Lecture : Modular Arithmetic

online test.

Agenda

- Introduction and properties.
- $a^n \% m$
- Pairs having sum $\% m = 0$
- Inverse modulo.

Introduction

% $\Rightarrow$ Modulo operator

a % b $\Rightarrow$ Remainder when b divides a.

Range of a % b $\Rightarrow$ [0, b-1]

a % 21 $\Rightarrow$ [0, 1, ... 20]

21
2
41

Qu. Why do we need % ?

Limit the range of data.

int $\simeq 10^9$

long $\simeq 10^{18}$

BigInteger $\simeq 10^{100}$

$10^{108} \longrightarrow$ Memory overflow

10^{108} % __5__ $\simeq$ [0, 1, 2, 3, 4]

Properties of %

1) $(a + b) \% m \Rightarrow (a \% m + b \% m) \% m.$

Example: $a = 3$

$b = 4$

$m = 5$

LHS: $(3 + 4) \% 5 \Rightarrow 7 \% 5 \Rightarrow 2$

RHS: $(3 \% 5 + 4 \% 5) \% 5 \Rightarrow 2.$

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

3) $(a + m) \% m \Rightarrow (a \% m + m \% m) \% m$

$\Rightarrow (a \% m + 0) \% m$

$\Rightarrow (a \% m) \% m$

$\Rightarrow a \% m.$

4:> $(a-b)\%m \Rightarrow (a\%m - b\%m)\%m$ [wrong]

Example $a = 17$

$b = 8$

$m = 5$

LHS: $(17-8)\%5 \Rightarrow 4$

RHS: $(17\%5 - 8\%5)\%5$

$(2 - 3)\%5$

$-1\%5$

$-1 + 5 = \boxed{4} = LHS.$

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

5:> $a\%m \Rightarrow (((a\%m)\%m)\%m)\%m)$ ....

6:> $a^b\%m \Rightarrow \{(a\%m)^b\}\%m$

Ex: $a = 7$

$b = 3$

$m = 3$

LHS: $(7^3)\%3 \Rightarrow 343\%3 = 1$

RHS: $(7\%3)^3\%3$

$1^3\%3 = 1$

Qu Calculate the value of $a^n \% m$.

Constraints $1 <= a <= 10^9$

$1 <= n <= 10^5$

$1 <= m <= 10^9 + 7$

Iterative approach

Worst case

$ans = a^n$

$\Rightarrow (10^9)^{10^5}$

- int X
- long X
- BigInteger X

```
int solve(int a, int n, int m) {
    long ans = 1;    // int crossed out, replaced by long
    for( i=1 ; i<=n ; i++) {
        ans = ans * a;   X
        ans = (ans % m * a % m) % m   ✓
    }
    return (int) ans % m;
}
```

$\underbrace{ans \% m * a \% m}$ never exceed $(10^9 * 10^9)$

max value of ans % m ; a

$\simeq 10^{18}$ (long)

TC: O(n)

SC: O(1)

Recursive approach

int power(int a, int n, int m) {

    if(n==0) {

        return 1;

    }

    int sa = power(a, n-1, m);

long ~~int~~ ans = sa * a; X (sa%m * a%m)%m ✓

    return (int)ans % m;

}

a^n

sa * a

sa = a^{n-1}

TC: O(n)

SC: O(n)

Stack space.

<u>Quiz</u> $(37^{103} - 1) \% 12 \Rightarrow$

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

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

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

$(\cancel{1} \quad -\cancel{1} \quad + 12) \% 12 = \boxed{0}$ <u>Ans</u>

Optimised approach

int power(int a, int n, int m) {

1 if (n == 0) {

return 1;

}

2 int sa = power(a, $\frac{n}{2}$, m);

3 if(n % 2 == 0) {

long ~~int~~ ans = sa * sa; X

(sa % m * sa % m) % m ✓

return (int) ans % m;

4 } else {

~~int~~ long ans = sa * sa * a; X

(sa % m * sa % m * a % m) % m X

10^9 10^9 10^9 $\simeq 10^{27}$

long temp = (sa % m * sa % m) % m ✓

long ans = (temp % m * a % m) % m

return (int) ans % m;

}

}

TC: O(log n)

SC: O(log n)

Qu Count pairs whose sum % m == 0.

Given A[n], find count of pairs (i, j) such that $(arr[i] + arr[j]) \% m = 0$.

$n <= 10^5$
$A[i] <= 10^9$
$m <= 10^9+7$

Note: i != j and pair(i, j) is same as (j, i).

Example: A =

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

m = 5.

