SCALER

Modular Arithmetic & GCD

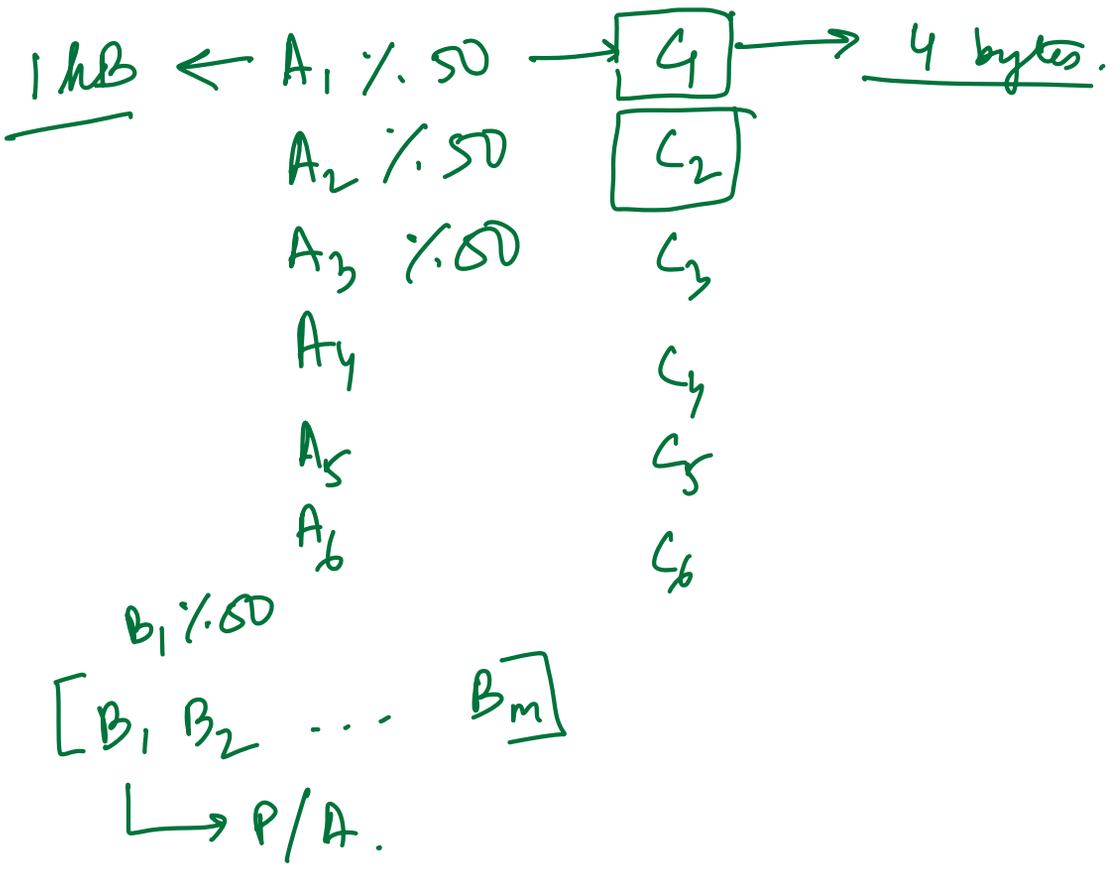
TABLE OF CONTENTS

Modulo (%)

A % B ⟶ Remainder when A is divided by B

Range of A % m ⟶ $[0, m-1]$

Why do we need % ⟶ Mostly to limit the range of data.



Modular Arithmetic

1. $(a + b)\%m = (a\%m + b\%m)\%m$

$(11 + 7)\%5 = 3$

$(11\%5 + 7\%5)\%5 = (1 + 2)\%5 = 3$

$a = 9$
$b = 8$
$m = 5$

$(9 + 8)\%5 \rightarrow 2$

$9\%5 \quad 8\%5$

$4 + 3 = 7 \xrightarrow{\%5} 2$

2 $(a * b) \% m = (a \% m * b \% m) \% m$

3 $(a + m) \% m$

$= (a \% m + m \% m) \% m$

$= (a \% m + 0) \% m$

$= (a \% m) \% m$ → no impact

$[0, m-1]$

$= (a \% m)$

4 $(a - b) \% m = (a \% m - b \% m + m) \% m$

$a = 7, b = 3, m = 5$

$(7 - 3) \% 5 = 4$

$(7 \% 5 - 3 \% 5) \% 5 = (2 - 3) \% 5$

$= (-1) \% 5$

$= (-1 + 5) \% 5 = 4$

5 $a^b \% m = (a \% m)^b \% m$ → $b \% \phi(m)$ Euler Totient fn.

