Ff

Maths 1 : Modular Arithmetic & GCD

AGENDA

- → Modular Arithmetic Introduction
- → Count pairs whose sum mod m is 0.
- → Introduction to GCD
- → Properties of GCD
- → Qusion : Delete One

MODULAR ARITHMETIC INTRODUCTION (%)

A%B → Remainder when A is divided with B

↳ Range → [0 to B-1]

Ex:- x % 6 → Ans [0 to 5] (Range)

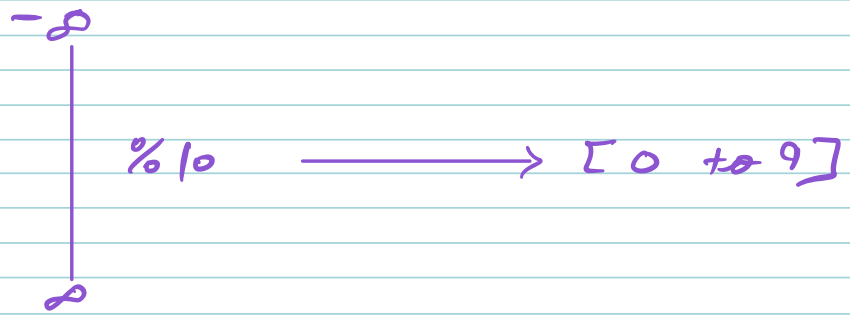
↳ 30 % 7 → 2

↳ 40 % 9 → 4

↳ 5 % 5 → 0

↳ 1 % 2 → 1

Question :- why do we need Modular Arithmetic ?



↳ % is used for limiting the range of output.

⇒ **Another way of Finding Mod**

↳ $30\%7 = 30-7 = 23-7 = 16-7 = 9$
$9-7 = \boxed{2}$ Ans

★ $30\%7$ = We are trying to subtract multiple of 7 just less than 30

$$7 \overline{)\,30\,(4}$$
$$-28$$
$$\underline{\quad 2 \quad} \leftarrow \text{Ans}$$

Generic

A%B = Keep Subtracting B from A till $A \geq B$

Ex:- ↳ 30 % 7 = 30 - 28 = 2

↳ 61 % 5 = 61 - 60 = 1

↳ -7 % 3 = -7 - (-9) = -7 + 9 = 2

↳ -30 % 9 = -30 - (-36) = -30 + 36 = 6

Ans

⇒ In machines, % works fine when A is +ve. But gives wrong Ans when A becomes -ve except python

Eg:- In Machine

↳ -7 % 3 = -1

↳ -30 % 9 = -3

Question :- How to get correct Ans?

a % m ⟶ fine (a >= 0)

↳ (x) + m (a < 0)

Rules of Modular Arithmetic

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

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

L.H.S:-

$(a+b)\%5$

$(9+8)\%5$

$17\%5 \Rightarrow 2$

R.H.S

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

$(4+3)\%5$

$7\%5$

$= 2$

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

③ $(a+m)\%m \longrightarrow a\%m$

$\hookrightarrow (a\%m + m\%m)\%m \Rightarrow (a\%m + 0)\%m$

$\Rightarrow (a\%m)\%m$

$\Rightarrow a\%m$

④ $(a-b)\%m \longrightarrow [a\%m - b\%m + m]\%m$

Eg:- $a=10, \quad b=8, \quad m=9$

L.H.S $(a-b)\%m$

$\Rightarrow (10-8)\%9$

$\Rightarrow 2\%9 \Rightarrow 2$

R.H.S $\Rightarrow (a\%m - b\%m)\%m$

$\Rightarrow (10\%9 - 8\%9)\%9$

$\Rightarrow (1-8)\%9$ ✗ Wrong

So, $(1-8+9)\%4$

$\Rightarrow (2)\%9 \Rightarrow \boxed{2}$

Hence, from point (3) & (4) we can say if -ve then you can always take $(+m\%m)$ because if Result is -ve then point 3 states it will not impact.

