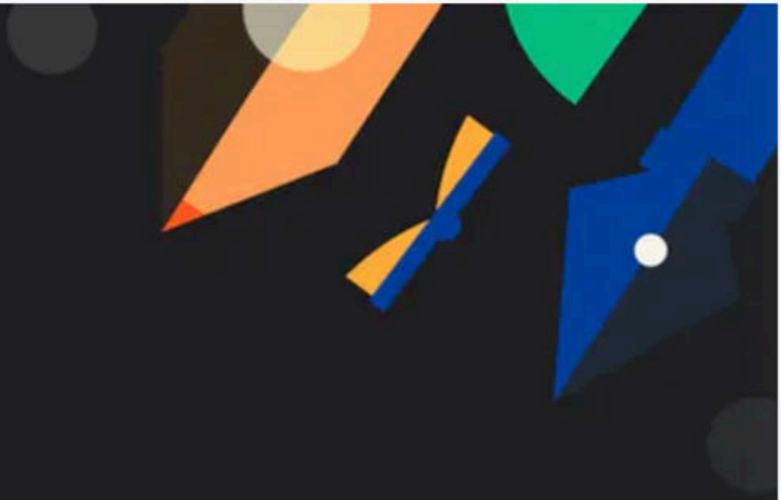


Modular Arithmetic and Exponentiation

Course on Mathematics & Puzzles for Interview Preparation

Arjun Arul • Lesson 2 • Feb 11, 2021

Maths and Puzzles

Lecture 1

CONCEPT -
Prime Numbers and Prime Factorisation

Prime Factorisation

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

Results from Prime Factorisation of a number

$$\tau(n) = \prod_{i=1}^{k} (a_i + 1)$$

Number of Prime Factors

$$\sigma(n) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{a_i})$$

Sum of Prime Factors

$$\mu(n) = n^{\tau(n)/2}$$

Product of Prime Factors

QUIZ -
Prime Numbers and Prime Factorisation

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.

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

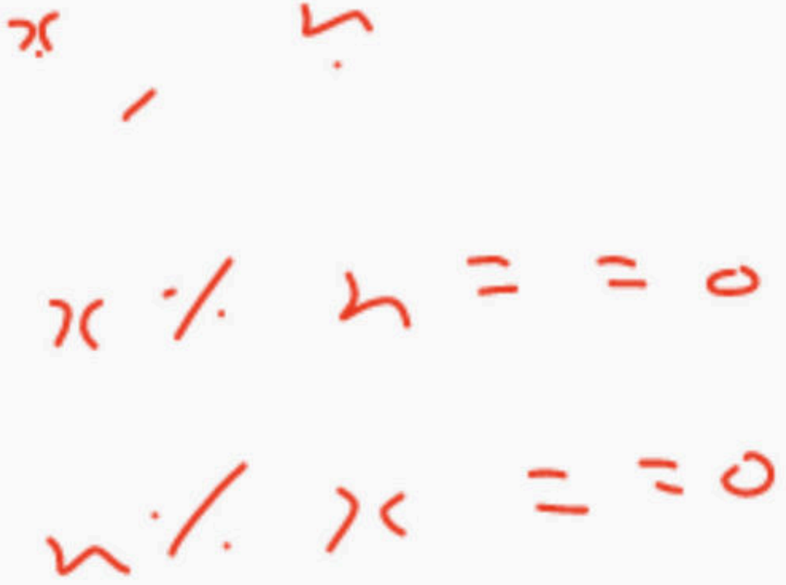
A. True
B. False

Bonus: Can a_1 be same as a_2 ?

CONCEPT -
Checking Primality and Sieve of Eratosthenes

Naive Primality Test

```
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
```

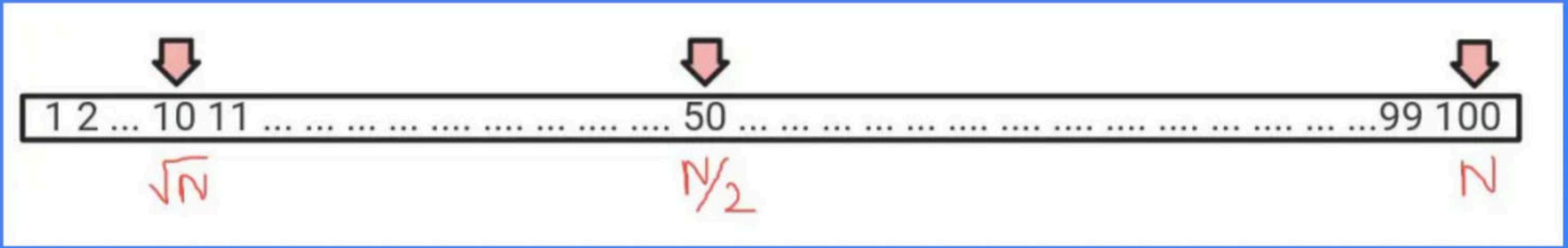


Sqrt(N) Primality test

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

$O(\sqrt{n})$

Sqrt(N) is a big improvement!