(0, 2)
(0, 3)
(1, 4)
(2, 5)
(3, 5)

Brute force:

TC: $O(n^2)$
SC: $O(1)$

Intuition

$(1+4) \% 5 = 0$ True ✓ false

$(11 + 49) \% 5 = 0$ true ✓ false

$\underset{\substack{\uparrow \% 5 \\ 1}}{11} + \underset{\substack{\uparrow \% 5 \\ 4}}{49}$

$(131 + 434) \% 5 = 0$ true ✓ false

$\underset{\substack{\uparrow \% 5 \\ 1}}{131} + \underset{\substack{\uparrow \% 5 \\ 4}}{434}$

$(1032 + 8393) \% 5 = 0$ true ✓ false

$\underset{\substack{\uparrow \% 5 \\ 2}}{1032} + \underset{\substack{\uparrow \% 3 \\ 3}}{8393}$

Generalisation for $m = 5$

$(a+b) \% 5 = 0$

$a \% 5 = 0$	$b \% 5 = 0$	(true)
$a \% 5 = 1$	$b \% 5 = 4$	(true)
$a \% 5 = 2$	$b \% 5 = 3$	(true)
$a \% 5 = 3$	$b \% 5 = 2$	(true)
$a \% 5 = 4$	$b \% 5 = 1$	(true)

same

same

Duplicates

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	8	6	15	5	12	17	7	18	10	9	16	21

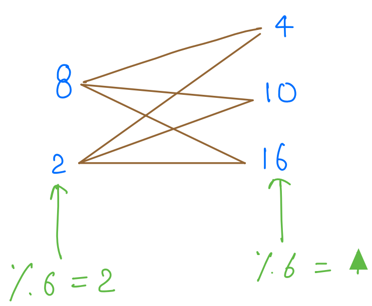
$m = 6$

After doing $\% 6$ —

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	2	0	3	5	0	5	1	0	4	3	4	3

Remainders :- 0, 1, 2, 3, 4, 5

0	1	2	3	4	5
3	1	2	4	3	2



Dry run:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	8	6	15	5	12	17	7	18	10	9	16	21

$m = 6$

After doing mod with 6, we get –

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	2	0	3	5	0	5	1	0	4	3	4	3

All possible pairs –

map

int (Rem)	int (freq)
0	3
1	1
2	2
3	4
4	3
5	2

→ rem = 1 and rem = 5 ⇒ $1 * 2 = 2$

a % 6 (1)   b % 6 (2)

→ rem = 2 & rem = 4 ⇒ $2 * 3 = 6$

(2)   (3)

→ rem = 3 & rem = 3 ⇒ $4 * 4 = 16$ ✗

(4)   (4)

3, 15, 9, 21 ⟹ (3,15) (15,9) (9,21) (3,9) (15,21) (3,21)

$^{4}C_{2} \Rightarrow \frac{\cancel{4}^{2} * (4-1)}{\cancel{2}} = 2 * 3 = 6$ ✓

$^{n}C_{2} \Rightarrow \frac{n(n-1)}{2}$

→ rem = 0 & rem = 0

$^{3}C_{2} = \frac{3 * (3-1)}{2} = \frac{3 * \cancel{2}}{\cancel{2}} = 3$

6, 12, 18 ⟹ 6, 12; 6, 18; 12, 18

Algorithm

```
int countPairs(int[] arr, int m) {
        Map<Integer, Integer> map = new HashMap<>();
        for (int el : arr) {
                int rem = el % m;
                if (map.containsKey(rem)) {
                        int freq = map.get(rem);
                        map.put(rem, freq+1);
                } else {
                        map.put(rem, 1);
                }
        }
      // if rem = 0, handle it alone.
      int freq0 = map.containsKey(0) ? map.get(0) : 0;
      int ans = freq0 * (freq-1) / 2 ;

      int l = 1
      int r = m-1;
      while(l < r) {
          int freql = map.containsKey(l) ? map.get(l) : 0;

          int freqR  map.containsKey(r) ? map.get(r) : 0;

          ans = ans + (freql * freqR);

          l++;
          r--;
      }
      if (l == r) {
          int freql = map.containsKey(l) ? map.get(l) : 0;
              ans += freql * (frel-1) / 2 ;
      }
      return ans;
}
```

TC: O(n)

SC: O(m)

Break: 8:39 : 8:50

Inverse Modulo

* $\frac{a}{b} \% m = \left(\frac{a \% m}{b \% m} \right) \% m$ [wrong]

Eg: $a = 16$

$b = 4$

$m = 5$

LHS: $\frac{16}{4} \% 5 = 4$

RHS: $\left(\frac{16 \% 5}{4 \% 5} \right) \% 5 = \left(\frac{1}{4} \right) \% 5 = 0 \% 5 = 0$

Correct formula

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

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

How do we find $b^{-1} \% m$?

Inverse modulo.

The value of $b^{-1} \% m$ only exists if $\gcd(b, m) = 1$, $\underline{m > 1}$

(Proof is not needed)

$\Rightarrow b^{-1} \% m \longrightarrow$ To find

$\Rightarrow \quad b * \frac{1}{b} = 1$? — Assuming

$b * b^{-1} = 1$

Take $\% m$ both side

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

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

range $= [0, m-1]$ X

$[1, m-1]$ ✓

Iterate from 1 to m-1, and check if condⁿ holds true.

$b = 10 \quad m = 7 \quad b^{-1} \% m = 5$ Ans

iterate 1 — 6

$i = 1 \quad (10 \% 7 * 1) \% 7 = 3$

$i = 2 \quad (10 \% 7 * 2) \% 7 = 6$

$i = 3 \quad (10 \% 7 * 3) \% 7 = 2$

$i = 4 \quad (10 \% 7 * 4) \% 7 = 5$

$i = 5 \quad (10 \% 7 * 5) \% 7 = 1 = \text{RHS}$

* fermat little theorem

① Given b & m –

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

② if m is prime

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

$b = 3$

$m = 29$

$3^{28} \% 29 = 1$

Thankyou ☺