Number Theory

- Divisor
- GCD, LCM
- Divisibility
- Prime numbers
  - Checking
  - Generating
  - Factorization

- Modular arithmetic

Divisors

N → N > 0 , integer

10 : 1 [2, 5, 10

10/2

1, [2, 3, 4, 5,] 6, 7, 8, 9, 10

N

O(N) — O(N/2) → O(N)

N → 1, 2, ... [N/2], N

9 → 1, 3, 9

1) 10 (10

0

2) 10 (5

40 → 1, 2, 4, 5, 8, 10, 20, 40

$\sqrt{40}$ = 6.—

→ (1, 40), (2, 20), (4, 10), (5, 8)

64 → (1, 64), (2, 32), (4, 16), (8, 8), ~~(1, 7)~~

8 = $\sqrt{64}$

Given an integer, N, find its +ve divisors.

Given the +ve divisors, find N;

GCD, LCM

GCD (A, B) =

LCM (A, B) =

A = 10, B = 15

GCD (A, B) = 5

LCM (A, B) = 30

30, 60, 90, 120, ...

10: 1, 2, 5, 10

15: 1, 3, 5, 15

GCD(A, B) সর্বোচ্চ কত-হতে পারে?

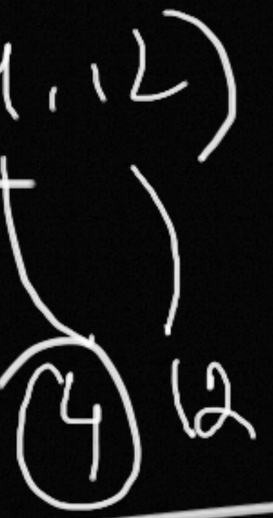
(10, 15) = 5

(3, 5) = 1

(3, 4) = 1

(6, 8) = 2

(4, 12) = 4



O(N)

GCD(A, B) : min(A, B)

[1, 10]

Euclidean method

10	15	1
	10	
5	10	2
~~5~~	10	
	0	

↑

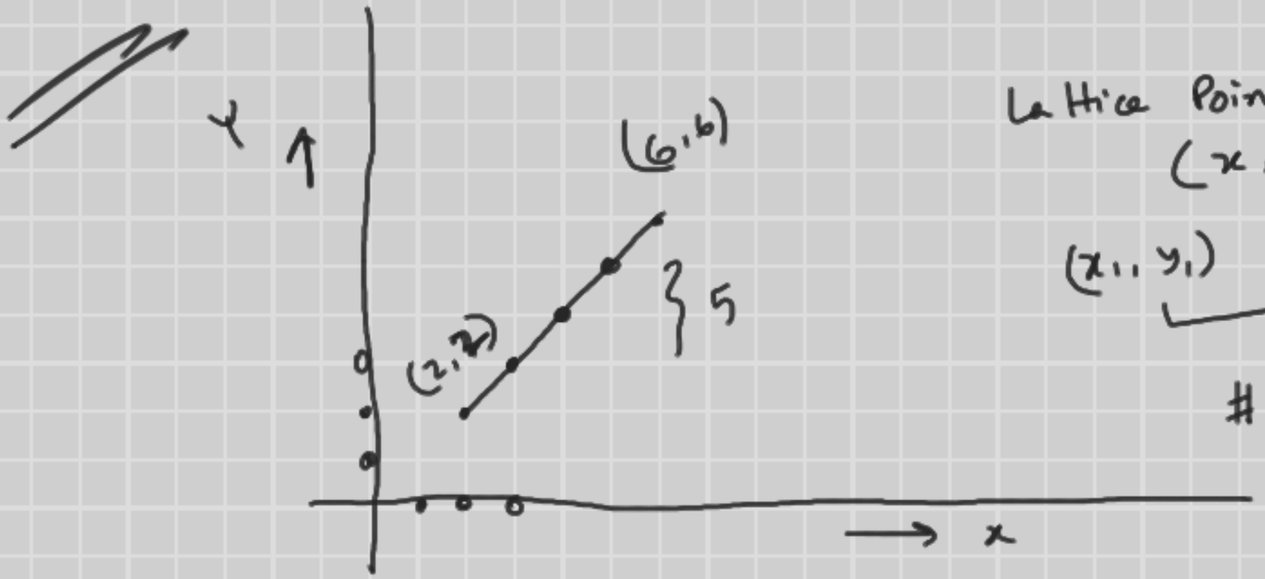
15	10

LCM(A, B) : Max(A, B)

LCM(10, 15) → 15, 16, 17, 18, . . . , 30

↑

$$LCM(A,B) = \frac{A \times B}{GCD(A,B)}$$



Lattice Points

(x, y)

(x_1, y_1) (x_2, y_2)

↓

# of lattice points

Given A, B → GCD, LCM

Given. GCD(A, B) and LCM(A, B)

→ Find A and B ?

Prime Numbers

$O(\text{sqrt}(N))$

$N = 1, N$

1, 2, 3, 5, 7, 11, 13, ...