Find all primes from 1 to N

N = 10

↳ 2, 3, 5, 7

Sieve of Eratosthenes

O(n) space.

$\geq \leq O(n \log n)$

$\geq = \Theta(n \log \log n)$

```
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;
    }
}
```

$i \leq \sqrt{n}$

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

19

$\lambda \rightarrow 2\lambda, 3\lambda, 4\lambda \ldots$

2

19 x 19

$2, \ldots (\lambda - 1)$

$n = 1024 = 2^{10}$

$\log_2(n) = 10$

$\lg^2(n) = 100$

$\log \log n = \lg_2(10) = 3.2$

Filling the sieve

$2 \to \frac{n}{2}$

$3 \to \frac{n}{3}$

$4 \to \frac{n}{4}$

$5 \to \frac{n}{5}$

$6 \to \frac{n}{6}$

$$\frac{n}{2} + \frac{n}{3} + \frac{n}{4} \cdots + \frac{n}{n}$$

$$\leq \log n$$

$$\textcircled{n}\left[\frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots + \frac{1}{n}\right]$$

$n \log n$

Harmonic Series

$n = 2^3$ $\frac{1}{2}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{4}$

$\frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}$

$1 + 1 = 2$

$\leq \log n$

$\frac{1}{3} < \frac{1}{2}$

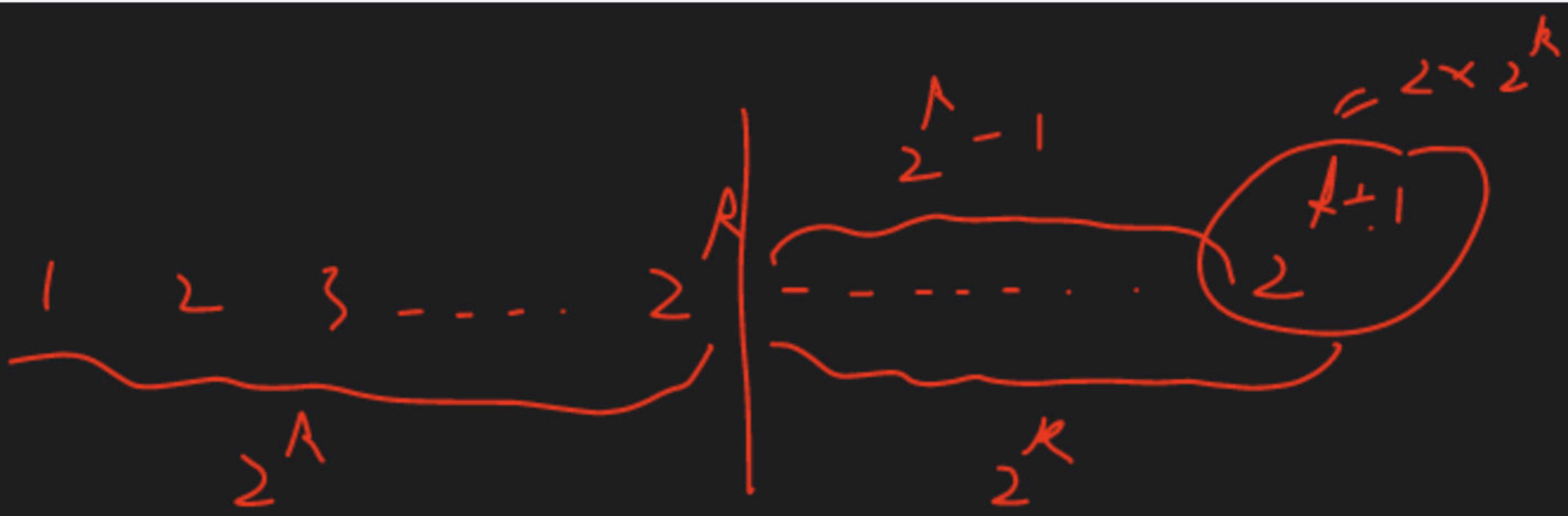
$\frac{1}{a} < \frac{1}{2}$ 이면 $a > 2$

$$n = 2^h - 1$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots \frac{1}{n} \qquad \frac{1}{n+1} \qquad \frac{1}{2^{h-1}}$$

