Prime and Lowest Prime

```

graph TD
    A[Prime factorization] --> B[i := 3]
    B --> C[while(n % i == 0)]
    C --> D[i := i + 1]
    D --> E[n := n / i]
    E --> F[n == 1]
    F --> G[return result]
    
```

The diagram illustrates a hand-drawn pseudocode for prime factorization. It starts with a box labeled "Prime factorization". An arrow points from this box to a box containing the assignment  $i = 3$ . Another arrow points from this box to a loop structure. The loop is defined by a box labeled "while( $n \bmod i == 0$ )". Inside the loop, there is a brace labeled " $i = i + 1$ ". Below this, another brace labeled " $n = n / i$ " is shown. Finally, an arrow points from the condition box to a box labeled "n == 1", which then points to a final box labeled "return result". A large brace on the right side groups the entire loop structure and the final return statement, with the label "O(n)" written next to it.

L, Using Sieve

$O(n \log(n))$

Highest - Prime factor

Lowest - Prime factor

$HP, LP$        $\varnothing \rightarrow$

$$36 = 2 + 2 + 3 * 3$$

$$\begin{cases} LP = 2 \\ HP = 3 \end{cases}$$

Vector  $\langle \text{int} \rangle \rightarrow \text{Prime-factors};$

$\log(n)$

while ( $num > 1$ )  
 int prime-factor =  $\lfloor num / i \rfloor$ ;

$8 \cdot 1 \cdot 9 = 88$

$11 \cdot 2$

$n = 88$

$$num = P_1 * \dots * P_k$$

$num = 1$

while ( $num \neq 1$  &  $P\text{-factor} \neq 0$ )  
 num =  $P\text{-factor};$   
 Prime factors. Push-back ( $P\text{-factor}$ )

$$88 \rightarrow 2 * 2 * 2 * 11$$

88

$$LP(88) = 2$$

Prime factors.

$$11 | 2 | 2 | 2$$

$$HP(88) = 11$$

$$HP(88) = 11$$

$$HP(88) = 11$$

$O(\sqrt{n})$

for ( $i=3$ ;  $i * i \leq n$ ;  $i+=2$ )  
 while ( $n \neq 0$  &  $i \neq 0$ )  
 $n := i;$

