A %. B → Remainder left after dividing A by B

```
      2  → Quotient
   5 ) 14 → Dividend
      -10
   ----
       4  → Remainder
```

Divisor

Dividend = (Divisor × Quotient) + Remainder

Remainder = Dividend − Divisor × Quotient

⇓

largest multiple of divisor <= dividend

Division is repeated subtraction

14 %. 5 = 14 − 5 = 9 − 5 = 4 < divisor

⇓

2

5 × 2 = 10

5 × 3 = 15 > 14 ✗

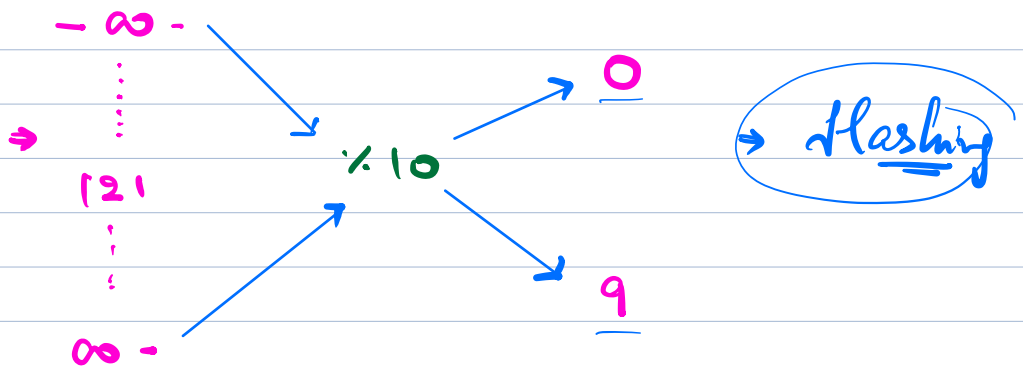
40 %. 6 = 40 − 6 ↵
34 − 6 ↵
28 − 6 ↵
22 − 6 ↵
16 − 6 ↵
10 − 6 ↵

(4) ⇒ (5) , 6 - 6 = 0

$40 - (6 \times 6) = 4$

⇓

$a \,\%\, M = [0, M-1]$



Q ⇒ $-40 \,\%\, 7 \Rightarrow [0, 6]$

$-40 - ((7) \times \_\,)$

7 ⇒ 7, 14, 21, 28, 35 .... ✗ (+ve)

7 ⇒ -7, -14, -21, -28, -35, -42, -49 ....

Ans = $-40 - (-42) = 2$

$-(40 \% 7) = (-5 + 7) \% 7$

$[-(M-1), 0]$ $\quad$ $2 \% 7 = 2$

$[1, M]$

Modular Arithmetic $[0, 2M-2]$

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

$a \% M \in [0, M-1]$ $\quad$ $b \% M \in [0, M-1]$

$a = 4, \; b = 5, \; M = 6$

$(4+5) \% 6$

$= 9 \% 6$

$= 3$

$((4 \% 6) + (5 \% 6)) \% 6$

$(4 + 5) \% 6$

$= 9 \% 6$

$= 3$

2) $a \% M = (a+M) \% M$

$= (a \% M + M \% M) \% M$ $\quad$ ($M \% M = 0$)

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

$= a \% M$

$21 \% 5$

$1 \% 5 = 1$

$[0, 4]$

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

4) $(a - b) \% M = (a \% M - b \% M) \% M$

$a = 8, \quad b = 4, \quad M = 5$

LHS

$(8 - 4) \% 5$

$= 4 \% 5$

$= 4$

$(8 \% 5 - 4 \% 5) \% 5$

$= (3 - 4) \% 5$

$= -1 \% 5 = -1$

C / C++ / Java / C# / JS

$-(1 \% 5) = -1$

Python

$-1 \% 5 = 4$

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

+ve

$[0, M-1]$

Given A, B, $(A > B)$

find M s.t. $A \% M = B \% M$.

A = 16 B = 4

$16 \% M = 4 \% M$

$M = 2, 3, 4, 6, 12$

Q1 Can $M > A$???