$= (\underbrace{a * a * a * a * \dots * a}_{b \text{ times}}) \% m$

$= (\underbrace{(a \% m) * (a \% m) * (a \% m) \dots * (a \% m)}_{b})$

$5^3 \% 3 = (5 \% 3)^3 \% 3$

$= 2^3 \% 3 = 8 \% 3 = 2$

QUIZ

$(37^{103} - 1) \% 12$

$= ((37 \% 12)^{103} - 1) \% 12$

$= (1^{103} - 1) \% 12$

$= 0$

$b \% m$ → -ve

$(\underbrace{(b \% m)}_{[-m+1, 0]} + m) \% m$ → $[0, m-1]$

Fast - power

$(a^b \% m)$

Code

```
fn fast_pow(a, b, m) {
    if (b == 0)
        return 1
    half_pow = fast_pow(a, b/2, m) % m
    if (b % 2 == 0)
        return (half_pow * half_pow) % m
    return ((half_pow * half_pow) % m * (a % m)) % m
}
```

O(log b) T.C.

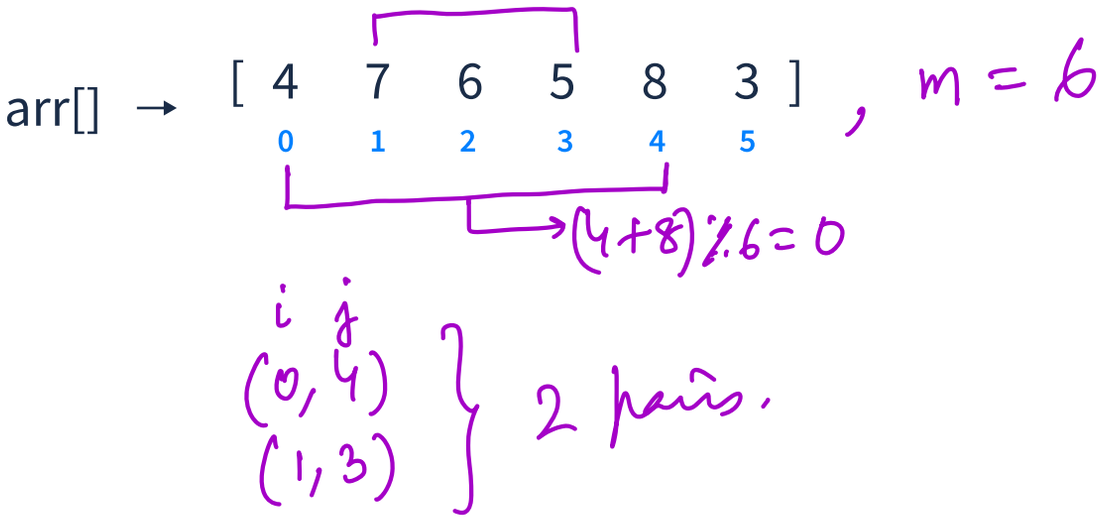
O(log b) S.C

Question

Given N array elements. Find the count of pairs (i, j) such that (arr [i] + arr [j]) % m = 0.

$(1 \le N \le 10^5)$

Note : i! = j and pair (i, j) is same as pair (j, i)



Idea 1

Nested loop

i → [0, n-1]

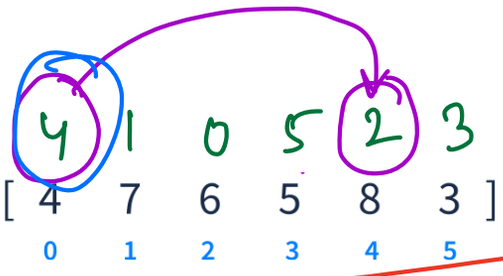
j → [i+1, n-1]

check (arr[i] + arr[j])% m == 0

O(n²) T.C

✦ Idea 2

arr[] →



$[0, m-1]$

$(a+b)\%m = ((a\%m) + (b\%m))\%m = 0$

→ multiple of m.