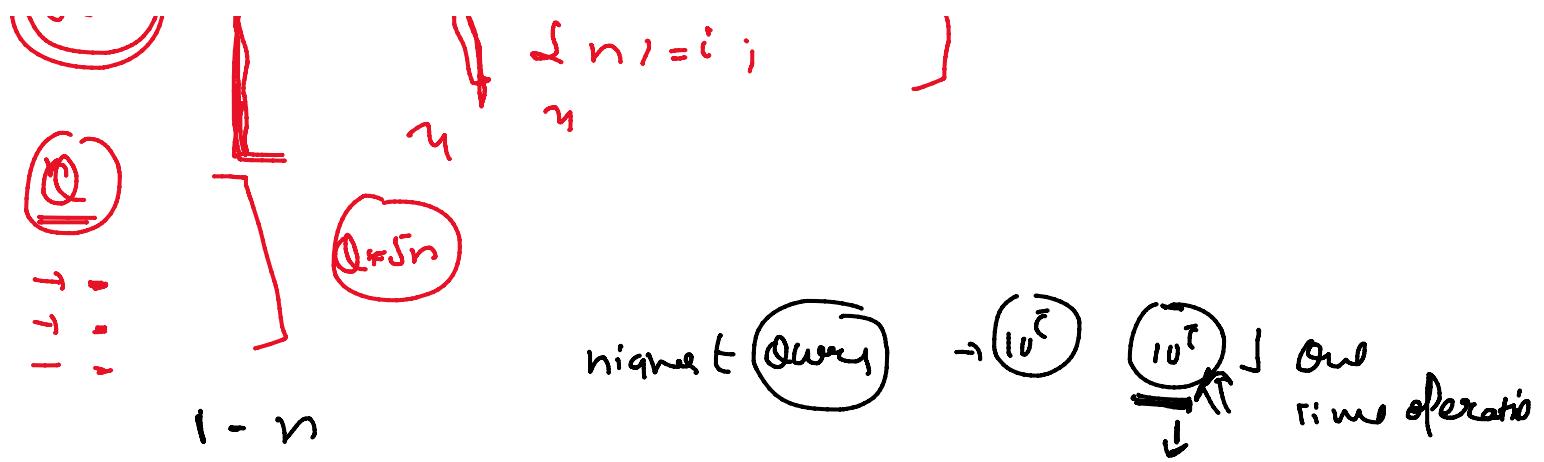
$$88$$

5

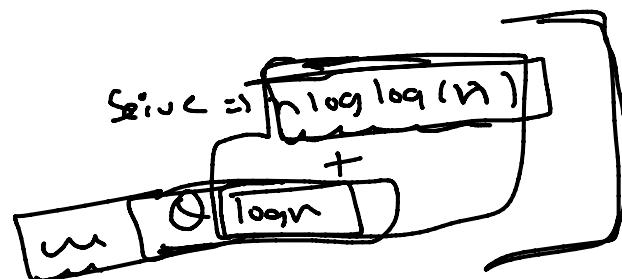
7

9

11



$$\begin{aligned}
 6 &= 2, 3 \\
 \underline{\text{hP}(6)} &= 3 \quad \text{hP}(2) = 0 \\
 \text{With respect to } 6^{403} &= 01 \quad (2^{403} = 0)
 \end{aligned}$$



Sieve  $\rightarrow 1 - n \text{ Primes } \rightarrow n \log \log n$   
 $\rightarrow$  Highest Prime  $\times 2^p$   
 $\rightarrow$  Prime factorization  
 $\rightarrow$  Divisors?

$1 - N$

$36 \rightarrow 1, 2, 3, 4, 6, 9, 12, 18, 36$

$\rightarrow$  Divisors  
 for 1 element

```

    for (i = 1; i * i <= N; i++)
      if (n % i == 0)
        t[n] = i
  
```

```
    ^      '
    |      |
For (i=1; i<=n; i++)
    )
```

$n \cdot \sqrt{n}$

Seive

3

1

2

```
vector<int> divisors(N);
```

221 3rd, 4x1

2, 4, 6, 8, 10, 12 —

i<sup>th</sup> element divisor of  
j<sup>th</sup> element

6, 12, 18      ) no log in-

$3 \rightarrow 3$  G, a, 12, 15, 18 --

$$z + \frac{z}{z} + \frac{z}{z} + \frac{z}{z} + \frac{z}{z} + \dots$$

$$6 \rightarrow \underline{3, 6}$$

$$q \rightarrow \overline{3}$$

12 73

$$N \left\{ 1 + \frac{1}{2^1} + \frac{1}{3^1} + \frac{1}{4^1} + \dots \right\}$$

$$12 \rightarrow 3, 6$$

leaf

Nlogn

## → facts about Numbers

## Goldbach's Conjecture

## Goldbach's Conjecture

Every even number greater than 4 can be written as sum of 2 odd prime

$$6 \rightarrow 3 + 3$$

$$12 \rightarrow 7 + 5$$

$$18 \rightarrow 13 + 5$$

$$8 \rightarrow 5 + 3$$

$$14 \rightarrow 7 + 7$$

$$20 \rightarrow 17 + 3$$

$$10 \rightarrow 7 + 3$$

$$16 \rightarrow 11 + 5$$

1 → Prime

## Twin Prime Conjecture

There are many

-twin prime

↳ prime nos with diff of 2

$$(5, 3) (7, 5) (11, 13) (17, 19) (29, 31) - - -$$

- - - -

## Legendre's Conjecture

$$n^2 < p < (n+1)^2$$

Between any 2 consecutive perfect square we always have atleast prime no

$$\boxed{4, 9}$$

$$\textcircled{4} < \textcircled{3, 5} < \textcircled{9}$$

$$\begin{array}{c} 73 \\ 89 \\ \hline \end{array}$$

$$\begin{array}{ccccccccc} 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 \\ \hline 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 \\ \hline 3 & 5 & 7 & 11, 13 & 19, 23 & 29, 31 & 37, \dots & 53, 59 & \end{array}$$

~~Time complexity~~

## Modular Exponentiation

$\log(P)$

$$\left( \frac{u^P}{n} \right) \text{ O(nm)}$$

$$P \cdot \text{pow}(u, P) \cdot \text{O}(nm)$$

```

int ans = 1;
for (i = 1; i <= P; i++) {
    ans = (ans * P) % mod;
}
  