[1000 digits]

$N = \{1, N\}$

$\{1\}$

$[1, N]$

$[1, 1]$

M

M x N → O(sqrt(N))

→ O(M x sqrt(N))

→ O(P x log(log(P)))

Sieve of Eratosthenes

$\frac{N \times \sqrt{N}}{N \times \log(\log(N))}$ → Prime

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

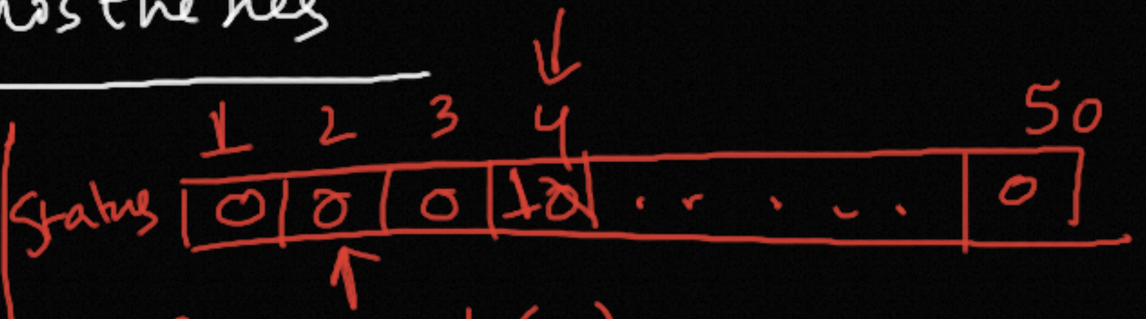
$3 \to 9$ (7×3)

$5 \to 25$ (7×5) 35 = 7×5

(7×4, 7×6)

$7 \to 49 \longrightarrow 7 \times 7$

$11 \to 11 \times 11$




```
for(i = 3 ; i <= sqrt(N) ; i+=2)
    if(status[i] == 1) continue;
    for(j = i*i ; j <= N ; j+= i*2)
        status[j] = 1;
```

⇒

$$N/3 + N/5 + \cdots + N/p = \text{sqrt}(N)$$

$$= N\left(1/3 + 1/5 + \cdots + 1/p\right)$$

$$= N \times \log(\log(p))$$

$$\log(10\text{-digit}) = 10$$

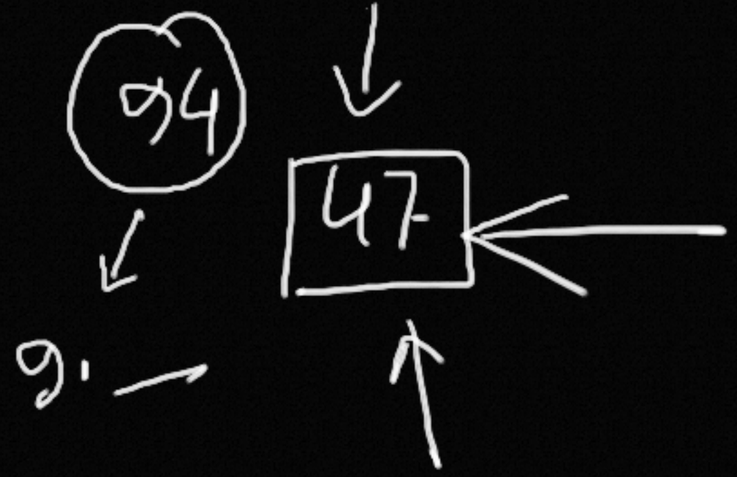
Prime factorization

$20 = 2 \times 2 \times 5 = 2^2 \times 5^1$

$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3^1 \times 5^1$

$N = p_1^{a_1} \times p_2^{a_2} \times \ldots\ldots \times p_n^{a_n}$

2, 3, 5, 7, 11, 13, 17, - - - , 47



$40 = 2^3 \times 5^1$

$98 = 2^1 \times 7^2$

$94 = 2^1 \times 47^1$

2×997

	2	3	5	7	11	13
40(6-)	11		1			
60(7-)	30	5	1			
	↓					
	15					
14(3-)	7		1			

2×7

	2	3	5	7
60	30	15	5	
↓	↓	↓	↓	
7	15	5	1	
	(4)			

$$N = p_1^{a_1} \times p_2^{a_2} \times \ldots \times \underbrace{p_n}_{\uparrow}^{a_n}$$

Largest Prime factor of N

Find the prime that occurs maximum times

Given the prime factor of N, find # of divisors of N

$40 = \boxed{2^3 \times 5^1}$

$= 1, 2, 4, 5, 8, 10, 20, 40$

$$A = \frac{p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}}{}$$

$$B = \frac{p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_m^{a_m}}{}$$

$GCD(A,B) =$ _____

$LCM(A,B) =$ _____

$$10 = \frac{2^1 \times 5^1}{}$$

$$15 = \frac{3^1 \times 5^1}{}$$

$GCD = 5^1$

$LCM = 2^1 \times 3^1 \times 5^1$

✓