a%m	b%m
1	5
2	4
3	3
4	2
5	1
0	0

$a \longleftrightarrow b$

$b\%m = (m - a\%m)\%m$

Example :

M = 6

arr[] → [2 3 4 8 6 15 5 12 17 7 18 10 9 16 21]

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14

i	arr[i]%m	Partner h	f[h]	count
0	2	4	0	0
1	3	3	0	0
2	4	2	1	1
3	2	4	1	2
4	0	0	0	2
5	3	3	1	3

f[ ]

0 1 2 3 4 5

0 0 0 0 0 0

0 0 1 0 0 0

0 0 1 1 0 0

0 0 1 1 1 0

0 0 2 1 1 0

1 0 2 1 1 0

1 0 2 2 1 0

0 2 1 1 0

0 2 1 1 0

0 2 1 1 0

0 2 1 1 0

0 2 1 1 0

0 2 1 1 0

Code

```
fn PairSumDivM(A, m)
    n = len(A)
    freq[m] = {0}
    cnt = 0
    for(i → 0 to n-1){
        r = A[i] % m
        h = (m-r) % m
        cnt += freq[h]
        freq[r]++
    }
    ret cnt
}
```

O(n) T.C.
O(m) S.C.

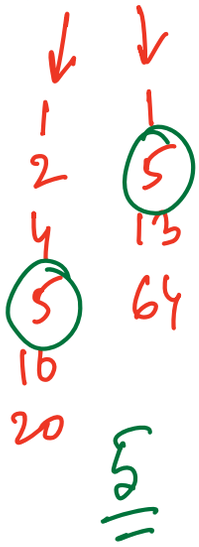
If m is large, replace freq. array by HashMap → <K, V>

rem freq.

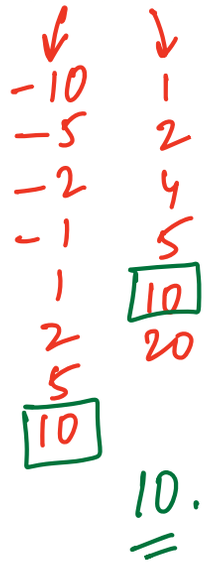
GCD → Greatest Common Divisor / Highest Common Factor

GCD (a, b) → Greatest factor that divides both a and b.

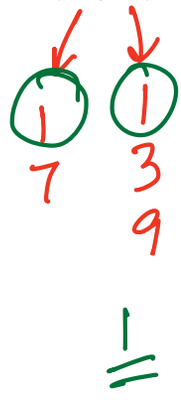
GCD (20, 65)



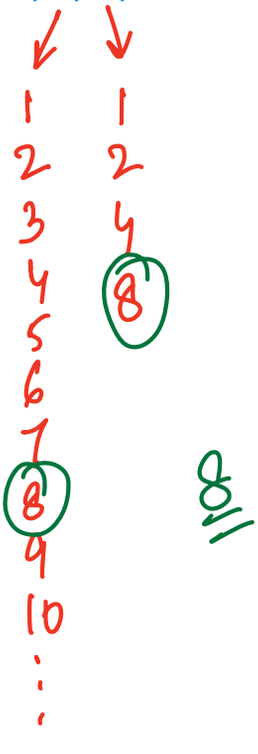
GCD (-10, 20)



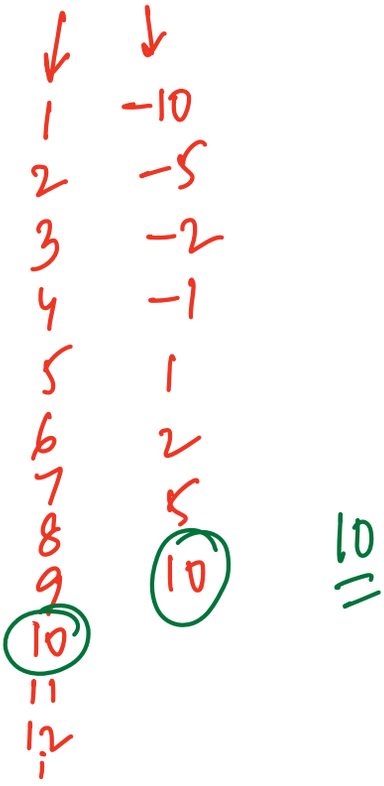
GCD (7, 9)



