Modular Arithmetic

→ Content

→ Introduction & Properties
→ Pair sum divisible by M
→ Power & Fast Power Function
→ Inverse mod & Fermat Theorem

Modulo %

$14 \% 5 = 4$

$40 \% 7 = 5$

$A \% B$ = Remainder when A is divided by B

$\{\text{Input}\} \% M = \begin{cases} \text{min} & \text{max} \\ 0 , & M-1 \end{cases}$

A − {multiple of B just smaller than A}

Modular Arithmetic

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

$(0 , 2m-2) \% m$

$[0, m-1]$

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

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

$(12 - 6) \% 5 = (12 \% 5 - 6 \% 5 + 5) \% 5$

$(6) \% 5 = (2 - 1 + 5) \% 5$

$1 \quad = 6 \% 5 = 1$

$a = 13, \; b = 9, \; m = 5$

$= (13 - 9) \% 5 \qquad (13 \% 5 - 9 \% 5) \% 5$

$= (4) \% 5 \qquad (3 - 4) \% 5$

$= (4) \% 5 \qquad (-1) \% 5$

$(-1 \% 5) = -1 \% 5 + 0 \qquad \{0, 4\}$

$= -1 \% 5 + 5 \% 5$

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

$= 4 \% 5 = \underline{\underline{4}}.$

just add 5

multiple of 5 just smaller than -1

$= -1 - (-5)$

$= -1 + 5 = \underline{\underline{4}}.$

Apart from python all languages evaluate negative mod as negative

If after mod value is < 0, add + mod

Q> Given A[N], M, calculate no. of pairs i, j such that

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

NOTE : $i \ne j$ and pair (i, j) is same as pair (j, i)

Eg :

$$A[6] = \{\overset{0}{4}\ \overset{1}{7}\ \overset{2}{6}\ \overset{3}{5}\ \overset{4}{5}\ \overset{5}{3}\} \quad M = 3$$

i	j	A[i]	A[j]	(A[i] + A[j]) % M
0	3	4	5	(4 + 5) % 3 = 0
0	4	4	5	(4 + 5) % 3 = 0
1	3	7	5	(7 + 5) % 3 = 0
1	4	7	5	(7 + 5) % 3 = 0
2	5	6	3	(6 + 3) % 3 = 0

5

Eg :

$$A[7] = \{\overset{0}{13}\ \overset{1}{14}\ \overset{2}{22}\ \overset{3}{3}\ \overset{4}{32}\ \overset{5}{19}\ \overset{6}{16}\} \quad M = 4$$

i	j	A[i]	A[j]	(A[i] + A[j]) % M
0	3	13	3	(16) % 4 = 0
0	5	13	19	(32) % 4 = 0
1	2	14	22	(36) % 4 = 0
4	6	32	16	(48) % 4 = 0

4.

Bruteforce : Check all the pairs, sum % m = 0

TC : $O(N^2)$

SC : $O(1)$

Idea 2 : $(A[i] + A[j]) \% M = 0$

Expand

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

0	0
1	m - 1
2	m - 2
⋮	
K	m - K

Eg :

$M = 4$, $A = 13$, $B \% M = 3$

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

$\Rightarrow (A \% M + B \% M) \% M = 0$

$(13 \% 4 + B \% m) \% M = 0$

$(1 + \underset{m-1}{3}) \% 4 = 0$

$M = 8$, $A = 24$, $B \% M =$

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

$(24 \% 8 + \overbrace{B \% 8}^{0-7}) = 0$

$0 + 0$

$M = 3$, $A = 7$, $B \% M =$

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

$\Rightarrow 7 \% 3 + \{\ \} = 0$

$\Rightarrow (1 + \underset{3-1}{\{\ \}}) \% 3 = 0$

$=$

$M = 10$, $A = 25$, $B \% M =$

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

$\Rightarrow (25 \% 10 + \{\ \}) \% 10 = 0$

$(5 + \{\ \}) \% 10 =$

$10 - 5 = 5$

Eg : $A[7] = \{13 \quad 14 \quad 22 \quad 3 \quad 32 \quad 19 \quad 16\}$ $M = 4$

Are we really interested in values ? A[i] % mod

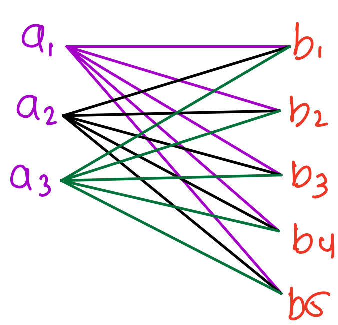
Apply mod 4 $= \{1 \quad 2 \quad 2 \quad 3 \quad 0 \quad 3 \quad 0\}$

$1 \to 3$ $\qquad$ $1 \to 3$

There are 3 values with
— " — 5 — " —

$\boxed{\begin{array}{l} A[i] \% 4 = 1 \\ A[i] \% 4 = 3 \end{array}}$

freq



15 pairs.

