Agenda

1. Introduction & Properties of % wrt [+, -, x, and Power]
   A. Mod on Power Function
   B. Pair sum divisible by M
2. Find GCD(a, b)
   A. Properties of GCD.
   B. GCD optimised code

Modulo (%) Operator

- A % B $\Rightarrow$ remainder when A is divided by B.
- Range of A % B $\Rightarrow$ $[0, B-1]$

- Why do we need % ? $\rightarrow$ to limit the range.

$$\left.\begin{array}{c} -\infty \\ \vdots \\ +\infty \end{array}\right\} \% \, m \Rightarrow [0, m-1]$$

Modular Arithmetic

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

$$(3+4) \% 5 = (\underbrace{(3 \% 5)}_{3} + \underbrace{(4 \% 5)}_{4}) \% 5 \Rightarrow \underline{\underline{2}}.$$

<u>Assumption</u> → the largest integer value → 9

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

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

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

$(4 \times 5) \% 7 = (4 \% 7 \times 5 \% 7) \% 7$

$= (20) \% 7 = 6$

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

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

$(a + m) \% m = (a \% m + \overset{0}{\cancel{m \% m}}) \% m$

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

$= a \% m$

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

$a = 10, \quad b = 2, \quad m = 9$

$(10 \% 9 - 2 \% 9 + 9) \% 9$

$= (1 - 2 + 9) \% 9$

$\Rightarrow 8 \% 9 = 8$

$a = 7, \quad b = 2, \quad m = 9$

$\Rightarrow (7 \% 9 - 2 \% 9) \% 9$

$\Rightarrow (7 - 2) \% 9 = 5$

5. $a^b \% m = (\underbrace{a \times a \times a \times a \times a \text{ --- --- } \times a}_{b \text{ times}}) \% m$

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

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

Quiz :

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

$$= \left(\underbrace{37^{103} \% 12} - 1 \% 12 + 12\right) \% 12$$

$$= (1 - 1 + 12) = 12 \% 12 = \underline{0}$$

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

$$= 1^{103} \% 12 = 1 \% 12 = 1$$

Apply MOD on Fast Power

(a^n % m)

Constraints:
1 <= a <= 10^9
1 <= n <= 10^9
2 <= m <= 10^9

```
int pow( int a, int n, int m){
    if (n==0) { return 1 }
    long p = pow( a, n/2 , m);
    if ( n%2 == 0){
        return (int)((p×p)%m) ;
    }
    else{
        return int (((p× p) %m × a) %m);
    }
}
```

$1 \leq a \leq 10^9$
$1 \leq n \leq 10^9$
$1 \leq m \leq 10^9$

T.C → $O(\log_2 N)$
S.C → $O(\log_2 N)$

→ sum of all array elements % (10^9+7) .

$m = 10^9+7$

```
long sum = 0;
for( i = 0; i < N; i++){
      sum = (sum + arr[i]) % m
}
return sum % m
```

$1 \le N \le 10^9$

$1 \le arr[i] \le 10^{10}$

< 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)

arr → [**4 7 6 5 8 3**]

0 1 2 3 4 5

m = 6

ans = 2

(4 + 8) % 6 → 0

(7 + 5) % 6 → 0

Idea -1

Consider all the pairs & check if their sum is divisible by m.

T.C → O(n^2)

S.C → O(1)

Idea -2

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

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

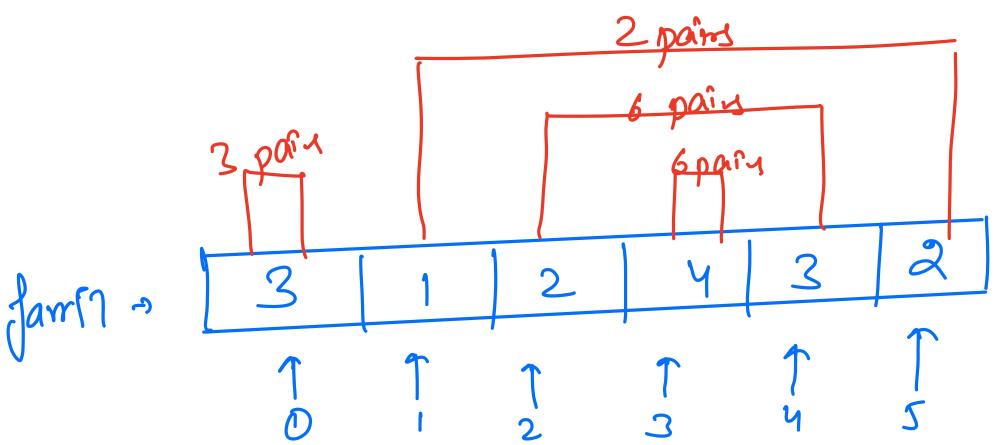
0	+	0	→	0
1	+	m-1	→	0
2	+	m-2	→	0
3	+	m-3	→	0
⋮		⋮		
i	+	m-i	→	0

Example :

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

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

marr[] → [2 3 4 2 0 3 5 0 5 1 0 4 3 4 3]



$$^{x}C_2 = \frac{x(x-1)}{2}$$

$\boxed{ans \rightarrow 17}$

</> Code

```
int farr[m];

for( i=0; i<N; i++){
    farr[arr[i]%m]++;
}

ans = 0;
ans += (farr[0] x (farr[0]-1)) / 2;
if (m%2 == 0){
    ans += (farr[m/2] x (farr[m/2]-1)) / 2;
}

l = 1,  r = m-1

while( l < r){
    ans += (farr[l] x farr[r]);
    l++;
    r--;
}
return ans;
```

case of '0' and m/2

T.C → O(N+m)

S.C → O(m)

GCD → Greatest Common Divisor / Highest Common Factor

$GCD(A, B) = x \Rightarrow \begin{array}{l} A \% x = 0 \\ B \% x = 0 \end{array}$ $x \to$ highest no. to hold this property true.

GCD (20, 65) → 5

20	65
1	1
2	5
4	13
5	65
10	
20	

GCD (-10, 20) → 10

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

GCD (7, 9) → 1

7	9
1	1
7	3
	9

GCD (0, 8) → 8

0	8
1	1
2	2
3	4
4	8
5	
6	
7	
8	
9	
⋮	
∞	

GCD (0, -10) → 10

0	-10
1	-10
2	-5
3	-2
4	-1
5	1
⋮	2
⋮	5
⋮	10
∞	

GCD(4, 7) → 1

4	7
1	1
2	7
4	

Properties of GCD

① $GCD(A, B) = GCD(B, A)$

② $GCD(0, A) = |A|$

③ $GCD(A, B, C) = GCD(GCD(A, B), C)$

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

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

④ Special Property

$A, B > 0$ and $A > B$

given, $GCD(A, B) = x$

$A \% x = 0$

$B \% x = 0$

$x \rightarrow$ highest no.

$GCD(A - B, B) = x$

$(A - B) \% x = 0$

$B \% x = 0$

$x \rightarrow$ highest no.

$\Rightarrow (\cancel{A \% x}^{0} - \cancel{B \% x}^{0} + x) \% x$

$\Rightarrow 0$

<u>Conclusion</u> :- $GCD(A, B) = GCD(A-B, B)$

$GCD(23,5) = GCD(18,5) = GCD(13,5) = GCD(8,5)$

$= GCD(3,5) = 1$

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

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

GCD Function

T.C → $O(\log_2 \min(a,b))$
S.C → $O(\log_2 \min(a,b))$

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

    return gcd( b, a%b);
}
```