Prime numbers, Factorization and GCD-LCM

Course on Mathematics & Puzzles for Interview Preparation

Arjun Arul • Lesson 1 • Feb 9, 2021

Maths and Puzzles

Lecture 1

Prime Numbers and Prime Factorisation

Prime No -> 1 & n -> divisors.

$a \mid b \rightarrow$ a divides b.

$10/5 = 2$

$a \nmid b = 0$

$5/10 = 1/2$

$a/b \Rightarrow a \mid b$

$5 \mid 10$

$x = \frac{b}{a}$

$\exists$ $a \mid b \rightsquigarrow b = xa$

$b \mid c \rightsquigarrow c = yb$ (2)

$\Rightarrow a \mid c$ $\quad c = yxa$

$= (yx)a$

$a \mid c$

$a \mid b$

$a \mid c$

$a \mid mb + nc$

$a \mid mb + nc$

$mb + nc$

a

$\frac{mb}{a} + \frac{nc}{a}$

$a \mid b$ $\quad$ $a \mid c$

$\Downarrow$ $\quad$ $\Downarrow$

$\frac{b}{a} = n$ $\quad$ $\frac{c}{a} = m$

$a \mid xb + yc$

$\frac{xb + yc}{a}$ $\quad$ $\frac{xb}{a} + \frac{yc}{a}$

$= xn + ym$

$3 \mid 12 \qquad 3 \mid 9$

$\Rightarrow 3 \mid 12 \times 7 + 8 \times 9$

$a \mid b$ & $c \mid d$

$\frac{b}{a} = n$

$\frac{d}{c} = m$

$ac \mid bd$

$2 \mid 8$

$\frac{8}{2}$ is integer

$\frac{bd}{ac} = \frac{b}{a} \cdot \frac{d}{c}$

$= n \cdot m$

$3 \mid 21$

↳ $\frac{21}{3}$ is an integer

$2 \mid 6$ $\quad$ $7 \mid 21$

$\Rightarrow 14 \mid 126$

63

~~125~~

~~4~~

>

$= 9$

$a \mid b \;\&\; b \mid c \Rightarrow a \mid c$

$a \mid b \;\&\; a \mid c \Rightarrow a \mid xb + yc$

$a \mid b \;\&\; c \mid d \Rightarrow ac \mid bd$

1) $2 \mid 6 \;\&\; c \mid 18 \Rightarrow 2 \mid 18$

2) $2 \mid c \;\&\; 2 \mid 4 \Rightarrow 2 \mid 6x + 4y \Rightarrow 2 \mid 12 + 2y$

$ac \mid bd$

~~$\Rightarrow$~~ $a \mid b$ & $c \mid d$?

$3 \cdot 7 \mid 6 \cdot 49$

$\Rightarrow 3 \mid 6$ & $7 \mid 49$

$2 \times 3 \mid 3 \times 2$

$2 \nmid 3$ $\quad$ $3 \nmid 2$

$a \mid c$ & $b \nmid c$

$\not\Rightarrow$ $a \mid b$?

$2 \mid 6$ & $3 \mid 6$

$a \mid c$ & $a \nmid b$

$\Rightarrow$ $b \mid c$?

$2 \mid 10$ & $2 \mid 14$

$14 \mid 10$

$10 \mid 14$

Prime factorization

$\frac{84}{2} = 42$ $\quad\quad$ $\frac{21}{3} = 7$

$\frac{42}{2} = 21$

$84 = 2 \times 42 = 2 \times (2 \times 21) = 2 \times 2 \times 3 \times 7$

$= 2^2 \times 3 \times 7$

$84 = 11 \times 7$

non-1

1) Smallest factor of any integer is a prime.