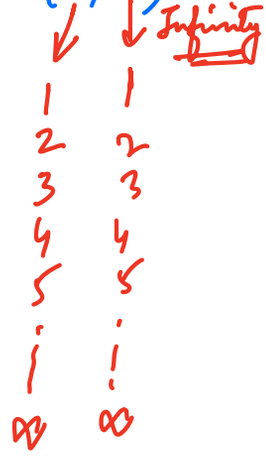
GCD (0, 8)



GCD (0, -10)



GCD (0, 0)



Properties of GCD →

1) $GCD(A,B) = GCD(B,A)$

2) $GCD(0,A) = A$

3) $GCD(A,B,C) = GCD(GCD(A,B), C)$
$= GCD(GCD(B,C), A)$
$= GCD(GCD(A,C), B)$

4) $A >= B > 0$
$GCD(A,B) = GCD(A-B, B)$

5) $GCD(A,B) = GCD(A \% B, B)$

[Break till 10:51 PM]

$GCD(15, 21, 33, 45)$

3 3

3

$GCD(A,B) = GCD(A\%B, B)$

$GCD(30,12) = GCD(6,12) = GCD(\underbrace{6\%12}_{6}, 12)$

Infinite steps.

$$GCD(A,B) = GCD(B, A\%B)$$

$A\%B < B$.

$GCD(14,21) = GCD(21,14)$
$= GCD(14,7)$
$= GCD(7,0)$
$= 7.$

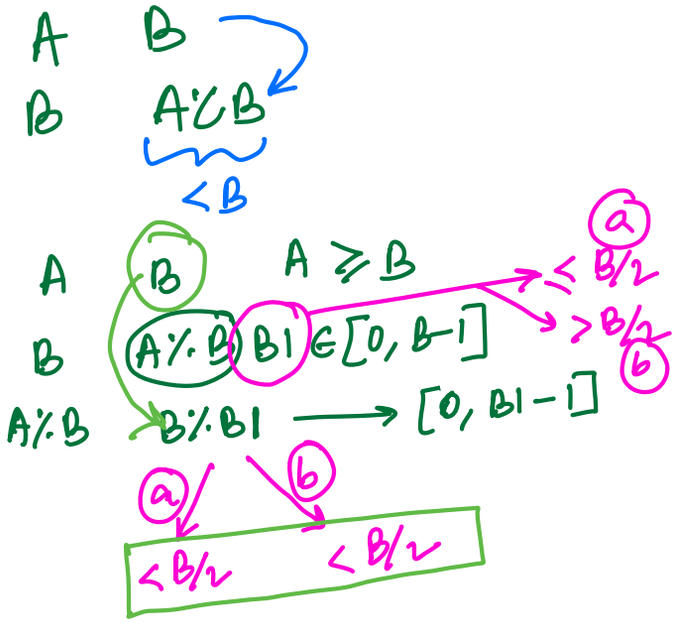
$GCD(30,12) = GCD(12,6)$
$= GCD(6,0)$
$= 6.$

