Modulo. (%)

$A\%B$ → remainder when A is divided by B.

Range of $a\%m$ → $[0, m-1]$

Why do we need %. // to limit the range.

$$\left.\begin{matrix}-\infty\\ \\ +\infty\end{matrix}\right\} \%10 \Rightarrow [0,9]$$

$$a\%m \Rightarrow [0, m-1]$$

Modular arithmetic $(\% + \{+,-,*,/\})$

① $(a+b)\%m = (a\%m + b\%m)\%m$

$$(3+4)\%5 \qquad (3\%5 + 4\%5)\%m$$

$$\Downarrow \qquad\qquad \Downarrow \qquad \Downarrow$$

$$2 \qquad (3 + 4)\%m = 7\%5 = \underline{\underline{2}}.$$

② $(a+m)\%m = (a\%m + \overset{0}{\cancel{m\%m}})\%m$

$= (a\%m)\%m = \underline{a\%m}$

③ $(a * b) \% m = (a \% m * b \% m) \% m$

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

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

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

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

$= (-1 + 9) \% 9 = 8 \% 9 = \underline{8}$

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

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

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

$\Rightarrow 14 \% 9 = \underline{5}.$

⑤ $a \% m = (((a \% m) \% m) \% m) \% m \; - - -$

⑥ $a^b \% m = (\underbrace{a * a * a * a * \; - - - \; * a}_{b \text{ times}}) \% m$

$= (a \% m * a \% m * a \% m * \; - - - \; a \% m) \% m$

$[a^b \% m = (a \% m)^b \% m]$

Quiz →

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

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

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

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

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

$$\begin{bmatrix} \text{int} \to [-2^{31}, 2^{31} - 1] \Rightarrow [-2 \times 10^{9}, 2 \times 10^{9}] \\ \text{long} \cdot\cdot [-2^{63}, 2^{63} - 1] \Rightarrow [-9 \times 10^{18}, 9 \times 10^{18}] \end{bmatrix}$$

① Calculate $[a^N \% m]$

$1 \le a \le 10^9$

$1 \le N \le 10^5$

$1 \le m \le 10^9$

```
long ans = 1
for( i = 1; i <= N; i++) {
        ans = (ans * a) % m
}
return (int) ans;
```

T.C → O(N)
S.C → O(1)

```
int power( a, N, m){
    if (N==0) { return 1 }
    int rr = power( a, N-1, m);
    long ans = ((long) a * rr ) % m
    return (int)(ans);
}
```

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

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

T.C → O(N)
S.C → O(N)

observation :

N→even $a^N = a^{N/2} * a^{N/2}$

N→odd $a^N = a^{N/2} * a^{N/2} * a$

$$\begin{cases} a^{10} = a * 10^9 \\ a^{10} = a^5 * a^5 \\ a^{12} = a^6 * a^6 \\ a^{15} = a^7 * a^7 * a \end{cases}$$

$1 \le a \le 10^9$

$1 \le N \le 10^5$

$1 \le m \le 10^9$

```
int  fastpower( a, N ,m ) {
|     if (N==0) { return 1 }
|    long p = (long) fastpower ( a, N/2 , m) ;
|     if( N%2 == 0){
|    {         return (int)((p * p) %m);
|    }
|    else{
|    {         return (int)((p*p*a) %m);
|    }
}
```

$$\downarrow$$

$$(p\%m * p\%m * a\%m)\%m$$

$$((p*p)\%m * a)\%m$$

$$\boxed{\begin{array}{l} T.C \rightarrow O(\log_2 N) \\ S.C \rightarrow O(\log_2 N) \end{array}}$$

Q.1) Given N array elements. Find count of pairs (i, j) such that $(arr[i] + arr[j]) \% m = 0$

Note → $i \, != j$ and pair(i, j) is same as pair(j, i)

$$arr[6] : \begin{array}{cccccc} [4 & 7 & 6 & 5 & 8 & 3] \\ 0 & 1 & 2 & 3 & 4 & 5 \end{array} \quad , m = 3$$

[ans = 5]

i	j	arr[i] + arr[j]
0	3	$4+5 = 9 \% 3 = 0$
0	4	$4+8 = 12 \% 3 = 0$
1	3	$7+5 = 12 \% 3 = 0$
1	4	$7+8 = 15 \% 3 = 0$
2	5	$6+3 = 9 \% 3 = 0$

Idea-1 Consider all the pairs T.C → $O(N^2)$, S.C → $O(1)$

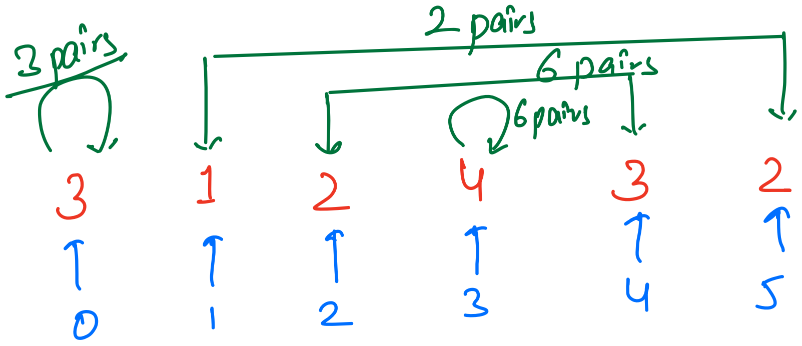
Idea-2 $(a+b) \% m = (\underline{a \% m} + \underline{b \% m}) \% m = 0$

1	m-1	
2	m-2	
3	m-3	
4	m-4	
⋮	⋮	
i	m-i	
m/2	m/2	: Both values are same
0	0	: Both values are same

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

$m = 6$.