$M = 10$

$A[] = \{ 29 \;\; 11 \;\; 21 \;\; 17 \;\; 2 \;\; 5 \;\; 4 \;\; 6 \;\; 23 \;\; 13 \;\; 26 \;\; 14 \;\; 18$
$15 \;\; 30 \;\; 35 \;\; 50 \;\; 20 \;\; 40 \;\; 9 \}$

0	1	2	3	4	5	6	7	8	9
4	2	1	2	2	3	2	1	1	2
30	11	2	13	4	5	6	17	18	29
50	21		23	14	15	26			9
20					35				
40									

M=10

$M=10 : (A[i] \% M + A[j] \% M) \% M = 0$

0   0

freq[1] x freq[9] → 4

freq[2] x freq[8] → 1 x 1 = 1

3   7 → 2

4   6 → 4

5   5 → 3

~~6   4~~ Repetition

5   15   30

2   1   0

$$\boxed{{}^{n}C_2 = \frac{n \times n-1}{2}}$$

30   50   20   40

3   2   1   0   = 6

```
int   pairSumM ( A[] , M) {
      // Step 1    Create freq array
       freq [M]  // init.

      for( i -> 0 to n-1) {
      |     val = A[i]
      |     freq [val % M] ++
      }
       // Edge case  0
       count = 0
       x = freq[0]
       count = count + x(x-1)/2

        // Edge case same value
        if (M%2 ==0) {
        |    x = freq[m/2]
        |    count = count + x(x-1)/2
        }

        l = 1  , r = M-1

        while ( l < r ) {
        |     count += freq[l] * freq[r]
        |      l++;
        |      r--;
        }                          TC : O(N+M)
        return count ;             SC : O(M)
}
```

Fast Power Function

Break : 8:35

$2^{32}-1$

$2^3 = 2 \times 2 \times 2$

$2^{20} = 2 \times 2 \times 2 \ldots \}$ 20 times.

2^{33} = overflow

MOD = $1e9 + 7$ → prime no.

$\Rightarrow \quad a^p \% m$

$\Rightarrow \quad 2^{1000} \% m = \cancel{(\underbrace{2 \times 2 \times \ldots\ldots 2}_{1000})} \% m.$

$= ((\underbrace{2 \times 2) \% m \times 2 \ldots\ldots}_{1000.}) \% m$

$2^{1000000} \% m$ → for loop will TLE.

$2^{10} \longrightarrow 2^5 \times 2^5$

$2 \times 2^2 \times 2^2 \qquad\qquad 2 \times 2^2 \times 2^2$

$2^1 \times 2^1 \qquad 2^1 \times 2^1 \qquad\qquad 2^1 \times 2^1 \qquad 2^1 \times 2^1$

```
long power ( long a, long p ) {
    if( p == 0) {
        return 1
    }
    half = power(a, p/2 , m)

    if( p % 2 == 0 ) {
        return half x half
    }
    else {
        return a * half * half
    }
}
```

TC: log(p) *

SC: log(p).

```
long fastPower ( long a, long p, long m ) {
    if( p == 0) {
        return 1
    }
    half = power(a, p/2 , m) % m

    if( p % 2 == 0 ) {
        return (half x half) % m
    }
    else {
        return ((a * half) % m * half) % m.
    }
}
```

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

Eg: $a = 10$, $b = 5$, $m = 10$

LHS

$2 \% 10$

$\underline{\underline{2}}$

RHS

$a\%m = 10\%10 = 0$

$b\%m = 5\%10 = 5$

$\underline{\underline{0}}$

$a * x = 1$ $\quad\quad x = 1/a$

$a + x = 0$ $\quad\quad x = -a$

$$(a/b) \% m = (a \times \frac{1}{b}) \% m$$

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

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

Inverse modulo.

$\Rightarrow$ $(1) \% m = 1$

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

$\Rightarrow$ $((b\%m) * (b^{-1} \% m)) \% m = 1$

1. $\gcd(b, m) = 1$
2. $m > 1$

Eg : $b = 10$, $m = 7$, $b^{-1} \% 7 = 5$

$\gcd(10, 7) = 1$ ✓

$7 > 0$ ✓

$\Rightarrow ((10 \% 7) * (b^{-1} \% 7)) \% 7 = 1$

$\Rightarrow (3 * \underbrace{(b^{-1} \% 7)}_{[1,\ 6]}) \% 7 = 1$

Substitute 1 $(3 * 1) \% 7 = 1$ ✗

Substitute $(3 * 2) \% 7 = 1$ ✗

Substitute $(3 * 3) \% 7 = 1$ $9 \% 7 = 2$ ✗

$(3 \times 4) \% 7 = 1$ $12 \% 7 = 5$

$(3 \times 5) \% 7 = 1$

NOTE : b^{-1} mod m will be in range [1, M-1] since 0 can never be an answer

```
int inverseMod ( b , m ) {

    for (inv -> 1 to m-1) {
        if(((b % m)* inv) % m == 1 ) {
            return inv
        }

    return -1 ;
}
```

TC : O(M)

SC : O(1)

Fermat's Little Theorem

Given b, m, $\gcd(b,m) = 1$, m is prime, $m > 1$

$$b^{m-1} \% m = 1$$

apply $b^{-1} \% m$

$$\Rightarrow \quad b^{-1} * b^{m-1} \% m = b^{-1} \% m$$

$$\Rightarrow \quad \boxed{b^{m-2} \% m = b^{-1} \% m}$$

$b = 3 \quad m = 13$

$$\Rightarrow \quad 3^{13-2} = 3^{11} \% 13 = 9$$

TC: $O(\log m)$

use fastPower func.

fastpower(3, 11, 13)

fastPower(a, p, m)

$b = 3 \qquad m = 13$

$$((3 \% 13) * \boxed{(3^{-1} \% 13)}) = 1$$

$(1 \rightarrow 12)$

$\Rightarrow \quad (3 \times 1) \% 13 = 1 \; ..$

$\vdots$

$(3 \times 9) \% 13 = 27 \% 13 = 1$

fast power (3, 11, 13)