④ Modular Arithmetic

+, −, ×, /

modulo ← %

$a \% b$ → remainder when a is divided by b

$10 \% 3 \to 1$

$$\begin{array}{r} 3 \\ 3\overline{)10} \\ -9 \\ \hline 1 \end{array}$$

3 → quotient
10 → dividend
3 → divisor
1 → remainder

$100 \% 5 \to$

$$\begin{array}{r} 20 \\ 5\overline{)100} \\ -100 \\ \hline 0 \end{array}$$

dividend = divisor × quotient + remainder

⇒ $\boxed{\text{remainder} = \text{dividend} - \text{divisor} \times \text{quotient.}}$

$\boxed{a \% b = a - b \times (a/b)}$

(a/b) → int div (C++)

(a/b) → floor(a/b) (py)

$35 \% 4 = 35 - 4 \times (35/4)$

$35 - 4 \times 8$

$35 - 32 = 3$ //

$a \% b \rightarrow [0, b-1]$

Remainder = dividend − greatest multiple of divisor <= dividend

$35 \% 4 = 35 - 32 = 3$

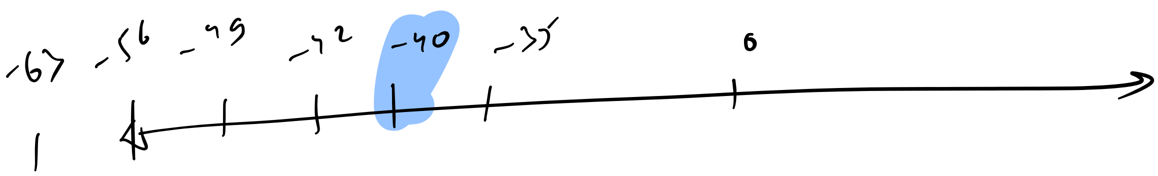
$-40 \% 7 \rightarrow -40 - (-42) = 2$

C++/Java

-5

$+7$

python

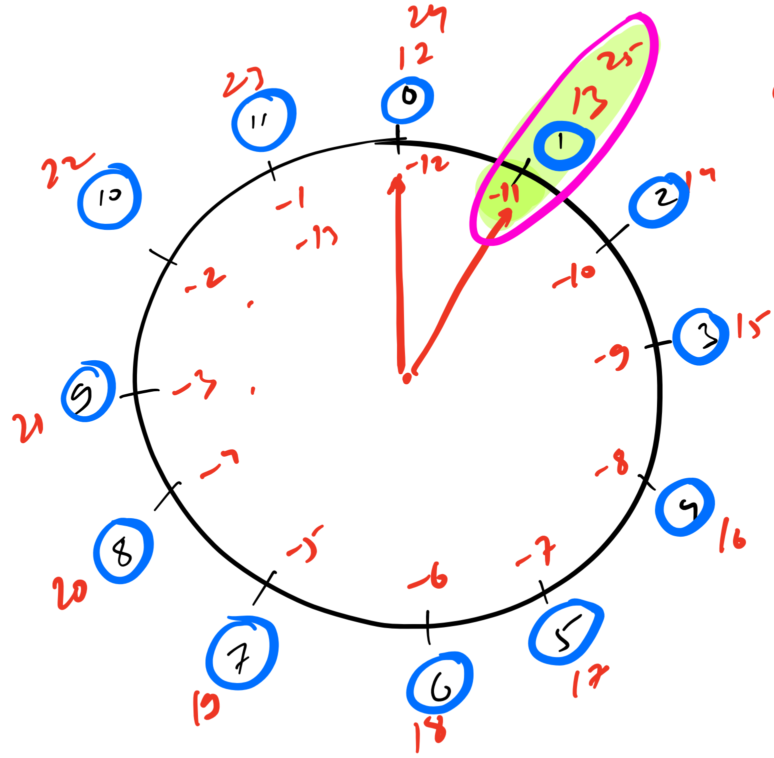


Why?

$$\begin{Bmatrix} -\infty \\ \vdots \\ +\infty \end{Bmatrix} \xrightarrow{\% M} \begin{Bmatrix} 0 \\ M-1 \end{Bmatrix}$$

Reduce the range!

