Modular Arithmetic
& GCD

Content

- Introduction
- Count pairs whose sum % m == 0
- GCD
- Properties
- Delete one { if time permits }.

By monday

66.48 → 66.08 → 75%

personal target ≃ 100%.

Introduction

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

Range of $A \% B$ = $[0, B-1]$

why do we need % ?

Needed to limit the range of our ans.

Rules

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

Eg : $a = 9 \quad b = 8 \quad m = 5$

our data type can hold at max $\underline{\underline{10}}$

$(a+b) \% m$

$(9+8) \% 5$

$\underbrace{(17)}_{\text{overflow}} \% 5 = 2$

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

$(4+3) \% 5 = 7 \% 5 = 2$

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

3) $(a+m) \% m = ((a \% m) + \underbrace{(m \% m)}_{0}) \% m$

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

$= a \% m \rightarrow [0, m-1]$

$(12+5) \% 5 \rightarrow 12 \% 5 = \underline{\underline{2}}$

$= 17 \% 5$

$= \underline{\underline{2}}$

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

Eg : $a = 12 \quad b = 9 \quad m = 5$

$(12-9)\%5 = 3\%5 = 3$

$\Longrightarrow (12\%5 - 9\%5)\%5$

$\Longrightarrow (2-4)\%5$

$$\begin{tikzcd}
 & (-2+5)\%5 = 3 \\
(-2)\%5 \arrow[ur] \arrow[dr] & \\
 & 3
\end{tikzcd}$$

java, c++ js....

python.

$a = 9 \quad b = 12 \quad m = 5$

$(a-b)\%5 = (9-12)\%5 = 2$

$(a\%5 - b\%5 + 5)\%5$

$(4 - 2 + 5)\%5$

$(2+5)\%5 = \underline{\underline{2}}$.

$a = 7 \quad b = 14 \quad m = 5$

$(a-b)\%5$

$(-7)\%5 = 3$

$(a\%5 - b\%5 + 5)\%5$

$= 7\%5 - 14\%5$

$(2 - 4 + 5)\%5 = 3\%5 = \underline{\underline{3}}$

5> $(a^{b})\%m = ((a\%m)^{b})\%m$

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

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

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

$\longrightarrow (1\%12 - 1 + 12)\%12$

$\longrightarrow 12\%12 = 0$

Count of pairs whose sum % m == 0 ***

Given A[], find count of pairs (i, j) such that

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

NOTE : $i \,!= j$ and $(i, j) == (j, i)$

$N <= 10^5$ $0 < A[i] <= 10^9$

	0	1	2	3	4	5
A[] =	4	3	6	3	8	12

m = 6

0, 6, 12, 18, 24 ....

i	j	(A[i] + A[j]) % 6
1	3	3 + 3 = 6 % 6 = 0
0	4	4 + 8 = 12 % 6 = 0
2	5	6 + 12 = 18 % 6 = 0

ans = 3

Brutforce ∀ i, j check $(A[i] + A[j]) \% m == 0$

Optimized approach

$$(A[i] + A[j]) \% m$$

$$\underbrace{(\underset{\downarrow\,[0,\, m-1]}{A[i] \% m} + \underset{\downarrow\,[0,\, m-1]}{A[j] \% m})}_{[0,\, 2m-2]} \% m \longrightarrow 0,\, m$$

multiples of m in range 0 to 2m-2

⟹ step 1 → mod each element.

m = 6

A[] =	2	3	4	8	6	15	5	12	17	7	18
A[i] % 6	2	3	4	2	0	3	5	0	5	1	0

max value of A[i] % 6 + A[j] % 6 = 10

Check if sum of any pair is 0 or m. {0, 6}

Count all pairs with sum 0 or 6.

Freq Araray $\left[\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 1 & 1 & 6 & 5 \end{array}\right]$ N = 6

1 : 3 2 : 1 6 : 1 5 : 1

Create an array of 3 max(A) + 1

$$\text{freq}[7] = \left[\begin{array}{ccccccc} 0 & \overset{\cancel{2}\,\cancel{1}}{\cancel{0}} & \overset{1}{\cancel{0}} & 0 & 0 & \overset{1}{\cancel{0}} & \overset{1}{\cancel{0}} \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}\right]$$

```
for i ⟶ 0 to N-1 {
    freq[A[i]] += 1
}
```

$$\text{freq} = \left[\begin{array}{ccccccc} 0 & 3 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}\right]$$

HW.

learn basics of hashmap

dictionary

$A_i + A_j == 0$ or 6

$A_i + A_j == 0$

Both $A_i == A_j == 0$

$A_i + A_j == 6$

$A_j = 6 - A_i$

A[] =	2	3	4	8	6	15	5	12	17	7	18
A[i] % 6	2	3	4	2	0	3	5	0	5	1	0

Remainder	Pair	count	freq
2	6−2 = 4	0	2:1
3	6−3 = 3	0	2:1, 3:1
4	6−4 = 2	1	2:1, 3:1, 4:1
2	6−2 = 4	2	2:2, 3:1, 4:1
0	0	2	0:1, 2:2, 3:1, 4:1
3	6−3 = 3	3	0:1, 2:2, 3:2, 4:1
5	6−5 = 1	3	0:1 2:2 3:2 4:1 5:1
0	0	4	0:2 2:2 3:2 4:1 5:1
5	6−5 = 1	4	0:2 2:2 3:2 4:1 5:2
1	6−1 = 5	6	0:2 2:2 3:2 4:1 5:2 1:1
0	0	8	0:3 2:2 3:2 4:1 5:2 1:1

Pseudocode

```
count = 0                                        O(M)
freq  = create an array of size m with all 0s

for i → 0 to N-1 {                 O(N)
    val = A[i] % m

    if (val == 0) {
        pair = 0
    } else {
        pair = m - val
    }
    count += freq[pair]
    freq[val] += 1
}

print (count)
```

TC : O(N + M)

SC : O(M)

initialising freq[i] = 0
for i → 0 to M-1

Break : 22 : 40

GCD Basics

→ Greatest Common Divisor

HCF { Highest Common Factor }

gcd (15 , 25) = 5

25 → 1 5 25

15 → 1 3 5 15

gcd (12 , 30)

30 → 1 2 3 5 6 10 15 30

12 → 1 2 3 4 6 12

gcd (0 , 4)

4 → 1 2 4

0 → 1 2 3 4 5 ....

