

Modular Arithmetic & GCD

TABLE OF CONTENTS

- 1. Modular arithmetic introduction
- 2. Count pairs whose sum mod m is 0
- 3. Introduction to GCD / HCF
- 4. Properties of GCD
- 5. Delete one



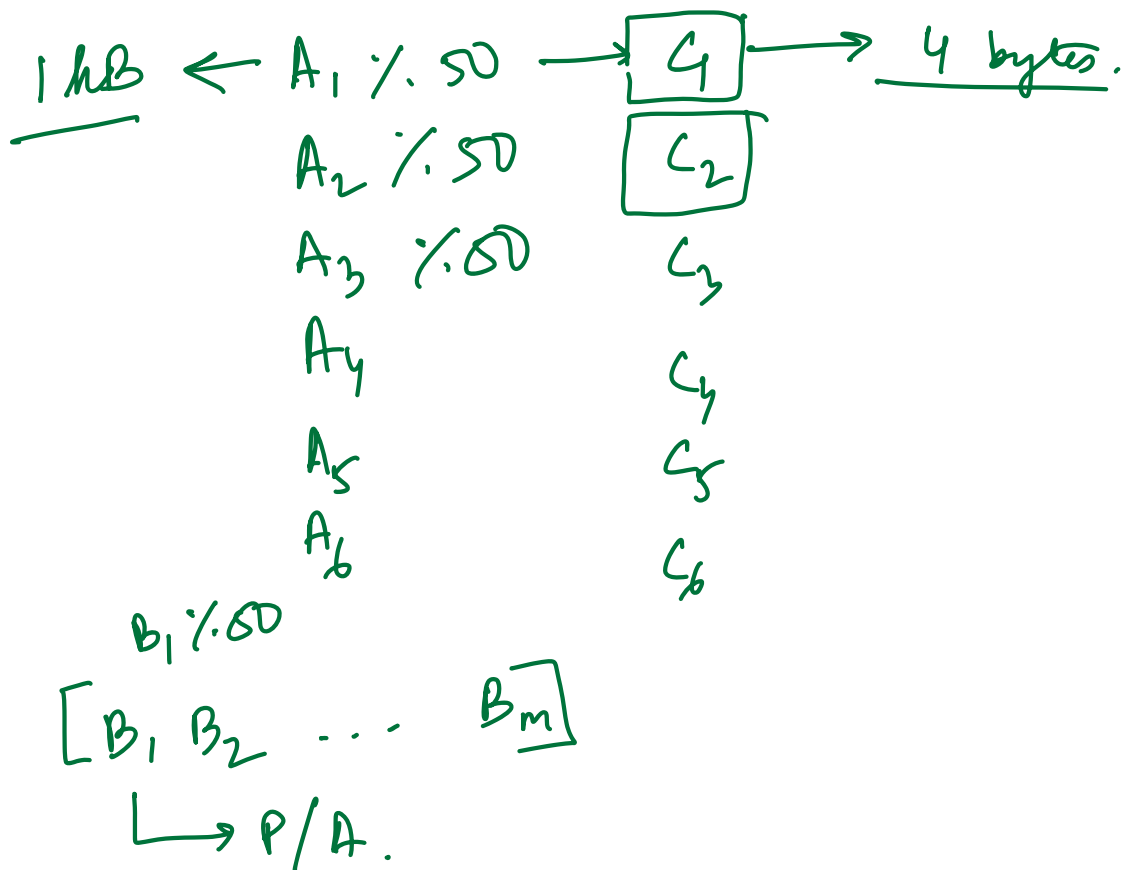


Modulo (%)

$A \% B \rightarrow$ Remainder when A is divided by B

Range of $A \% m \rightarrow [0, m-1]$

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





Modular Arithmetic

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

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

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

$$\begin{aligned} a &= 9 \\ b &= 8 \\ m &= 5 \end{aligned}$$

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

$$\begin{array}{cc} \%5 \downarrow & \%5 \downarrow \\ 4 + 3 = 7 & \xrightarrow{\%5} 2 \end{array}$$



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

$$3 \quad (a + m) \% m$$

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

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

$$= (a \% m) \% m \rightarrow \text{no impact}$$

$$\underbrace{\hspace{1cm}}_{[0, m-1]}$$

$$= (a \% m)$$

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

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

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

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

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

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



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

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

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

$$\begin{aligned} 5^3 \% 3 &= (5 \% 3)^3 \% 3 \\ &= 2^3 \% 3 = 8 \% 3 = 2 \end{aligned}$$