Wheel



$0 \leftarrow 12 \% 12$

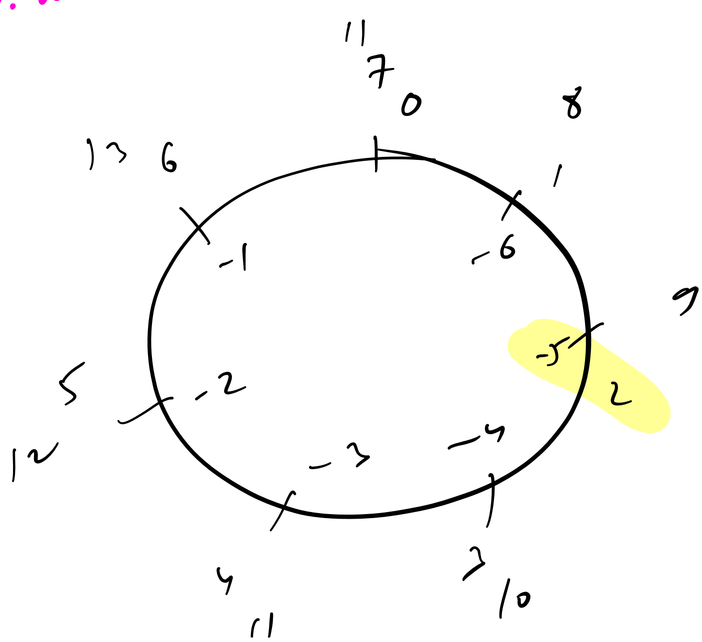
$1 \leftarrow 13 \% 12$

$1 \leftarrow 25 \% 12$

$-11 \% 12 =$

$1 \% 12 = 13 \% 12 = 25 \% 12 = 1$

$-11, 1, 13, 25 \ldots$ are all modular congruent w.r.t to 12



$-5 \% 7$
$= 2 \% 7$

④ Properties of modular arithmetic

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

$\underbrace{(a+b) \% M}_{[0, M-1]}$

$\underbrace{\underbrace{(a \% M)}_{[0, M-1]} + \underbrace{(b \% M)}_{[0, M-1]}}_{[0, 2M-2]}$

$a = 7, \quad b = 11, \quad M = 4$

$(7+11) \% 4$

$18 \% 4$

$= 2$

$(7 \% 4 + 11 \% 4) \% 4$

$(3 + 3) \% 4$

$6 \% 4$

$= 2$

2) $\boxed{a \% M = (a \% M) \% M}$

$\underbrace{12 \% 5}_{2} = \underbrace{(12 \% 5)}_{2} \% 5 \% 5 \% 5$

3) $\boxed{a \% M = (a + M) \% M}$

4) $\boxed{(a \times b)\ \%\ M = ((a\ \%\ M) \times (b\ \%\ M))\ \%\ M}$

$a = 7, \quad b = 11, \quad m = 4$

$(7 \times 11)\ \%\ 4$ | $((7\ \%\ 4) \times (11\ \%\ 4))\ \%\ 4$

$77\ \%\ 4$ | $(3 \times 3)\ \%\ 4$

| $9\ \%\ 4$

$1 \leftrightarrow 1$

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

$\underbrace{(a-b)\ \%\ M}_{[0,\ M-1]}$

$[0, M-1] - [0, M-1] + [M, M]$

$\boxed{[-M+1,\ M-1]}$ $\quad [1, 2M-1]$

$\%\ M$

$\boxed{[0, M-1]}$

$a = 6 \quad m = 4$

$b = 7$

$(6-7)\ \%\ 4 \rightarrow ((6\ \%\ 4) - (7\ \%\ 4) + 4)\ \%\ 4$

$-1\ \%\ 4$ | $(2 - 3 + 4)\ \%\ 4$

$= 3$ | $3\ \%\ 4 = 3$

Q. Given an Array, M.
Calculate the no. of pairs (i, j) : $i < j$

$$(A_i + A_j) \% M = 0$$

$\boxed{A_i \geq 0}$

A :