All positive no. are factor for 0

$0 \% x = 0$

gcd (0,0) = ∞ // undefined

```
gcd = 1
for i → 2 to min (a, b) {
    if (a % i == 0 && b % i == 0) {
        gcd = i
    }
}
print (gcd) .
```

TC : O(min (a, b))

Properties of GCD

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

2) $\gcd(0, a) = a \qquad a > 0$

3) $$\left.\begin{aligned} \gcd(a, b, c) &= \gcd(\gcd(a, b), c) \\ &= \gcd(\gcd(a, c), b) \\ &= \gcd(\gcd(b, c), a) \end{aligned}\right\}$$

4)** $\gcd(a, b) = \gcd(a - b, b)$

$A >= B > 0$

Eg : $\gcd(12, 5) = 1$

$\gcd(12 - 5, 5) = \gcd(7, 5) = 1$

eulidean division algo .

5)*** $\gcd(a, b) = \gcd(b, a \% b)$

Eg : $\gcd(30, 5) = 5$

$\gcd(30 - 5, 5)$

$\gcd(25 - 5, 5)$

$\vdots$

$\gcd(0, 5)$

$\gcd(a - b, b)$

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

$\vdots$

$\gcd(a - xb, b)$

$a >= x * b$

$\gcd(31, 6) = \gcd(31 \% 6, 6)$

$\gcd(31-6, 6)$

$\gcd(25-6, 6)$

$\gcd(19-6, 6)$

$\gcd(13-6, 6)$

$\gcd(7-6, 6)$

$\gcd(1, 6) = 1$

write a function to find gcd(a, b)

$\gcd(24, 16) =$ ~~$\gcd(24 \% 16, 16)$~~

~~$= \gcd(8, 16)$~~

~~$\gcd(8 \% 16, 16)$~~

~~$\gcd(8, 16)$~~

~~$\gcd(8 \% 16, 16)$~~

~~$\gcd(8, 16)$.~~

$\gcd(24, 16) = \gcd(16, 24 \% 16)$

$= \gcd(16, 8)$

$= \gcd(8, 16 \% 8)$

$= \gcd(8, 0) = \underline{\underline{8}}$

Pseudocode

$a > 0 \quad b > 0$

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

can be implemented iteratively.

SC : O(1)

TC : $O(\log(\max(a, b)))$ ← SC

$gcd(8, 24) \longrightarrow gcd(24, 8 \% 24)$

$\longrightarrow gcd(24, 8)$

Given an array calculate gcd of entire array.

$$A = \{\underbrace{6 \quad 12}_{6} \quad 15\}$$

$$\underbrace{6 \qquad 15}_{\underline{\underline{3}}}$$

```
ans = A[0]
for i → 1 to N-1 {
    ans = gcd (ans , A[i])
}
print(ans)
```

TC : $O(N * \overbrace{\log \max(A)}^{gcd})$

Given A[N] , we have to delete one element such that gcd of the remaining elements become max

	0	1	2	3	4
A[] =	24	16	18	30	15

return max gcd after deleting one element .

					gcd of rest.
~~24~~	16	18	30	15	1
24	~~16~~	18	30	15	3 → ans
24	16	~~18~~	30	15	1
24	16	18	~~30~~	15	1
24	16	18	30	~~15~~	2

Brute force

∀i ignore A[i] and calculate gcd for rest.

TC : $O(N^2 \log(\max A))$ SC: $O(1)$

You can implement gcd iteratively.

~~24~~	16	18	30	15
24	~~16~~	18	30	15
24	16	~~18~~	30	15
24	16	18	~~30~~	15
24	16	18	30	~~15~~

$$\gcd(\underbrace{\gcd(0 \dots i-1)}_{\text{prefix}}, \underbrace{\gcd(i+1 \dots N-1)}_{\text{suffix}})$$

$\text{prefix}[i] = \gcd(0-i)$

	0	1	2	3	4
	24	16	18	30	15
prefix gcd	24	8	2	2	1
suffix gcd	1	1	3	15	15

$\gcd(24, 3) = 3$

for any i $\quad \gcd = \gcd(\text{prefix}[i-1], \text{suffix}[i+1])$

$i \longrightarrow 1$ to $N-2$

if $i == 0$ $\quad \text{suffix}[i+1]$

if $i == N-1$ $\quad \text{prefix}[i-1]$

TC: $O(N * \log \max(A))$

SC: $O(N)$

Doubt session

subsets = <<>> { list of list}.

```
subsets.sort ( (a, b) ⟶ {
        la = a.size()
        lb = b.size()
        l = min(la, lb)

        for i ⟶ 0 to l-1 {
            if (a[i] < b[i]) {
                    return -1 // a comes first
            }
            if ( b[i] < a[i]) {
                    return 1 // b comes first
            }
        }

        return la - lb
});
```

1 2 3
1 2

Revision strategy.

which questions to revise ?

which took you hints in the PSF

Each and every sunday re-solve difficult problems.

Q solved within 25 mins

remove from revision

keep it and try again next week .