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



$\frac{3\times\cancel{2}}{\cancel{2}} = 3$ pairs

$^4C_2 = \frac{\overset{2}{\cancel{4}}\times 3}{\cancel{2}} = 6$ pairs

$^NC_2 = \frac{N(N-1)}{2}$

ans = 17.

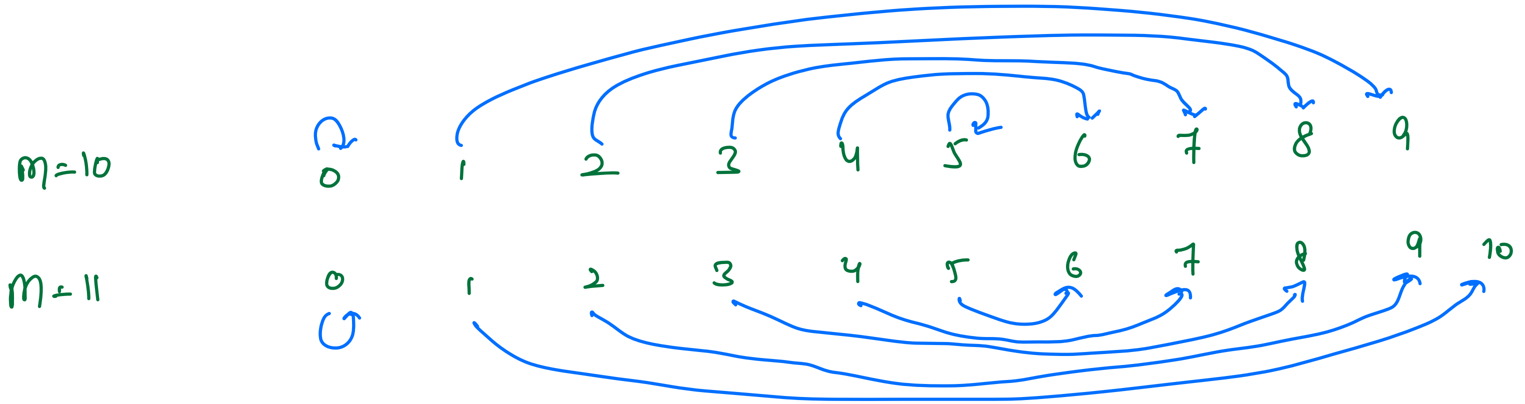
code.

```
Hashmap < int, int > map;

for( i = 0; i < N; i++){
        // insert arr[i] % m in map
}

ans = 0
  x = map[0];                      ]
  ans += (x * (x-1)) / 2;          ]  Case of 0

if (m % 2 == 0){
        x = map[m/2];              ]
        ans += (x * (x-1)) / 2;    ]  Case of m/2
}

for (i = 1; i < (m+1)/2; i++){
        ans += map[i] * map[m-i];
}

return ans;
```

```
class Solution:
    # @param A : list of integers
    # @param B : integer
    # @return an integer
    def solve(self, A, B):
        N=len(A)
        hasmap={}
        count=0
        for i in range(N):
            A[i]=A[i]%B
            k=(B-A[i])%B
            if k in hasmap:
                count+=hasmap[k]
            if A[i] in hasmap:
                hasmap[A[i]]+=1
            else:
                hasmap[A[i]]=1
        count=count%(pow(10,9)+7)
        return count
```

T.C -> O(N+m)

S.C -> O(m)



Congruency

x and y are said to be congruent w.r.t N, if

$$x \% N = y \% N$$

$$x \cong y \pmod{N}$$

$$(x * z) \cong (y * z) \pmod{N}$$

$$(x * z) \% N = (y * z) \% N$$

$$(\underset{\checkmark}{\underline{x \% N}} * \underline{z \% N}) \% N = (\underset{\checkmark}{\underline{y \% N}} * \underline{z \% N}) \% N$$

Fermat's Little Theorem

Fermat's little theorem

a, p

$\gcd(a, p) = 1$

↳ p = prime number

$\Downarrow$

$$\left[a^{p-1} \% p = 1 \right] \Rightarrow \text{Proved mathematically}$$

$\Downarrow$

$$a^{p-1} \% p = 1 \% p$$

$$\Rightarrow \quad a^{p-1} \cong 1 \pmod{p}$$

$$a^{p-1} * a^{-1} \cong a^{-1} \pmod{p}$$

$$\left\{ a^{p-2} \cong a^{-1} \pmod{p} \right\}$$

(inverse modulo)

$$(x / y) \% p = (x \% p * y^{-1} \% p) \% p$$

$$\left[(x/y) \% p = (x \% p * y^{p-2} \% p) \% p \right]$$

↓ fast power function

$p \rightarrow$ prime no.

What if p is not prime?

10^9+7.

⇓

[Extended Euclidean theorem]

$a^N \% m$.

N → odd and a is -ve. [we need to handle this case only]