0	1	2	3	4	5
4	7	6	5	5	3

$M = 3$

$(0, 3) = 4 + 5 = 9$
$(0, 4) = 4 + 5 = 9$
$(1, 3) = 7 + 5 = 12$
$(1, 4) = 7 + 5 = 12$
$(2, 5) = 6 + 3 = 9$

$\rightarrow$ 5

1) BF

```
cnt = 0
f (i: 0 → N-1)
    f (j: i+1 → N-1)
        if ((Ai + Aj) % M == 0)
            cnt++
ret cnt;
```

$\boxed{TC = O(N^2)}$

$\boxed{SC = O(1)}$

2)

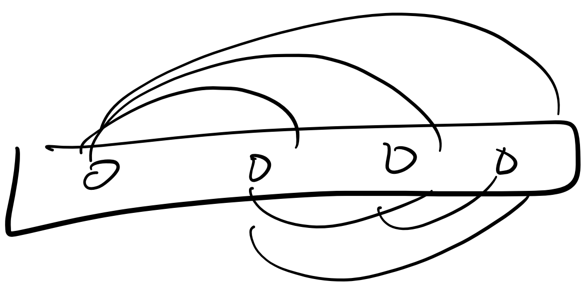
M = 10

A : 50, 17, 2, 5, 4, 6, 23, 13, 26, 14, 18, 15, 30, 35, 20

%10

0 7 2 5 4 6 3 3 6 4 8 5 0 5 0

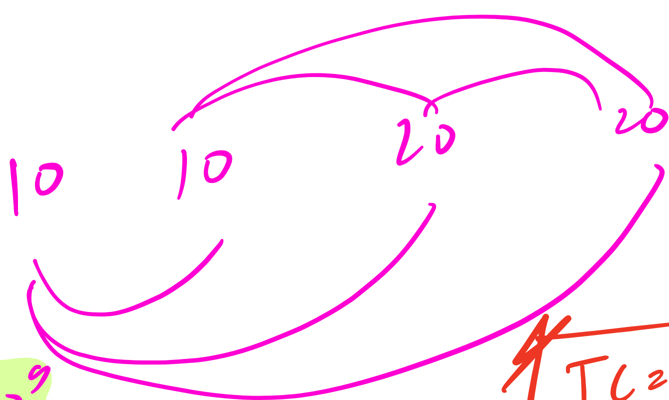
i		j
1	→	9
2	→	8
3	→	7
4	→	6
5	→	5
0	→	0



$^4C_2 = 6$

```
HashMap<int, int> hm;          // M
f(i: 0 → N-1) {                → N
    x = A[i] % M;
    hm[x]++;
}
i=1, j=M-1        ANS=0        → M
while(i<j) {
    ANS += hm[i] * hm[j];
    i++, j--;
}
if(M%2==0) {
    ANS += (hm[M/2] * (hm[M/2]-1))/2;
}
ANS += (hm[0] * (hm[0]-1))/2;
```

$M=10$



$1 <= A[i] <= 10^9$

$1 <= N <= 10^5$

$1 <= M <= 10^9$

$\boxed{TC = O(N+M)}$

$\boxed{SC = O(min(N,M))}$

$M = 10$

A : 50, 17, 2, 5, 4, 6, 23, 13, 26, 14, 18, 15, 30, 35, 20

%10

0 7 2 5 4 6 3 3 6 4 8 5 0 5 0

```
ANS = 0
HashMap<int, int> hm;
f (i = 0; i < N; i++) {            → O(N)
    x = A[i] % M;
    f = M - x;                     10-0=10
    if (x == 0) f = 0;
    ANS += hm[f];

    hm[x]++;

}
ret ANS;
```

$\boxed{TC = O(N)}$

$\boxed{SC = O(\min(N, M))}$

(A) Inverse Modulo

$$(a/b)\ \%\ M = ((a\ \%\ M)\ /\ (b\ \%\ M))\ \%\ M$$

$[0, M-1]$

1. $x/y = z....$

2. $x/0$

$$\boxed{(a/b)\ \%\ M} = (a \times 1/b)\ \%\ M$$

$$= (a \times b^{-1})\ \%\ M$$

$$= \boxed{((a\ \%\ M) \times (b^{-1}\ \%\ M))\ \%\ M}$$

$(1/b)\ \%\ M = (b^{-1})\ \%\ M \longrightarrow$ Inverse modulo of b w.r.t. M

Q given b, M. find inv. modulo of b w.r.t. M

$(b^{-1})\% M$.