$n \rightarrow$ Smallest factor $= x \leq \sqrt{x \times y}$

$c \mid n \equiv xy \mid n \Rightarrow x \mid n$

$84 = \cdots\cdots\cdots$

$2^{2} \times 3 \times 7$

$\frac{84}{2} = 42$

$\frac{42}{2} = 21$

$\frac{21}{3} = 7$

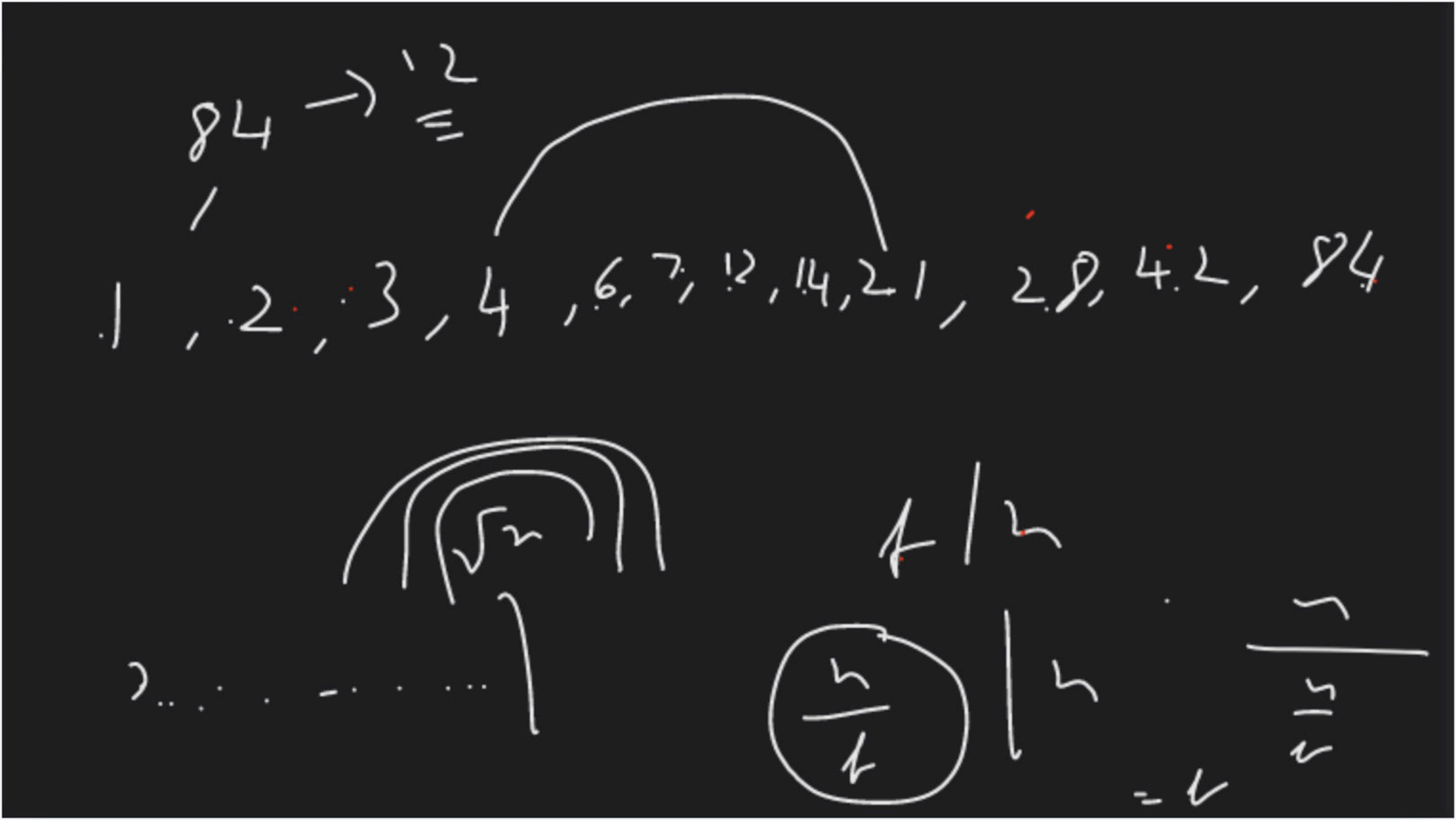
$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