$$\frac{1}{2^k} \quad \frac{1}{2^k} \quad \frac{1}{2^k} \qquad \frac{1}{2^R} = \frac{1}{2 \times 2^R}$$

$$\frac{1}{2^R} \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \frac{1}{2^{L+1}}$$



$$\frac{R}{2^A} \leq \frac{R}{2^k} + \frac{1}{2^k} = \boxed{1}$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{11} + \frac{1}{7} + \frac{1}{6} + \frac{1}{5}$$

$$\leq \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{11} + \frac{1}{4} + \frac{1}{11} + \frac{1}{4}\right)$$

$$= 2 \sim \log(7) + 1$$

$$\frac{d}{dx}(\lg x) = \frac{1}{x}$$

$$\int \frac{1}{x}\,dx = \lg x$$

If $a \mid b$, then every multiple of b is also a multiple of a.

$3 \mid 12$

$12 \times n = 3 \times (4n)$

QUIZ -
Checking Primality and Sieve of Eratosthenes

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. $O(\sqrt{n})$ ✓

Sieve

Sieve → n log n

primality → $\sqrt{n}$

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

$n = 10000$

$\frac{n}{\ln n}$ = # primes.

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

A. Using the Sieve of Eratosthenes ✓
B. Using O(N) Primality check on each number
C. Using O(√N) Primality check on each number
D. Randomly generating a list

$n = n \ln n$

$= n \ln n$.

CONCEPT -
GCD and LCM

GCD / HCF

Greatest Common Divisor

gcd(a, b) =

gcd(12, 21) = 3

12 → 1, 2, 3, 4, 6, 12

21 → 1, 3, 7, 21

$gcd(a, b)$

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

$b \longrightarrow q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$

$gcd(a, b) = 7 \times 19 \times 11$

g

$p_1 \; q_1 \; \ldots$

$p_2 = q_4 \Rightarrow$

$p_5 = q_3 \Rightarrow 19$

$p_1 = 11$

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

$$\Rightarrow r = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot 7^{\frac{4}{2}} \cdots q_k^{\beta_k}$$

$$c = \sqrt{7^4}$$

$$\delta =$$

$$a = 2^{10} \times 5^{3} \times 11^{1} \times 19^{3}$$

$$b = 2^{4} \times 3^{6} \times 7^{2} \times 11^{10} \times 13 \times 19$$

$$\gcd(a, b) = 2^{4} \times 11^{1} \times 19^{1}$$

$$= 2^{4} \times 11 \times 19$$

$$\text{lcm} = 2^{10} \times 3^{6} \times 5^{3} \times 7^{2} \times 11^{10} \times 13 \times 19^{3}$$

$$gcd(a,b) \times lcm(a,b) = a \times b$$

$\min(\alpha, \beta)$

$2^{\min(\alpha,\beta)}$

11^{1}

$\alpha + \beta$

$2^{\alpha+\beta}$

$\max(\alpha, \beta)$

2

11^{10}

$11^{\alpha+\beta}$

2

$11^{1} \times 11^{10}$

$$\gcd(a, b, c)$$

$$g$$

$$\gcd(12, 18, 42) = 6$$

LCM

a, 2a, 3a

lcm(a, b) ≤ ab

a × b

2a, 3a, 4a, ... ∞

2b, 3b, 4b ... 10b.

$$1 \leq \gcd(a,b) \leq \min(a,b) \leq$$

$$\max(a,b) \leq \operatorname{lcm}(a,b) \leq ab$$

$$g \leq b$$

$$\gcd(a,a) = a$$

$$\operatorname{lcm}(a,a) = a$$

$\alpha \to 7^{6}$ $\quad \mapsto 7^{11}$

$\ell(m$

$\alpha_1 \quad \alpha_2 \quad \alpha_3 \quad \alpha_k$

$a = p_1 \; p_2 \; p_3 \cdots p_k$

β_3

$\beta_1 \quad \beta_2 \quad \beta_s \quad \beta_t$

$\mu = q_1 \; q_2 \cdots q_s \cdots q_t$

$\min(\alpha_2, \beta_5)$

α_i

$\ell(m(a,\mu)) = p_1^{11} \; p_2 \; 7^{11} \; 7$

Properties of GCD and LCM

$$a * b = \gcd(a, b) * lcm(a, b)$$

$$\gcd(a_1, a_2, \cdots, a_n) = \gcd(a_1, \gcd(a_2, a_3, \cdots, a_n))$$

$$lcm(a_1, a_2, \cdots, a_n) = lcm(a_1, lcm(a_2, a_3, \cdots, a_n))$$

$$\gcd(m \cdot a, m \cdot b) = m \cdot \gcd(a, b)$$

$$\gcd(a + m \cdot b, b) = \gcd(a, b)$$

$$\gcd(a/m, b/m) = \gcd(a, b)/m$$

QUIZ -
GCD and LCM

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

9, 4

gcd(9, 4)