$M = 17$

$A \% M = A$

$B \% M = B$

$16 \% 17 = 16$

$4 \% 17 = 4$

1) Brute force

$\forall i$ from 1 to A check if $A \% i == B \% i$

2) $A \% M = B \% M$

$A \% M - B \% M = 0$

Add M on both sides

$A \% M - B \% M + M = M$

Take $\% M$ on both sides

$(A \% M - B \% M + M) \% M = M \% M$ → 0

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

$(A-B)$ is a multiple of M

M is a factor of $(A-B)$

$A = 16, \quad B = 4$

$A - B = 12$

All factors of $(A-B)$ are ans

Q2 Given N array elements.

Calculate no. of pair (i, j) s.t.

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

Note : $i \neq j$ & $(i, j) = (j, i)$

Eg $A: \underset{0}{4}, \underset{1}{7}, \underset{2}{6}, \underset{3}{5}, \underset{4}{5}, \underset{5}{3}$, $M = 3$

i j

1 0 3 $\Rightarrow (4+5) \% 3 = 0$

2	0	4	$\Rightarrow 9 \,\%\, 3 = 0$
3	1	3	$\Rightarrow (7+5) \,\%\, 3 = 0$
4	1	4	$\Rightarrow (7+5) \,\%\, 3 = 0$
5	2	5	$\Rightarrow (6+3) \,\%\, 3 = 0$

Ans = 5

Soln

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

$$(\underbrace{A[i] \,\%\, M}_{x} + \underbrace{A[j] \,\%\, M}_{y}) \,\%\, M = 0$$

x : $[0, M-1]$ $\quad$ y : $[0, M-1]$

$[0, 2(M-1)] \,\%\, M = 0$

$0, M$

$M = 6$

$[0, 10] \Rightarrow 0, 6$

$0 \,\%\, 6 = 0, \quad 6 \,\%\, 6 = 0$

pairs s.t. $x + y = 0$

or

$x + y = M$

Step 1 $\Rightarrow$ $\forall i$ $A[i] = A[i] \,\%\, M$

$M = 4$

$3 \,\%\, 4$

A: [13, 14, 22, 3, 32, 19, 16]

(0, 1, 2, 1)

$\downarrow \,\%\, 4 \Rightarrow [0, 3]$

[1, 2, 2, 3, 0, 3, 0]

ans = 0

$i \Rightarrow$ $A[i] = 1$ ans += 2

$(4-1) = 3$

Freq of 3 was important

Create a freq array

A:

M $\Rightarrow$ $A[i] \,\%\, M \Rightarrow [0, M-1]$

Array of size M

$i \Rightarrow$ $A[i] \,\%\, M = i$

$(5+15) \,\%\, 10$

A: [29, 11, 21, 17, 2, 5, 4, 6, 23, 13, 26, 14, 18, 15, 30, 35, 50, 20, 40]

5 + 5 = 10

M = 10

M = 9

M = 11

A[i] % 10 = [0, 9]

0	1	2	3	4	5	6	7	8	9
4	2	1	2	2	3	2	1	1	1
30	11	2	23	4	5	6	17	18	29
50	21		3	14	15	26			
20					35				
40									

f[0]C2

f[0]

S.C = O(M)

2×1 (Count of 1) × (Count of 9)

1×1 (Count of 2) × (Count of 8) i ⇒ m − i

2×1 (Count of 3) × (Count of 7)

2×2 (Count of 4) × (Count of 6)

+

(Count of 5) C2

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

$\frac{(\text{Count of } 5) \times (\text{Count of } 5 - 1)}{2} = 10$

+

(Count of 0) C2

M = 9 → 11

Code

Even

Time to create freq array = O(N)

f ⇒ freq array // M

ans = 0 ;

f[0] = 0

ans += $\frac{f[0] \times (f[0]-1)}{2}$ // 0

i = 1 ; j = M-1 ;

⇒ while (i < j) { (M)

ans += f[i] x f[j] ;

i++;
j--;

