Welcome ☺

Agenda: 1) Mod arithmetic
2) 1½ question
3) Fermat's Theorem.

A % B → remainder of A ÷ B

eg: 362 % 13 = 11

52 % 5 = 2

1) if A < B → A % B = A
2) A % 1 ⇒ 0
3) A % A ⇒ 0

$0 \le A \% B \le B-1$

Properties

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

eg: a = 17 → (17 + 8) % 5 = 25 % 5 = 0
b = 8 a % m = 17 % 5 = 2
m = 5 b % m = 8 % 5 = 3

$(a \% m + b \% m) \% m = (2+3) \% 5 = 0$

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

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

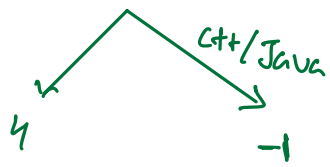
eg: $a = 17 \rightarrow (17-8)\%5 = 9\%5 = 4$

$b = 8$ $\quad a\%m = 17\%5 = 2$

$m = 5$ $\quad b\%m = 8\%5 = 3$

$(a\%m - b\%m)\%m = (2-3)\%5$

$= (-1)\%5$

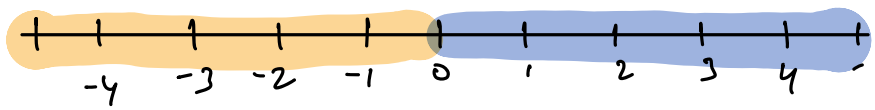


If $(A<0)$ $A\%B \Rightarrow (A\%B + B)\%B$

$A\%B \in [-(B-1), 0]$

eg: $-5\%5$

$B = 5$



Q Given an integer array A and an integer M. Find count of pairs in A s.t A[i] + A[j] is divisible by M (i < j)

eg: A : [1 3 4 8] M = 3

1,3 3,4 ✓4,8 Ans = 2
1,4 3,8
✓1,8

eg: A : [13, 14, 22, 3, 32, 19, 16] M=4

Ans = 4

Brute force

Check all pairs.

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

T.C → O(N²)
S.C → O(1)

Optimized

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

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

($A[i] \% m$: 0 … m-1; $A[j] \% m$: 0 … m-1)

0, M

0 … 2m-2

$0 \le \% \le 2m-2$

eg: A : [2 7 5 10 8 4 6 11] M = 5

⇒ %A [2 2 0 0 3 4 1 1]

→ Find pairs s.t sum = 0 or M

%M	count
0	2
1	2
2	2
3	1
4	1

$2C_2 = 1$

2*1 , 2*1

Ans = 1 + 2 + 2 = 5

Sum = 0 ⇒ $C_0 C_2$ ⇒ $\frac{C_0 * (C_0 - 1)}{2} = \frac{2*1}{2} = 1$

Sum = M

1	M-1	⇒ $C_1 * C_{M-1}$
2	M-2	⇒ $C_2 * C_{M-2}$
3	M-3	

Pseudocode

```
// count array
for( i -> 0 to N-1)
{
   C[ A[i]%m ]++
}

ans = C[0] * ( C[0]-1) / 2        ⇒ C0 = 0

if ( M%2 == 0 ) {
      ans += C[M/2] * (C[M/2] - 1) / 2      } M/2
}
```

```
for ( 1 → ceil(M/2)-1 ) {
        ans += c[i] * c[M-i]
}
return ans;
```

T.C ⇒ O(N + M)

S.C ⇒ O(M)

---

4) $(a^b) \% m \Rightarrow ((a \% m)^b) \% m$

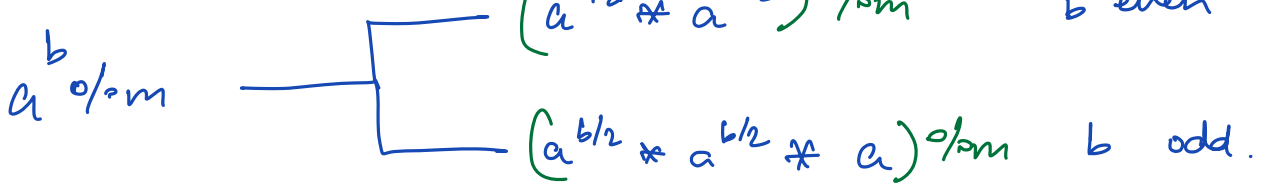
⇒

```
ans = 1
for ( i → 1 to b )
{
   ans = ans * a
}
return ans % m
```

⇒ Overflow

```
ans = 1      a = a%m
for ( i → 1 to b )
{
   ans = (ans * a)%m  →  ((ans %m) * (a %m)) %m
}
return ans %m
```

```
ans = 1      a = a%m
for ( i → 1 to b )
{
   ans = (ans * a)%m
}
return ans
```



Recursive soln

```
int solve ( a, b, m)
{
    if ( b == 0 )  return 1

    x = solve ( a, b/2, m)
    if( b%2 == 0)  // even
        return  (x * x)%m
    else
        return  (x * x * a)%m      <- careful

}
```

T.C
S.C

Fermat's Theorem

$$a^{P-1} \equiv 1 \pmod{p}$$

congruent — prime number.

$$x \equiv y \pmod{m} \Rightarrow \boxed{x\%m = y\%m}$$

$$\Rightarrow a^{P-1} \equiv 1 \pmod P$$

$$\Rightarrow a^{P-1} * a^{-1} \overset{(\text{mod } P)}{\equiv} 1 * a^{-1} \pmod P$$

$$a^{P-2} \equiv a^{-1} \pmod P$$

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

a^{-1} → inverse of a w.r.t to P

eg: $(2^{-1}) \% 7 \Rightarrow (2^{7-2}) \% 7 \Rightarrow 2^5 \% 7 = 4$

$\Rightarrow \quad 2 \Rightarrow \frac{1}{2}$

$3 * ? \equiv 1 \pmod 5$

Ans = 2

$2 * ? \equiv 1 \pmod{11}$

Ans = 6

Q What when multiplied by x gives remainder as 1 under $\% m$

$x \Rightarrow \boxed{x^{-1}}$ → multiplicative inverse.

$$(2 * x) \equiv 1 \pmod 7$$

$\Rightarrow (2 * x) \% 7 = 1$ → RHS ← LHS = RHS

$$((2 \% 7) * (2^{-1} \% 7)) \% 7$$

$$(2 * (2^{7-2} \% 7)) \% 7 = (2 * 4) \% 7 = 1$$

eg: $3^{1002} \% 11$

$3^{10} \% 11 = 1$

1002

$(3^{10} * 3^{10} * 3^{10} \ldots - \ldots 3^{2}) \% 11$

1 9

9