$p_1, p_2, p_3 \ldots, p_k$ are primes

$\alpha_i \geq 1$

$$5 = 7^0 \times 11^0 \times 5^1$$

$$3^0$$


84
1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84

n

t , o $\frac{n}{t} \leq \sqrt{n}$

$t > \sqrt{n}$

$\frac{n}{n} > \sqrt{n}$

$t * \frac{n}{t} > \sqrt{n} * \sqrt{n}$

$n > n$ ⊥

$\min\left(t, \frac{n}{t}\right) \leq \sqrt{n}$ ->

$\max\left(t, \frac{n}{n}\right) \geq \sqrt{n}$

Claim

$\min\left(f, \frac{n}{f}\right) \leq \sqrt{n}$

Fix $\frac{n}{f} > \sqrt{n} \times \sqrt{n}$

$n > n$

Proof

→ Assume the contrary.

Assume $\min\left(f, \frac{n}{f}\right) > \sqrt{n}$

$\Rightarrow f > \sqrt{n}$ & $\frac{n}{f} > \sqrt{n}$

$xy \mid n \Rightarrow \frac{n}{xy} = k$

$\Rightarrow n = kxy$

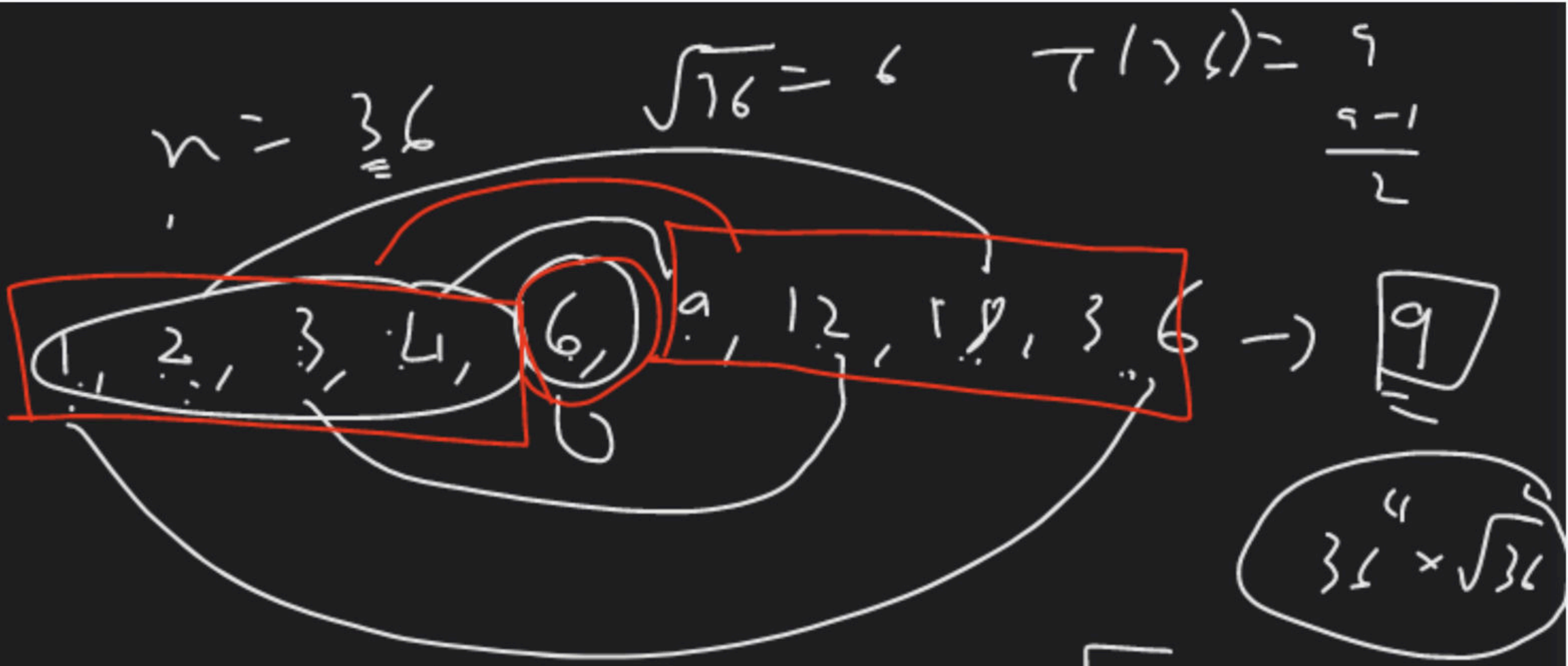
$= x(ky)$

$\Rightarrow x \mid n \;\&\; y \mid n$

$\frac{n}{x} = ky$

$n = y(kx)$

$\frac{n}{y} = kx$



Number of factors of $n \leq 2\sqrt{n}$

$\frac{9}{2}$

$36 =$

$\tau(n)$

$$\frac{\tau(n)-1}{2}$$

n

$$\times \sqrt{} \; n^{\frac{1}{2}}$$