QUIZ

$$\begin{aligned} &(37^{103} - 1) \% 12 \\ &= ((37 \% 12)^{103} - 1) \% 12 \\ &= (1^{103} - 1) \% 12 \\ &= 0 \end{aligned}$$

$b \% m$
↓
-ve

$$\begin{aligned} &\underbrace{((b \% m) + m)}_{[-m+1, 0]} \% m \\ &\quad \downarrow \\ &[0, m-1] \end{aligned}$$



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

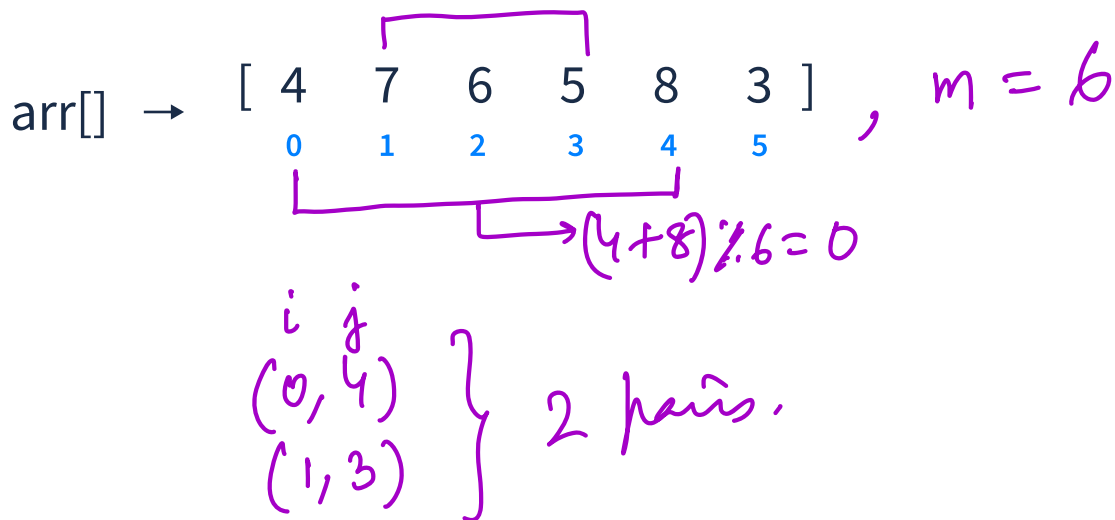


Question

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

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

Note : $i \neq j$ and pair (i, j) is same as pair (j, i)



★ Idea 1

Nested loop

$i \rightarrow [0, n-1]$

$j \rightarrow [i+1, n-1]$

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

$O(n^2)$ T.C

arr[] →

✦ Idea 2

Diagram illustrating the insertion of element 2 into the sorted subarray [4, 7, 6, 5, 8, 3]. The array is shown with indices 0 to 5. The element 2 is being inserted at index 4, shifting the element 8 to index 5. The sorted subarray [4, 7, 6, 5] is highlighted in green, and the element 2 is highlighted in purple.

 $[0, m-1]$

$$(a+b) \% m = (\underbrace{(a \% m) + (b \% m)}_{\text{multiple of } m}) \% m = 0$$