(5) $(a^b)\%m \longrightarrow (a\%m)^b\%m$

↳ $\underbrace{(a * a * a \ldots * a)}_{b \text{ times}}\%m$

$\Rightarrow [(a\%m) * (a\%m) * \ldots .. * (a\%m)]\%m$

Quiz! :- Evaluate $(37^{103} - 1)\%12$

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

$\Rightarrow [37^{103}\%12 - 1\%12 + 12]\%12$

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

$\Rightarrow [1^{103}\%12 + 11]\%12$

$\Rightarrow [1 + 11]\%12$

$\Rightarrow 12\%12 \Rightarrow \boxed{0}$ Ans

VVV Imp

Question :- Given N array elements, find count of pairs (i, j) such that

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

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

Ex :- $A[] = \{4, 3, 6, 3, 8, 12\}$

$m = 6$

Brute force

↳ check all the possible pairs & if satisfy above condition increase count.

TC → $O(N^2)$

↳ **OPTIMIZATION**

Hint :- Can We Use ?

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

IDEA :- $(a+b) \% m = 0$

$\Rightarrow [\underbrace{a\%m}_{[0-(m-1)]} + \underbrace{b\%m}_{[0-(m-1)]}] \% m = 0$

$[1 \rightarrow (m-1)] \% m = 0$

$[2 \rightarrow (m-2)]$

$[3 \rightarrow (m-3)]$

$[0 \rightarrow (m-0)/0] \% m = 0$

Conclusion :- In pair if we want the Sum % m to be zero, then if we know the first No. % m then the second No. % m should be [m - (first No % m)]