$$\frac{\tau(n)-1}{2} + \frac{1}{2} = \frac{\tau(n)}{2}$$

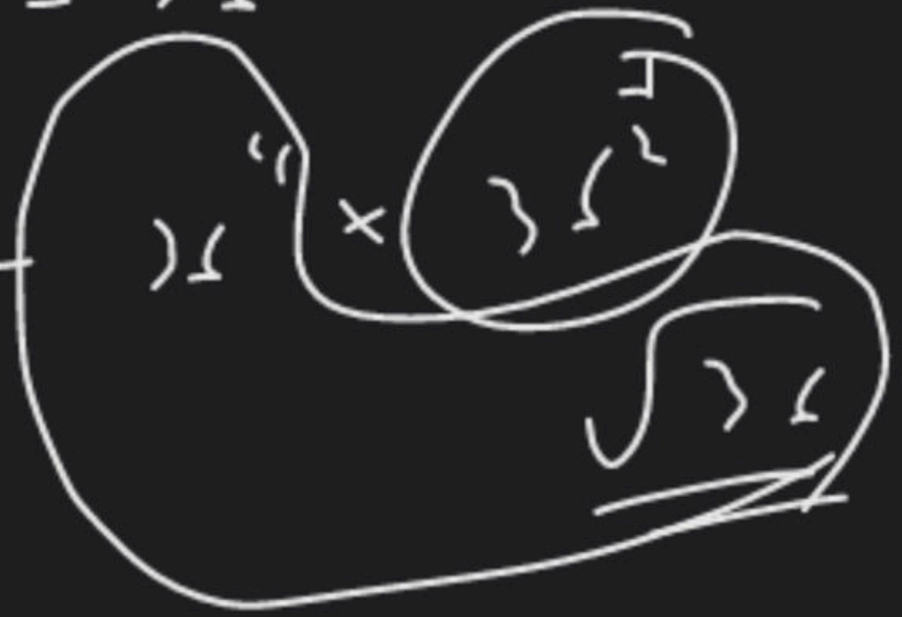
n

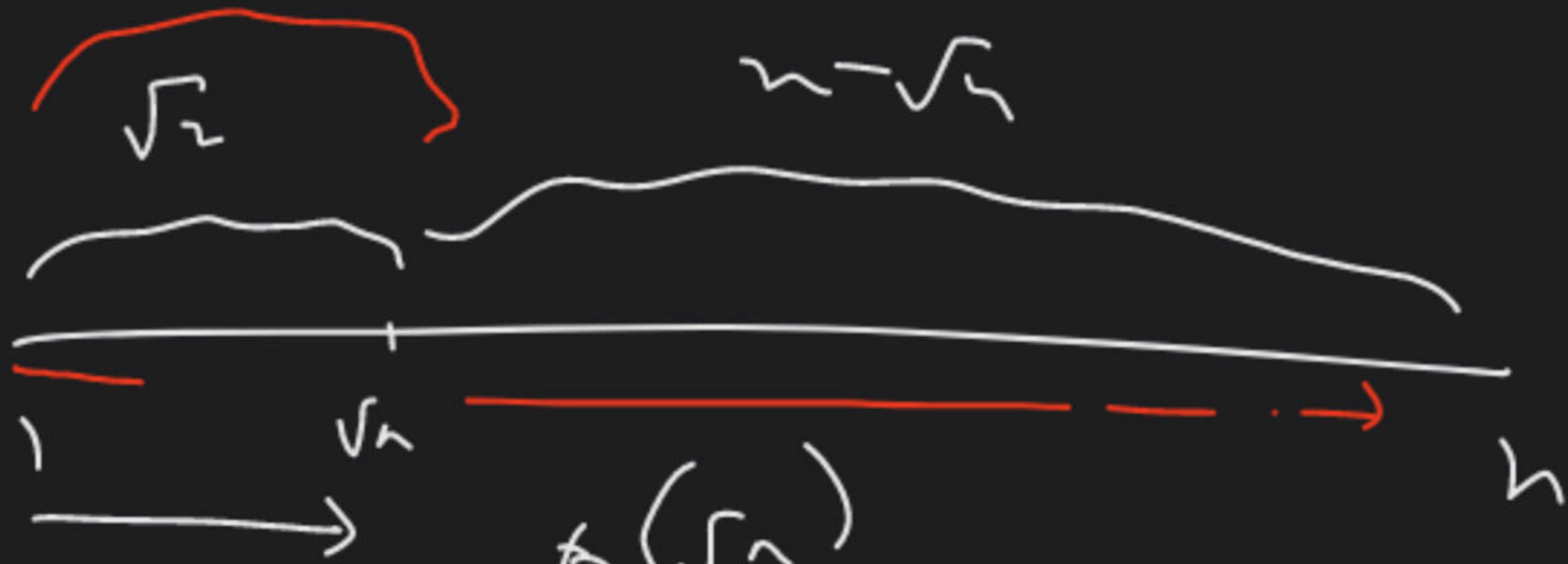
n

$$36^{\frac{9}{2}} = 36^{\frac{8+1}{2}} = 36^{4+\frac{1}{2}}$$

$$= 36^{4+\frac{1}{2}}$$

Perfect square → odd #





$O(\sqrt{n})$

$n = 100$

$\frac{n}{2} = 50$

$\sqrt{n} = 10$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$\tau(n)$ = The number of factors of n $= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$

$84 = 2^2 \times 3^1 \times 7^1$

$\tau(84) = (2+1)(1+1)(1+1) = 3 \times 2 \times 2 = \underline{12}$

$$36 = 2^2 \times 3^2$$

$$\tau(36) = (2+1)(2+1)$$

$$= 3 \times 3$$

$$= 9$$

$42 = 2^1 \times 3^1 \times 7^1$

$\tau(42) = 2 \times 2 \times 2$

$= 8$

1, 2, 3, 6, 7, 14, 21, 42

n

$[2, \sqrt{n}) - x$

$2 > \sqrt{n}$

$\frac{n}{2} < \frac{\sqrt{2} \times \sqrt{n}}{2} < \frac{\sqrt{n} \times \sqrt{n}}{\sqrt{n}}$

$n = p_1^{\alpha_1}$

$n = 5$

$p_1^0, p_1^1, p_1^2, p_1^3, \ldots\ldots, p_1^{\alpha_1}$

$a \mid b$

$\alpha_1 + 1$

$\exists t \qquad a \mid \mu$

$p_1 > \alpha_1$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$t \to p_1^{\beta_1}$

$\frac{\mu}{a}$ $\quad p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$n = p_1^{\alpha_1}$

$7^5 = 6$

$1, 7, 49, 343, \ldots$

$1, p_1, p_1^2, \ldots\ldots p_1^{\alpha_1}$

$\alpha_1 + 1$

$n = p_1^{\alpha_1} p_2^{\alpha_2}$

$\beta_1 \in \{0, 1, 2 \ldots \alpha_1\}$

$\beta_2 \in \{0, 1, 2, \ldots \alpha_2\}$

$\beta_1 \leq \alpha_1$

$(\alpha_1 + 1)(\alpha_2 + 1)$

↳ $p_1^{\beta_1} p_2^{\beta_2}$

$\beta_1, \beta_2 \geq 0$

$(\alpha_1 + 1)(\alpha_2 + 1)$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

$$\beta_i \in \{0, 1, \ldots, \alpha_i\} \quad \alpha_i + 1$$

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = n$$

Given n

Find number of integers x where $\tau(x) = n$

& prime factors of x are $[2, 3, 5, 7, 11]$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Find Sum of all factors.