<u>a/m</u>	<u>b/m</u>
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 ]
```

[illegible]

`</>` 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
Hash Map $\rightarrow \langle k, v \rangle$
 $\swarrow \quad \searrow$
 rem freq.



GCD → Greatest Common Divisor / Highest Common Factor

$GCD(a, b) \rightarrow$ greatest factor that divides both a and b .

GCD (20, 65)

↓ ↓
1 1
2 5
4 13
5 64
10 64
20 64
5

GCD (-10, 20)

↓ ↓
-10 1
-5 2
-2 4
-1 5
1 10
2 20
5 20
10 20
10

GCD (7, 9)

↓ ↓
1 1
7 3
9 9
1

GCD (0, 8)

↓ ↓
1 1
2 2
3 4
4 8
5 8
6 8
7 8
8 8
9 8
10 8
⋮
8

GCD (0, -10)

↓ ↓
1 -10
2 -5
3 -2
4 -1
5 1
6 2
7 5
8 10
9 10
10 10
11 10
12 10
10

GCD(0,0)

↓ ↓
1 1
2 2
3 3
4 4
5 5
⋮ ⋮
∞ ∞
Infinity



Properties of GCD →

$$1) \text{GCD}(A, B) = \text{GCD}(B, A)$$

$$2) \text{GCD}(0, A) = A$$

$$\begin{aligned} 3) \text{GCD}(A, B, C) &= \text{GCD}(\text{GCD}(A, B), C) \\ &= \text{GCD}(\text{GCD}(B, C), A) \\ &= \text{GCD}(\text{GCD}(A, C), B) \end{aligned}$$

$$4) A \geq B > 0$$

$$\text{GCD}(A, B) = \text{GCD}(A - B, B)$$

$$5) \text{GCD}(A, B) = \text{GCD}(A \% B, B)$$

[Break till 10:51 PM]

$$\begin{array}{c} \text{GCD}(15, 21, 33, 45) \\ \underbrace{\quad\quad\quad} \quad \underbrace{\quad\quad\quad} \\ 3 \qquad\qquad 3 \\ \underbrace{\quad\quad\quad} \\ 3 \end{array}$$



$$\text{GCD}(A, B) = \text{GCD}(A \% B, B)$$

$$\text{GCD}(30, 12) = \text{GCD}(6, 12) = \text{GCD}(\underbrace{6 \% 12}_6, 12)$$

Infinite steps.

$$\boxed{\text{GCD}(A, B) = \text{GCD}(B, A \% B)}$$

$< B$.

$$\begin{aligned} \text{GCD}(14, 21) &= \text{GCD}(21, 14) \\ &= \text{GCD}(14, 7) \\ &= \text{GCD}(7, 0) \\ &= 7. \end{aligned}$$

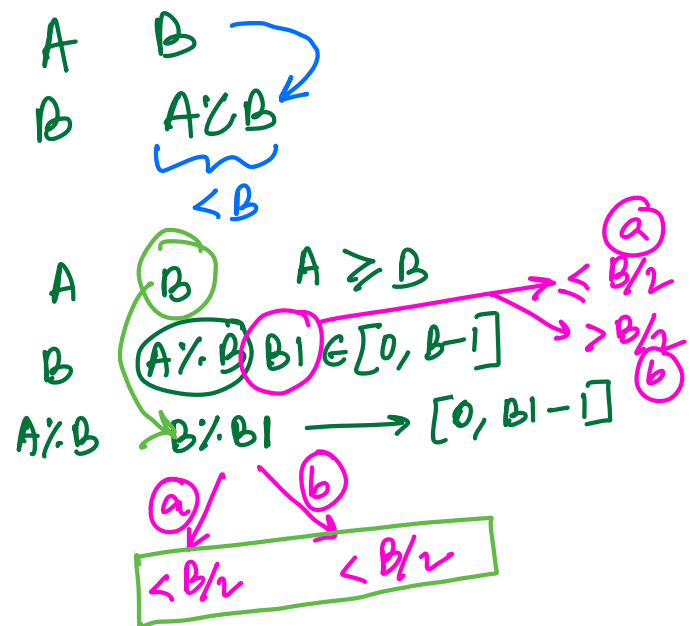
$$\begin{aligned} \text{GCD}(30, 12) &= \text{GCD}(12, 6) \\ &= \text{GCD}(6, 0) \\ &= 6. \end{aligned}$$

$$\begin{aligned} B1 &> B/2 \\ B \% B1 &= B - B1 \\ &< B/2 \end{aligned}$$

$$\boxed{O(\log(\min(a, b)))}$$

GCD Function

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



$$T.C. \rightarrow O(\log(\min(a, b)))$$



Delete One

Question

Given $\text{arr}[N]$. Find maximum GCD value after deleting one of the elements from array.

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

$\text{arr}[] \rightarrow \{ \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{matrix} \}$

GCD

1

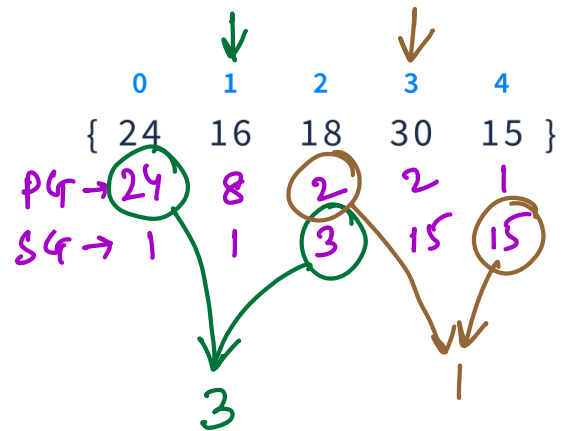
1

3

1

1

2



max

3 (Ans)

Brute force

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

$j \rightarrow [0 \text{ to } n-1] \text{ except } i \rightarrow \text{take GCD of all}$
 $O(n^2 * \text{max}(\text{arr}))$

2nd approach $\text{gcd}(0..i)$

$\text{PrefixGCD}[i] = \text{gcd}(\text{PrefixGCD}[i-1], \text{arr}[i])$

$\text{SuffixGCD}[i] = \text{gcd}(\text{SuffixGCD}[i+1], \text{arr}[i])$

$i \rightarrow \text{gcd}(\text{PrefixGCD}[i-1], \text{SuffixGCD}[i+1])$



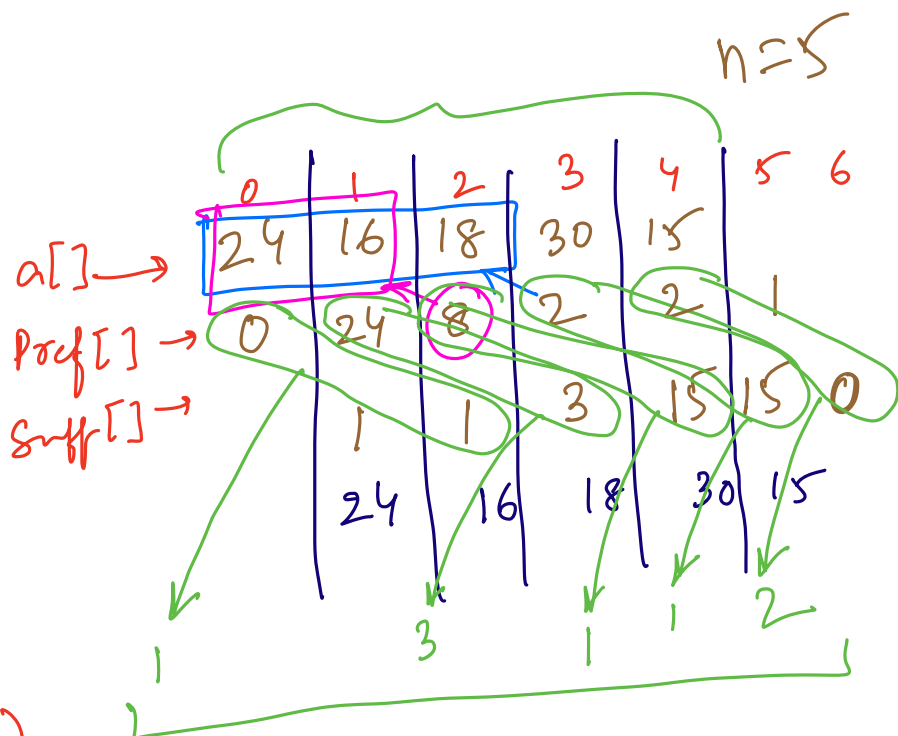
</> Pseudo-Code