}

if (M % 2 == 0) {

ans += $\frac{f[M/2] \times (f[M/2]-1)}{2}$

}

return ans;

T.C. = O(N + M)

S.C. = O(M)

11:13

4 ÷ (-3) ⇒ Not defined

Not defined

4) $(a/b) \,\%\, M = \left(\frac{(a \,\%\, M)}{b \,\%\, M}\right) \,\%\, M$ ✗

a = 16 , b = 4 M = 5

$(16/4) \,\%\, 5$

$(4 \,\%\, 5) = 4$

$\left(\frac{(16 \,\%\, 5)}{(4 \,\%\, 5)}\right) \,\%\, 5$

$= \left(\frac{1}{4}\right) \,\%\, 5$

$= (0) \,\%\, 5 = 0$

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

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

$b^{-1} \,\%\, M$ ⇓ Inverse mod of b w.r.t M

Inverse Mod

Given b, M

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

b & m are co-prime.

$b = 2$, $M = 5$ ✓

1, 2 — 1, 5

$\left(\frac{1}{2}\right) \% 5$

$b = 32$, $M = 9$ ✓

1, 2, 4, 8, 16, 32 — 1, 3, 9

$(2^{-1}) \% 5 =$

$b = 96$, $M = 9$ ✗

1, 2, 3, .. — 1, 3, 9

$$b \times \frac{1}{b} = 1$$

$1 \% M = 1$ if $M > 1$

$$\left(b \times \frac{1}{b}\right) \% M = 1$$

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

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

Ans will always be present in [1, M-1]

⇓

no need for proof

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

```
for ( i = 1 ; i < M ; i++ ){
    if( ( ( b % M ) x i ) % M ) == 1 ){
        return i ;
    }
}
```

T.C. = O(M)

Eg $b = 10, \quad M = 7$

$b^{-1} \% 7 \Rightarrow [1, 6]$

x

$((b^{-1} \% 7) \times x) \% 7 = 1$

$((10 \% 7) \times x) \% 7 = 1$

$(3 \times x) \% 7 = 1$

$1 = 3 \% 7 \mid = 1$

$2 = 3 \times 2 = 6 \not\equiv 1 \pmod 7$

$3 \times$

$4 \times$

$5 = 3 \times 5 = 15 \equiv 1 \pmod 7$

$10^{-1} \equiv 5 \pmod 7$

Fermat's Little Theorem

$b^{-1} \equiv 1 \pmod M \Rightarrow$ if M is prime

$a^p \equiv a \bmod p \rightarrow a^p \equiv a \pmod p$

$b^M \equiv b \bmod m \Rightarrow b^M \equiv b \pmod M$

$b^{M-1} \equiv 1 \bmod m$

$= b^{-1} \pmod m$ on both sides

$b^{M-2} \equiv b^{-1} \pmod M$

if M is prime $M \geq 2$

$(b^{M-2} \,\%\, M) \Rightarrow$ fast power

$a^p \Rightarrow a^{p/2} \times a^{p/2} \Rightarrow \log(p)$

$\log(M-2) = O(\log(M))$

$3 \cong 6 \,\%\, 3 = 3 \,\%\, 3 = 6 \,\%\, 3$

$a \cong b \bmod m \Rightarrow a \,\%\, m = b \,\%\, m$

$b^M \,\%\, M = b \,\%\, M$

$b^{-2} \,\%\, M$ on both sides

$(b^M \,\%\, M) \times (b^{-2} \,\%\, M) = b \,\%\, M \times b^{-2} \,\%\, M$

Take $\%\, M$ on both sides

$(((b^M \,\%\, M) \times (b^{-2} \,\%\, M)) \,\%\, M =$

$(((b \,\%\, M) \times (b^{-2} \,\%\, M)) \,\%\, M$

$(b^M \times b^{-2}) \,\%\, M = (b \times b^{-2}) \,\%\, M$

$(b^{M-2}) \cdot M = (b^{-1}) \cdot M$

$\downarrow$

$\log(M)$ time

Divide Integers $\Rightarrow$ H.W.