$n = 12 = 2^2 \times 3^1$

$\tau(12) = 3 \times 2 = 6$

1, 2, 3, 4, 6, 12

Sum $= 1+2+3+4+6+12$

$= \boxed{28}$

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}\right)$$

$$\left(1 + \cdots\right) \cdots$$

$$\left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}\right)$$

$$n = 12 = 2^2 \times 3^1$$

$$\text{Sum of factors} = (2^0 + 2^1 + 2^2)(3^0 + 3^1)$$

$$= (1 + 2 + 4)(1 + 3)$$

$$= 7 \times 4$$

$$= 28$$

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$$

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}\right)$$

$$= p_1^{\beta_1} p_2^{\beta_2}$$

$$= p_1^{\beta_1} p_2^{\beta_2}$$

$$(a+b)(c+d)$$

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$f \times \frac{n}{f} = n$

Product of all factors?

$n = 12$

$12 \times 12 \times 12 = 12^3$

1, 2, 3, 4, 6, 12

product $= 24 \times 72 = \underline{1728}$

$9 = 3^2$

$\tau(9) = 3$

1, 3, 9

$\frac{\tau(9)}{2}$ $\quad$ $\frac{3}{2}$

$9^{\frac{\tau(9)}{2}} \quad 9^{\frac{3}{2}} \quad 9^2$

$$n^{\frac{\tau(n)}{2}}$$

1. I understand what is Prime Factorisation

A. Very Clear
B. Somewhat Clear
C. Please explain again

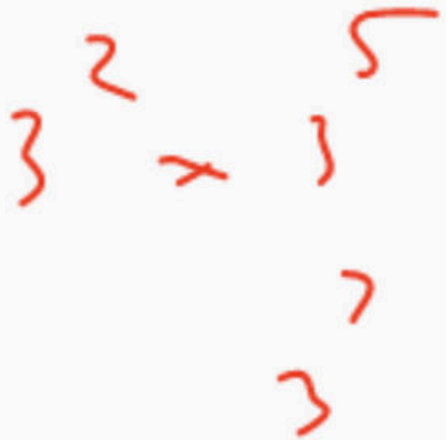
2. In the given Prime Factorisation, p1 can be same as p2.