```
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.
    for (i → 0 to n-1){
        Pref[i+1] = gcd(Pref[i], a[i])
    }
    for (i → n-1 to 0){
        Suff[i+1] = gcd(Suff[i+2], a[i])
    }
    ans = 0
    for (i → 0 to n-1){
        ans = max(ans, gcd(Pref[i], Suff[i+2]))
    }
    return ans
}
```

$O(n \log(\max(a_i)))$
T.C.

$Pref[i]$
↓
 $gcd(a[0] \dots a[i-1])$
 $Suff[i]$
↓
 $gcd(a[i+1] \dots a[n-1])$



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

$$\underbrace{\left(\underbrace{3^{-1} \% 5}_k \right) * \underbrace{(3 \% 5)}_3}_{2} \% 5 = (3^{-1} * 3) \% 5 = 1$$

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

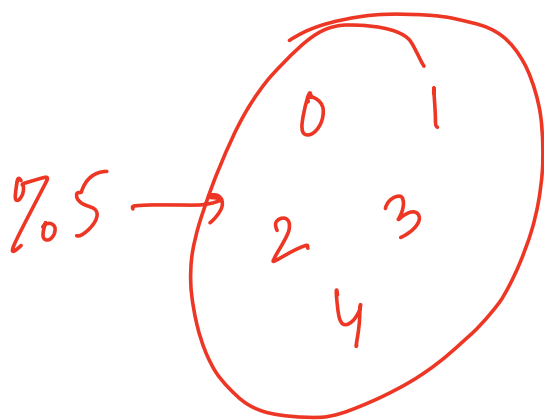
\downarrow
 $[0, 4]$

$\longrightarrow 2$

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

$$\begin{aligned}
 &= (3^{-1})^3 \% 5 \\
 &= (3^{-1} \% 5)^3 \% 5 \\
 &= 8 \% 5 = 3
 \end{aligned}$$

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



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

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

$$b^{\phi(m)} \equiv 1 \text{ modulo } m. \Rightarrow b^{\phi(m)} \% m = 1$$

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.
 $b < m$.

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

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