```

$O(n^2)$

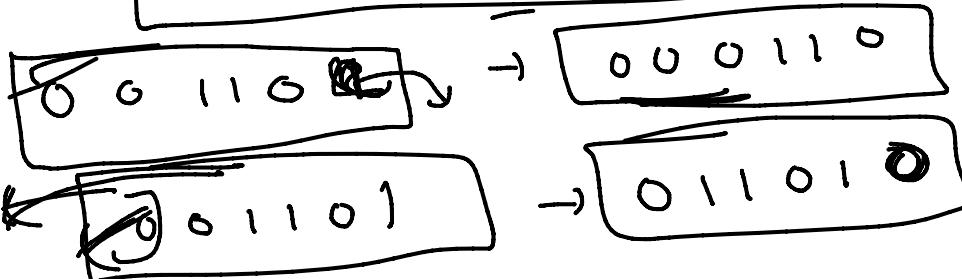
$O(P)$

Bits

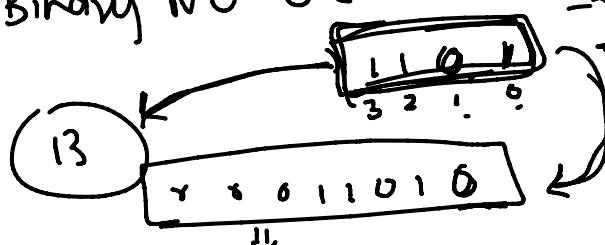
$3 \rightarrow 11$



left shift right shift



Binary NO decimal No  $\rightarrow$



$$2^3 \times 1 + 2^2 \times 0 + 2^1 \times 1 + 2^0 \times 1 = 13$$

$$2^3 \times 0 + 2^2 \times 1 + 2^1 \times 0 + 2^0 \times 1 + 2^3 \times 1 + 2^2 \times 1 + 2^1 \times 0 + 2^0 \times 1 = 26$$

$$2^0 \times 0 + 2^1 \times 1 + 2^2 \times 1 = 13$$

$$0 \ 0 \ 0 \dots 1 \ 1 \ 0 \rightarrow 2^0 \times 0 + 2^1 \times 1 + 2^2 \times 1 = 2 + 4 = 6$$

Binary No  $\rightarrow$  left shift  $n \leftarrow n \times 2$

Right Shift ( $n / 2$ )

$$\frac{13}{2} = 6$$

(n)

$$n \leftarrow n \times 2$$

$$n \leftarrow n / 2$$

$$n = n \gg 1$$

$$n = n \ll 1$$

$$n = n / 2$$

Put Power (int u, int y, int m)

int res = 1;

while ( $y > 0$ )

{ if ( $y \geq 1$ )

{ res = (res \* u) % M

y

$O(n) \rightarrow O(\log n)$

$y = y \gg 1$

$u = (u + u) \% M$

$$\begin{array}{r} 2 \\ 3 \times 3 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 2 \\ 3 \times 3 \\ \hline 3 \end{array} \times 3 = 3$$

$$T.C = O(nm)$$

$$O(n) \rightarrow O(\log n)$$

Modular  
exponentiation

Decimal representation

$$y \neq 1$$

$$\begin{array}{r} y \rightarrow - \\ u \\ \hline u - 2 \end{array}$$

$$13 \rightarrow \begin{array}{r} 11 \\ - \end{array} \quad y \rightarrow \begin{array}{r} 1 \\ - \end{array}$$

$y = 3^x$        $13 \rightarrow 11_3$        $y \rightarrow \underline{\quad}$   
 $3^{13} \Rightarrow u=3$        $u = 3^2 \times 3^2 \times 3^4 \times 3^4 = 3^8 \times 3^8 = 3^{16}$        $y \rightarrow 00000$   
 $\text{loop}$        $11_3 = 1 + 1 \times 3 + 1 \times 3^2 + 0 \times 3^3 + 1 \times 3^4 = 84$   
 $84 \rightarrow 101000_2$        $3^8 \times 3^8 \rightarrow 3^{16}$   
 $\text{Binary}$   
 $6^4 = 32 + 16 + 8 + 4 + 0 + 1$