$$n = p_1^{a_1} \cdot p_2^{a_2}$$

A. True
B. False

2. In the given Prime Factorisation, p1 can be same as p2.

$$n = p_1^{a_1} \cdot p_2^{a_2}$$



A. True

B. False

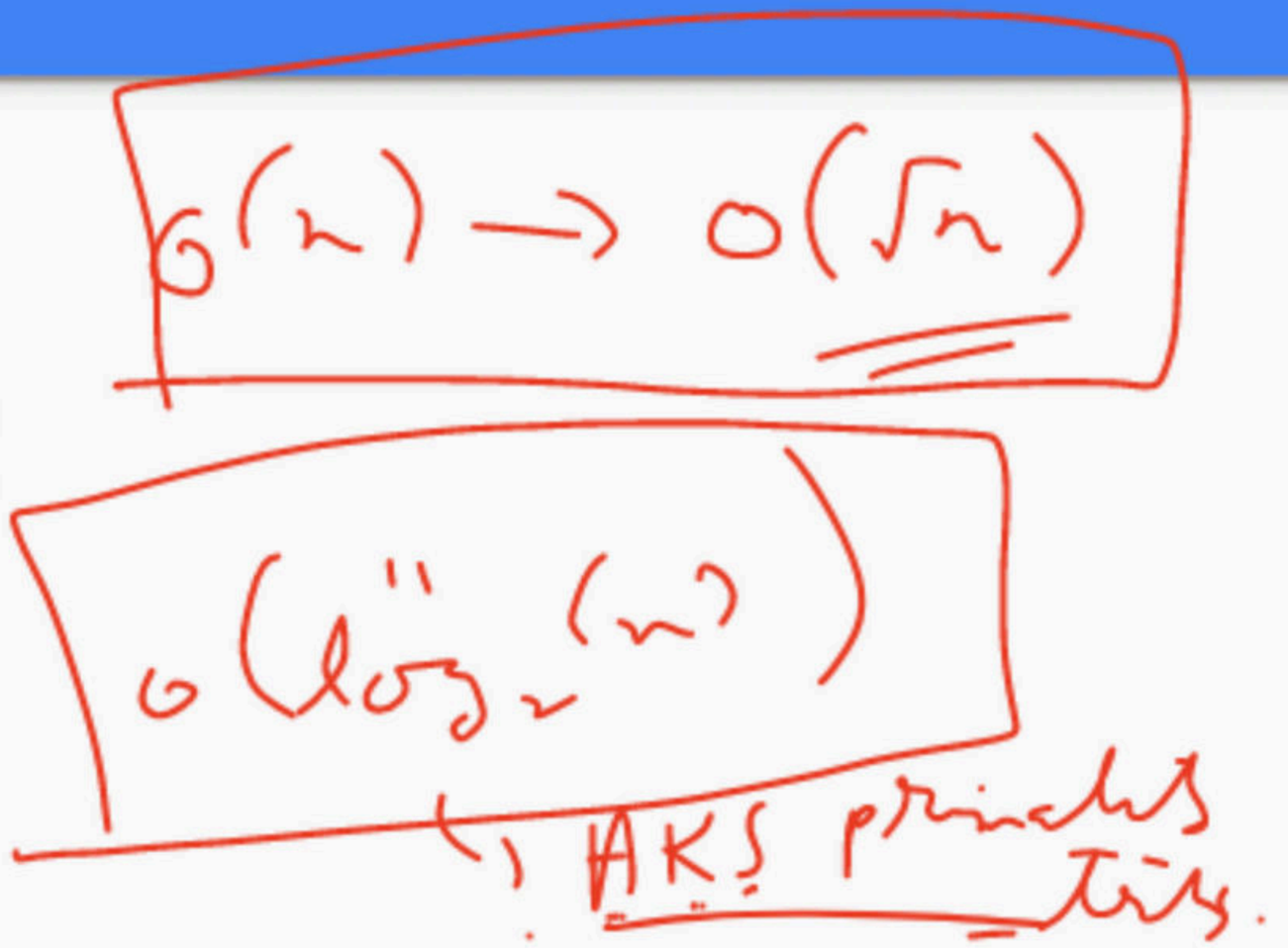
Bonus: Can a_1 be same as a_2 ?

Checking Primality and Sieve of Eratosthenes

```
prime(n) :
  if n < 2 :
    return false
  loop x=2 upto x=n-1 :
    if x divides n :
      return false
  //return outside loop
  return true
```

O(n)

```
prime(n) :
 if n < 2 :
  return false
loop x=2, x*x<=n, x++ :
   if x divides n:
      return false;
//outside loop
return true
```



```
int n;
vector<char> is_prime(n+1, true);
is_prime[0] = is_prime[1] = false;
for (int i = 2; i * i <= n; i++) {
    if (is_prime[i]) {
        for (int j = i * i; j <= n; j += i)
            is_prime[j] = false;
    }
}
```