Ex:- arr[12] = { 6, 7, 5, 11, 19, 20, 9, 15, 14, 13, 12, 23 }

%5 ↓

arr[12]%5 = { 1 2 0 1 4 0 4 0 4 3 2 3 }

Algo

remainder	freq	
0	3	→ $\frac{x*(x-1)}{2}$
1	2	
2	2	
3	2	
4	3	

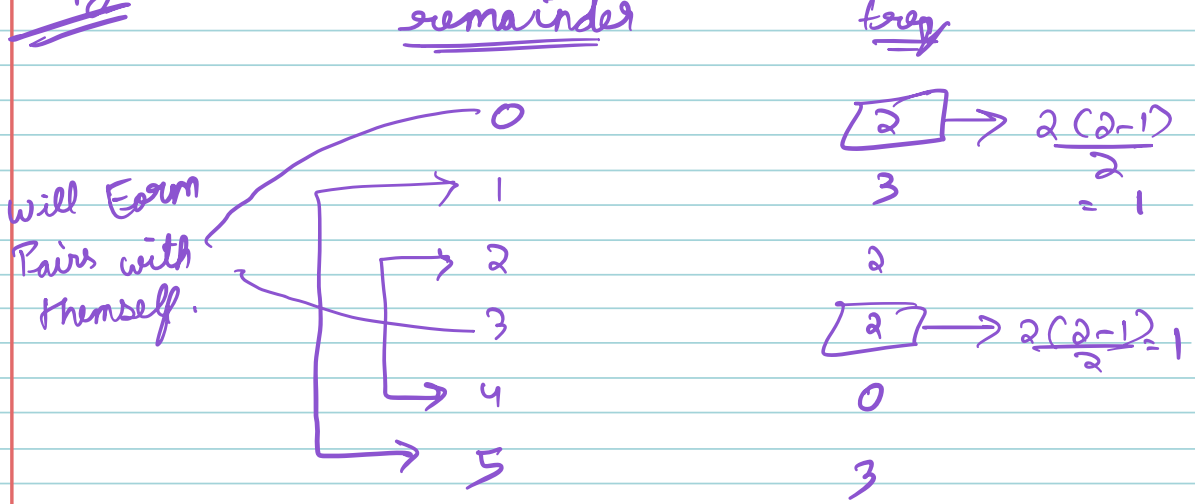
Ans ⇒ 6 + 4 + 3 = 13 pairs

arr[12] = { 6 7 5 11 19 20 9 15 14 13 12 23 }

%6 ↓

arr[12]%6 = { 0 1 5 5 1 2 3 3 2 1 0 5 }

Algo



Ans => 1 + 1 + 9 + 0 => 11 Ans

PSEUDO CODE

TODO {
Given arr[N] & m
hashmap < int, int > hm,
Remainder [arr[i] % m]
frequency

```
c = 0
x = hm[0];
c = c + x * (x-1) / 2 ;

if ( m % 2 == 0 ) {
    x = hm[m/2];
    c = c + x * (x-1) / 2 ;
}
```

DRY RUN

$m = 6$

$i = 1,\ m-i = 5$

$i = 2,\ m-i = 4$

```
for ( i = 1 ; i < (m+1)/2 ; i++ ) {
    c = c + (hm[i] * hm[m-i]);
}
```

i	hm[i]	hm[m-i]	
1	3	3	$\Rightarrow 9$
2	2	0	$\Rightarrow 0$

TC $\rightarrow O(N+m)$

Quiz :- Space Complexity : Pair Sum Divisible by m

Case :- $N = 100$, $m = 10$

SC $\rightarrow O(m)$

Case $N = 10$, $M = 100$

SC $\rightarrow O(N)$

SC $\rightarrow O(\text{Min}(m, N))$

GCD

↳ Greatest common Divisor

↳ Highest common factor (HCF)

⇒ gcd (a, b) = x

↳ x is biggest No. such that

a % x = 0

b % x = 0

Examples

① gcd (15, 25) = 5

factors: 1, 3, 5, 15 | 1, 5, 25

② gcd (12, 30) = 6

1, 2, 3, 4, 6, 12 | 1, 2, 3, 5, 6, 10, 15, 30

③ gcd (10, -25) ⇒ 5

1, 2, 5, 10 | 1, -25, -5, -1, 5, 25

④ gcd (0, 8) ⇒ 8

0, 1, 2, 3, ..., ∞ | 1, 2, 4, 8

(5) gcd(0, -10) => 10

0	-10
1	-5
2	-2
.	-1
.	1
.	2
.	5
∞	10

(6) gcd(0,0) => ∞ (Not Defined)

0	0
1	1
2	2
3	3
.	.
.	.
∞	∞

(7) gcd(-2, -3) = 1

-2	-3
-1	-1
1	1
2	3

(8) gcd(0, -5) = 5

0	-5
1	-1
2	1
3	5
4	
.	
.	
∞	

(9) gcd(0, 5) = 5

GENERIC

$$gcd(0, x) = |x| \qquad (x \neq 0)$$

PROPERTIES OF GCD

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

2. $gcd(0, x) = |x|$ $(x != 0)$

3. $gcd(A, B, C) = gcd(A, gcd(B, C))$
   $gcd(B, gcd(A, C))$
   $gcd(C, gcd(A, B))$

4. ★★★ Special property

   $A, B > 0$ & $A >= B$

   then $gcd(A, B) = gcd(A - B, B)$

   Eg :- $gcd(10, 5) = gcd(10 - 5, 5)$
   $gcd(5, 5)$
   $\downarrow$
   5

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

   Eg :- $gcd(10, 5) = gcd(10 \% 5, 5)$
   $gcd(0, 5)$
   $\downarrow$
   5

Function of GCD

So, $gcd(a, b) = gcd(a \% b, b)$

↳ $gcd(24, 16) = gcd(8, 16) = gcd(8, 16)$ ∞

.....