// $b^{-1} \% M$ exists only if $\gcd(b, M) = 1$

// $b^{-1} \% M \longrightarrow [1, M-1]$

$$(b \times 1/b) \% M = 1$$

$$(b \times (b^{-1})) \% M = 1$$

$$\boxed{((b \% M) \times \underbrace{(b^{-1}) \% M}_{\text{unknown} \to [1,\, M-1]}) \% M = 1}$$

```
f( i=1 → M-1) {
    if(((b % M) x i) % M == 1){
        ret i;
    }
}
```

$\boxed{\text{TC } O(M)}$

// SPECIAL CASES

$b^{-1} \% p$ | $p \rightarrow$ prime no.

$b \% p \neq 0$

1) $(b^{p-1}) \% p = 1$: fermat's theorem

2) $\boxed{(b^{-1}) \% p = (b^{p-2}) \% p}$

Inv mod

$a^n \longrightarrow (a^{n/2})^2$: n is even

$a^n \longrightarrow (a^{n/2})^2 \times a$: n is odd

$2^{10} \longrightarrow (2^5)^2$

$2^{11} \longrightarrow (2^5)^2 \cdot 2$

```
pow(a, n) {
   if(n==0) ret 1;
  ha = pow(a, n/2);
  if( n % 2 == 0) {
       ret  ha × ha;
  }
  else {
       ret  ha × ha × a;
  }
}
```

a^n

$a^{n/2}$

$a^{10} = \underline{a^5 \times a^5}$

$a^{11} = \underline{a^5 \times a^5 \times a}$

$a^n \rightarrow a^{n/2} \rightarrow a^{n/4} \text{ — — — — } a^0$

$\underline{O(\log_2 n)}$

$\boxed{TC = O(\log n)}$

$\underline{10^9} < p$

$a^n \% p$

$p \to$ int

$a <= 10^9$

$\underline{p = 10^9 + 7}$

int pow(a, n, p)

if(n==0) ret 1;

long ha = pow(a, n/2, p);

if(n % 2 == 0) {

ret $((ha \cancel{\% p}) \times (ha \cancel{\% p})) \% p$;

}

else {

ret $(((ha \cancel{\% p}) \times (ha \cancel{\% p})) \% p \times (a \cancel{\% p})) \% p$;

}

}

$\boxed{TC = O(\lg n)}$

$$\boxed{(b^{-1}) \% p = \underbrace{(b^{p-2}) \% p}_{}}$$

Inv mod

pow(b, p-2, p)

$$\boxed{TC = O(\log_2 p)}$$

$$(a/b) \% p = (a \times b^{-1}) \% p$$

$$= (a \% p \times (b^{-1}) \% p) \% p$$

$$\boxed{(a/b) \% p = ((a \% p) \times (b^{p-2}) \% p) \% p}$$

Q Calc. $(10^5!) \% (10^9+7)$

int $p = (10^9+7);$

long $f = 1;$

$f(i = 2;\ i <= 10^5;\ i{+}{+})\ \{$

$f = ((f \cancel{\%p}) \times (i \cancel{\%p})) \% p;$

$\}$

$f < p$

ret $f;$

Q Given N, M $1 <= M <= N <= 10^5$

Calc $^N C_M \% 10^9+7$ $p = 10^9+7$

$$\frac{N!}{(N-M)!\,M!} \% p$$

$$\left(N! \times \left((N-M)! \times M!\right)^{-1}\right) \% p$$

```
int ad ( int x, int y, p) {
    ret ( ((x % p) + (y % p)) % p);
}
  sub (  ,  )
  mul (  ,  )
  div (  ,  )

 inv ( a, p) {
    ret pow( a, p-2, p);
 }
```

$$\left(N! \times \left((N-M)! \times M! \right)^{-1} \right) \% \; p$$

```
mul( f(N,p), inv( mul( f(N-M,p), f(M,p), p), p), p)
```

x