$B1 > B/2$

$B\%B1 = B - B1$

$< B/2$

$O(\log(\min(a,b)))$



GCD Function

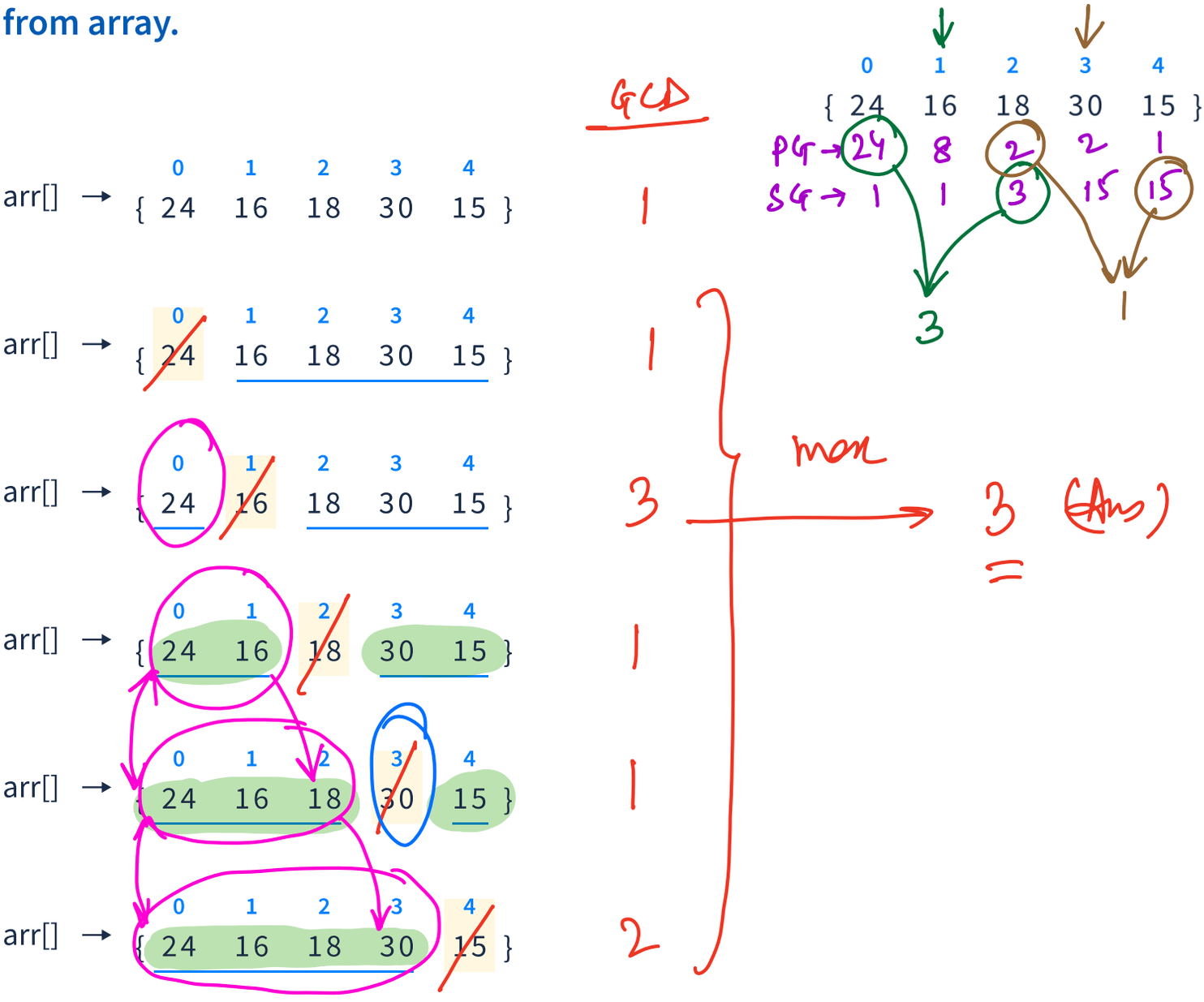
```
int gcd( int a, int b){
    if (b==0)
        return a

    return gcd(b, a%b)

}
```

T.C. → $O(\log(\min(a,b)))$

Delete One

Question

Given arr[N]. Find maximum GCD value after deleting one of the elements from array.



Brute force

Nested loop $i \rightarrow [0 \text{ to } n-1]$

$j \rightarrow [0 \text{ to } n-1]$ except i → take GCD of all

$O(n^2 * \max(a_n))$

2nd approach GCD(0...i)

PrefixGCD[i] = GCD(PrefixGCD[i-1], a[i])

SuffixGCD[i] = GCD(SuffixGCD[i+1], a[i])

$i \rightarrow$ GCD(PrefixGCD[i-1], SuffixGCD[i+1])