CONCEPT -

Euclid's Algorithms

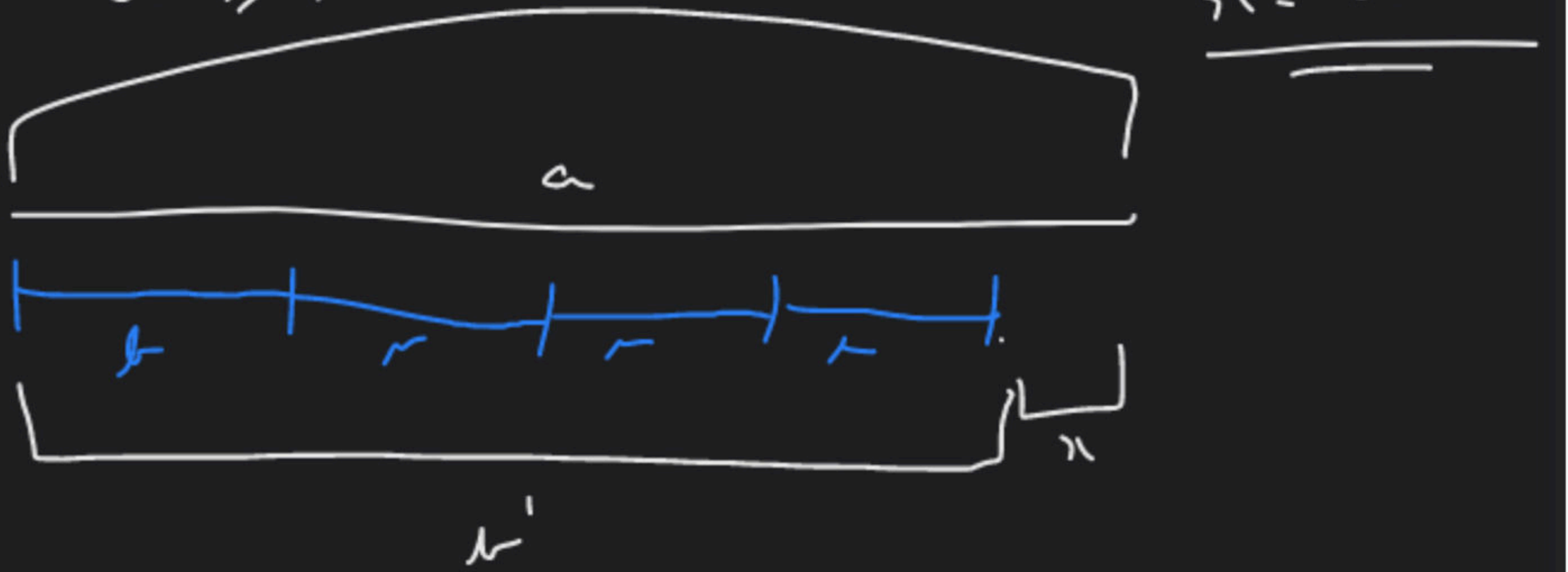
$gcd(a, b) = g$

$x = a - b$

$b' = 4b$

$a \geq b$

$r = a \% b$



$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$x \mid a$ & $x \mid b \Rightarrow x \mid a+b$

$a = x a'$ $\quad b = x b' \Rightarrow x \mid a-b$

$a \mp b = x a' \mp x b'$

$= x(a' \mp b')$

Recurrence Relation

$$\gcd(a,b) = \begin{cases} a & b = 0 \\ \gcd(b, a \mod b) & b \neq 0 \end{cases}$$

Visualizing Euclid's Algorithm

Finding GCD and LCM by Euclid's Algorithm

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

```
lcm(a, b) :
   return a / gcd(a, b) * b
```

Extended Euclid's Algorithm

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

```
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;
}
```

QUIZ -
Euclid’s Algorithms

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

A. True
B. False

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. $O(N)$