other way

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

↳ $gcd(24, 16) = gcd(16, 8) = gcd(8, 0) = \boxed{8}$

↳ $gcd(14, 21) = gcd(21, 14) = gcd(14, 7)$

Swapped automatically

$= gcd(7, 0)$

$= \boxed{7}$

↳ $gcd(3, 5) = gcd(5, 3) = gcd(3, 2) = gcd(2, 1)$

$= gcd(1, 0) = \boxed{1}$

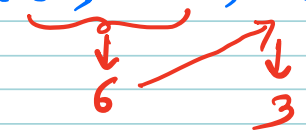
PSEUDO CODE

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

TC ⟶ O(log(max(a,b)))

Question :- Given an array, calculate GCD of entire array.

Ex :- {6, 12, 15} ⇒ Ans 3



PSEUDO CODE

```
ans = 0;
for (i = 0; i < A.length; i++){
    ans = gcd(ans, A[i]);
}
```

TC → O(N * log(max(A[i]))

Question :- Given arr[N] elements, we have to delete one element such that GCD of remaining element becomes maximum.

Ex :- arr[] = { 24 (0), 16 (1), 18 (2), 30 (3), 15 (4) }

		GCD
✓	arr[] = { ~~24~~, 16, 18, 30, 15 }	1
	arr[] = { 24, ~~16~~, 18, 30, 15 }	3
	arr[] = { 24, 16, ~~18~~, 30, 15 }	1
	arr[] = { 24, 16, 18, ~~30~~, 15 }	1
✓	arr[] = { 24, 16, 18, 30, ~~15~~ }	2

Ans = 3

Brute force

↳ Delete an arr[i] element, calculate GCD of remaining elements & get overall max.

TC → [N^2 * log (max (arr[i]))]

↳ OPTIMIZATION

IDEA :- Similar to Special index problem

Ex :- arr[] = { 24 , 16 , 18 , 30 , 15 }
(0) (1) (2) (3) (4)

Pf gcd = { 24 8 , 2 , 2 , 1 }

Sf gcd = { 1 , 1 , 3 , 15 , 15 }

so, then if i want gcd of except i^{th} position, will be what.

gcd = gcd [Pf gcd [i-1] , Sf gcd [i+1]]

PSEUDO CODE

```
int deleteOne(int[] arr, N){
TODO <- { Pfgcd;
          Sfgcd;
```

excluded. 0th index N-1th index

```
ans = max( Sfgcd[1], Pfgcd[N-2]);

for (i = 1 ; i < N-1 ; i++){
    // deleting ith element
    left = Pfgcd[i-1];
    Right = Sfgcd[i+1];
    currgcd = gcd(left, right)
    ans = max(ans, currgcd)
}

return ans;
```

TC → O(N log(max(arr[i])))
SC → O(N)

Optional proof:-

$$GCD(a,b) = GCD(a-b,b)$$

Proof:-

$\xrightarrow{L.H.S} gcd(23,5) = 1$

$\xrightarrow{R.H.S} gcd(23-5,5) = gcd(18,5) = 1$

L.H.S

Let, $gcd(a,b) = d$

$\Rightarrow a \% d = 0$ & $b \% d = 0$

$\Rightarrow (a-b) \% d = 0$

$\Rightarrow$ d is a factor of a, b, (a-b).

R.H.S

Let, $gcd(a-b,b) = t$

$\Rightarrow (a-b) \% t = 0$ & $b \% t = 0$

$\Rightarrow ((a-b)+b) \% t = 0$

$\Rightarrow a \% t = 0$

$\Rightarrow$ t is a factor of a, b, (a-b).

if, t is a common factor of a & b.
d is a greatest common factor of a & b.

$\Rightarrow \boxed{d >= t}$ — (1)

if, d is a common factor of (a-b) & b.
t is greatest common factor of (a-b) & b.

$\Rightarrow \boxed{t >= d}$ — (2)

Based on (1) & (2)

$$GCD(a, b) = GCD(a-b, b)$$

Hence proved