3. Best time complexity that I know, to check if a number is prime is -

A. O(n^2)
B. O(n)
C. $O(\log_2 n)$
D. $O(\sqrt{n})$

3. Best time complexity that I know, to check if a number is prime is -

A. O(n^2)
B. O(n)
C. $O(\log_2 n)$
D. $O(\sqrt{n})$ ✓

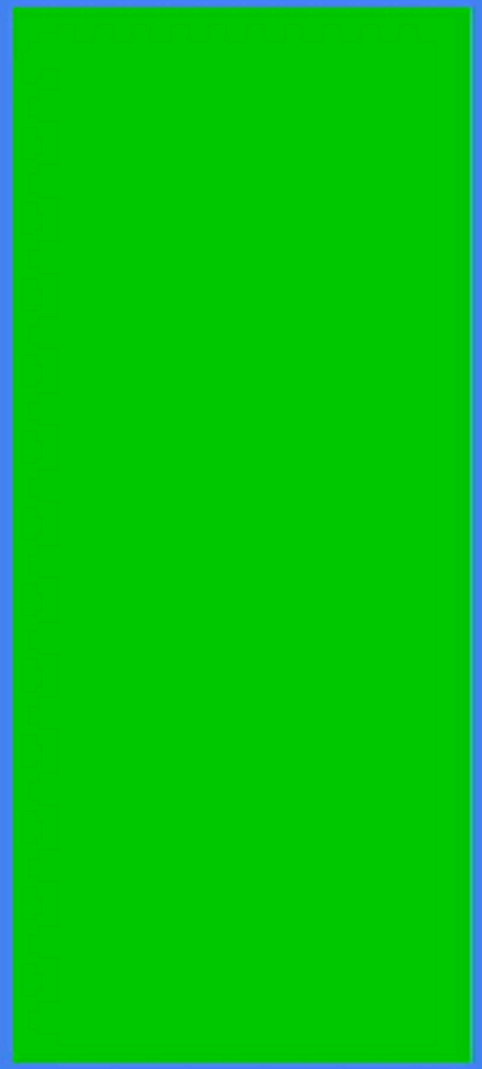
4. Best way to generate list of first 10,000 primes is

A. Using the Sieve of Eratosthenes
B. Using O(N) Primality check
C. Using O(√N) Primality check

4. Best way to generate list of first 10,000 primes is

A. Using the Sieve of Eratosthenes
B. Using O(N) Primality check
C. Using O(√N) Primality check

GCD and LCM



```
gcd(a, b) :
    if b == 0 : return a
    else return gcd(b, a%b)
```

```
int gcd(int a, int b, int& x, int& y) {
    if (b == 0) {
        x = 1;
        y = 0;
        return a;
    }
    int x1, y1;
    int d = gcd(b, a % b, x1, y1);
    x = y1;
    y = x1 - y1 * (a / b);
    return d;
}
```

5. What is the value of y in the following equation?

$$\gcd(a \cdot x, b \cdot x) = y \cdot \gcd(a, b)$$

A. x
B. x*x
C. a*b*x
D. x/(a*b)

5. What is the value of y in the following equation?

$$\gcd(a \cdot x, b \cdot x) = y \cdot \gcd(a, b)$$

A. x
B. x*x
C. a*b*x
D. x/(a*b)

6. What is the output, if GCD(A,B) = 1.

```
bool *marked = new bool[B+1];
memset(marked,0,B);
for(int i=A; i<B+1; i+=A){
        marked[i] = true;
}
cout<<marked[B]<<endl;
```

A. 0
B. 1
C. Can't Determine

6. What is the output, if GCD(A,B) = 1.

```
bool *marked = new bool[B+1];
memset(marked,0,B);
for(int i=A; i<B+1; i+=A){
        marked[i] = true;
}
cout<<marked[B]<<endl;
```

A. 0 ✓

B. 1

C. Can't Determine

Euclid’s Algorithms

7. Using Euclid's Algorithm we can check if two numbers are Coprime.

A. True
B. False

7. Using Euclid's Algorithm we can check if two numbers are Coprime.

A. True
B. False

Bonus : What is GCD(A,B) if A and B are coprime?

8. Time complexity for finding the GCD of an array of integers is

A. $O(N^2)$
B. $O(N \log_2 M)$, where M is maximum value of array
C. $O(N \log_2 N)$
D. $O(N)$

8. Time complexity for finding the GCD of an array of integers is

A. $O(N^2)$

B. $O(N \log_2 M)$, where M is maximum value of array

C. $O(N \log_2 N)$

D. $O(N)$