Pseudo-Code

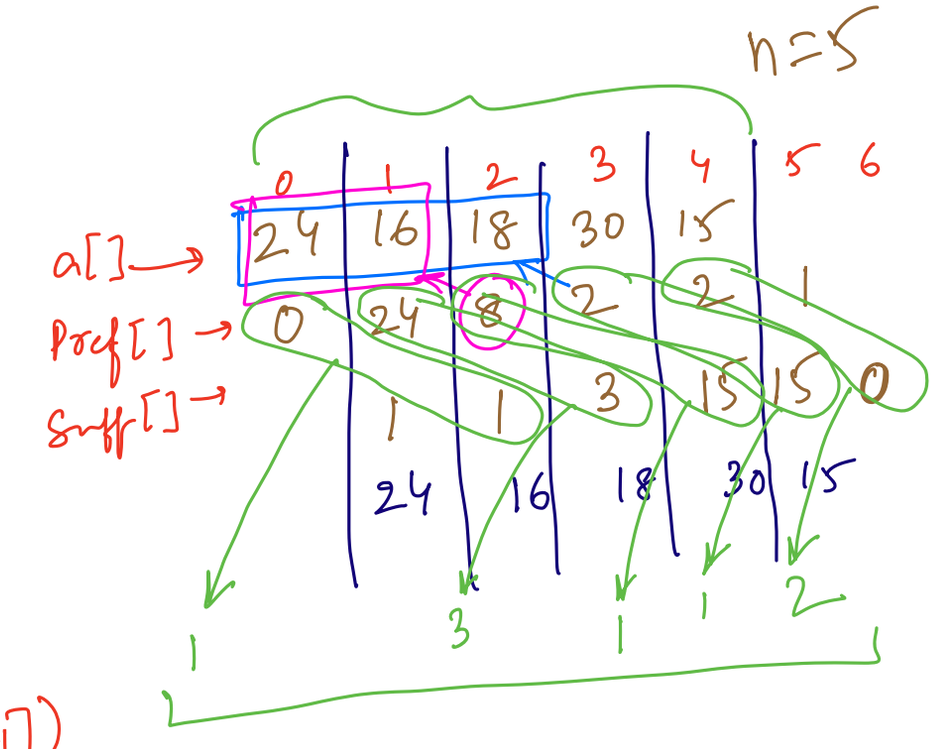
```
fn gcd(a, b){
    if(b==0)
        return a
    return gcd(b, a%b)
}
fn maxGCD(a[], n){
    Pref[n+2]
    Suff[n+2]
}  1-indexed.
    fn(i→0 to n-1){
        Pref[i+1] = gcd(Pref[i], a[i])
    }
    fn(i→n-1 to 0){
        Suff[i+1] = gcd(Suff[i+2], a[i])
    }
    ans = 0
    fn(i→0 to n-1){
        ans = max(ans, gcd(pref[i], suff[i+2]))
    }
    return ans
}
```

$O(n * \log(\max(a_i)))$

T.C.

Pref[i] → gcd(a[0]...a[i-1])

Suff[i] → gcd(a[i+1]...a[n-1])



$3^{-1} \% 5 \longrightarrow 2$

$((3^{-1} \% 5) * (3 \% 5)) \% 5 = (3^{-1} * 3) \% 5$

$= 1$

($3^{-1} \% 5 = 2$, $3 \% 5 = 3$, $2 = k$)

$(k * 3) \% 5 = 1$

k: $[0, 4]$ $\longrightarrow 2$

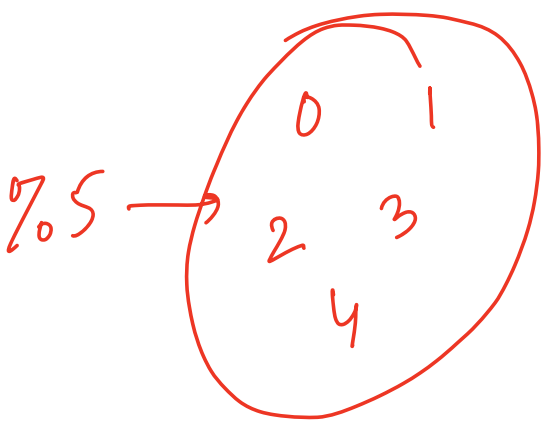
$3^{-3} \% 5$

$= (3^{-1})^3 \% 5$

$= (3^{-1} \% 5)^3 \% 5$

$= 8 \% 5 = 3$

$3^{-1} = 1/3$



$\frac{a}{b} \% m$

$= a * b^{-1} \bmod m$

$b^{\phi(m)} \equiv 1 \pmod{m} \Rightarrow b^{\phi(m)} \% m = 1$

If m is prime, $b < m$,

$$b^{m-1} \% m = 1$$

$$2^{7-1} \% 7 = 64 \% 7 = 1$$

$$3^{7-1} \% 7 = 729 \% 7 = 1$$

$$b^{m-1} \% m = 1$$

$$(b^{-1} * (b^{m-1} \% m)) \% m = (1 * b^{-1}) \% m$$

$$\Rightarrow b^{m-2} \% m = b^{-1} \% m$$

$$\Rightarrow \boxed{b^{-1} \% m = b^{m-2} \% m}$$ → m is prime. $b < m$.

$$3^{5-2} \% 5$$

$$= 3^3 \% 5 = 2$$