Modular Arithmetic

Today's content

1. % operator
2. Modular arithmetic
3. One hard problem

Range

int x : $[-2 \times 10^9, 2 \times 10^9]$

long y : $[-9 \times 10^{18}, 9 \times 10^{18}]$

% Basics (modular basics)

n % a = remainder when n is divided by a

r = dividend − (greatest mul. of a <= dividend)

10 % 4 = 2 = 10 − (greatest mul. of 4 <= 10)

= 10 − 8 = 2

13 % 5 = 3 = 13 − 5×2 = 3

remainder = dividend − divisor × quotient

quotient ↓ greatest multiple of divisor <= dividend

$150 \% 11 = r$

$r = 150 - (\text{greatest mul of } 11 <= 150)$

$11 \times 13 = 143$

$11 \times 14 = 154 > 150$

$= 150 - 143 = 7$

$100 \% 7 = r$

$r = 100 - (\text{greatest mul of } 7 <= 100)$

$100 - 98 = 2$

$7 \times 14 = 98$

$-40 \% 7 = r$

$r = -40 - (\text{greatest mul of } 7 <= -40)$

$7 \times -5 = -35 > -40$

$7 \times -6 = -42$

$= -40 - (-42)$

$= -40 + 42 = 2$

$-60 \% 9 = r$

$r = -60 - (\text{greatest mul of } 9 \text{ } <= -60)$

$= -60 - (-63)$

$= -60 + 63 = 3$

Modulo always returns a positive value.

Why %. ?

% limits the input data to required range

↳ Hashing : & coming claim }

$+\infty$
14
289
2581
20
$-\infty$

$\} \% 10 =$ 4, 9, 1, 0

$= [0, 9]$

$-\infty$ to $+\infty$ $\} \% p = [0, p-1]$

Modular Arithmetic

$(a+b) \% p = [a \% p + b \% p] \Rightarrow [0, 2p-2]$ ✗

($a \% p$: $[0, p-1]$, $b \% p$: $[0, p-1]$)

$(a+b) \% p = [a \% p + b \% p] \% p \Rightarrow [0, p-1]$

$p = 10 \qquad a = 29,\ b = 13$

$(29 + 13) \% 10 = 42 \% 10 = 2$

$[29 \% 10 + 13 \% 10] \% 10 = [9 + 3] \% 10 = 12 \% 10 = 2$

$(a \times b) \% p = a \% p \times b \Rightarrow [0, (p-1)b]$ ✗ ($a \% p \in [0, p-1]$)

$= (a \% p \times b \% p)$ ✗

$\boxed{(a \times b) \% p = (a \% p \times b \% p) \% p} \Rightarrow [0, p-1]$

$(a - b) \% p$

$(a / b) \% p$

→ Advanced Batch

$a = 23 \quad b = 15 \quad p = 5$

$(23 \times 15) \% 5 = 375 \% 5 = 0$

$(23 \% 5 \times 15 \% 5) \% 5 = (3 \times 0) \% 5 = 0 \% 5 = 0$

CHECK?

1. $(a \% p) \% p \equiv a \% p \rightarrow [0, p-1]$ ✓✓

$(a \% p) \% p$: $(a \% p) \rightarrow [0, p-1]$, $\% p \rightarrow [0, p-1]$

2. $(a \% p \times b) \% p \equiv (a \times b) \% p$ ✓✓

$(a \% p \times b) \% p \rightarrow ((a \% p) \% p \times b \% p) \% p$

$(a \% p \times b \% p) \% p$

$(a \% p \times b \% p) \% p$

Quiz: Number not divisible by 3 ?

231, 4562, 7821, 1026

sum of digit should by multiple of 3

$4+5+6+2 = 17 \% 3 = 2 \neq 0$

$2+3+1 = 6 \% 3 = 0$

$7+8+2+1 = 18 \% 3 = 0$

$1+0+2+6 = 9 \% 3 = 0$

Proof for %3 → sum of the digits

$$(2475)\%3 = (2\times10^3 + 4\times10^2 + 7\times10^1 + 5\times10^0)\%3$$

$$= [(2\times10^3)\%3 + (4\times10^2)\%3 + (7\times10^1)\%3 + (5\times10^0)\%3]\%3$$

$$= [(2\times1)\%3 + (4\times1)\%3 + (7\times1)\%3 + (5\times1)\%3]\%3$$

observations :

$$= [2 + 4 + 7 + 5]\%3$$

$10^0 \%3 = 1$

$10^1 \%3 = 1$

$10^2 \%3 = 1$

$10^3 \%3 = 1$

⋮

Proof for %4 → last 2 digits

$$(2457)\%4 \Rightarrow 57\%4 = 1$$

$$(2457)\%4 = [(2\times10^3)\%4 + (4\times10^2)\%4 + (5\times10^1)\%4 + (7\times10^0)\%4]\%4$$

observations

$$= [50 + 7]\%4$$

$10^0 \%4 = 1$

$10^1 \%4 = 2$

$10^2 \%4 = 0$

$10^3 \,\%\, 4 = 0$

$\vdots$

Proof for % 8 → last 3 digits

$10^2 \,\%\, 8 = 2 \neq 0$

$(2457) \,\%\, 8 \Rightarrow (457) \,\%\, 8$

$10^3 \,\%\, 8 = 0$

$10^4 \,\%\, 8 = 0$

$\vdots$

Proof for % 9 → Sum of the digits

$10^0 \,\%\, 9 = 1$

$10^1 \,\%\, 9 = 1$

$10^2 \,\%\, 9 = 1$

$10^3 \,\%\, 9 = 1$

$\vdots$

$(2475) \,\%\, 9 = (2+4+7+5) \,\%\, 9$

Divisibility Rules

2, 3, 4, 5, 6, 7, 8, 9

6 ↓ 2 & 3

7 → TODO

Question 1

Given a, n, p. Calculate $a^n \% p$ without inbuilt function.

Constraints: $1 <= a <= 10^9$, $2 <= p <= 10^9$

$1 <= n <= 10^5$

$a^n \% p = (a \times a \times a \ldots \text{n times} \times a) \% p$

```
int ans=1
for (i=0; i<n; ++i){
    ans = ans * a;
}                          // after the for loop
return ans%p;
```

ans = a^n

$= (10^9)^{10^5} = 10^{9 \times 10^5}$ — Overflow

long: 9×10^{18}

what if p = 1719855

Can't use divisibility rule

$ans = (a \times a \times a \ldots \times a) \% p$

$= (((a \times a) \% p \times a) \% p \ldots)$

```
int → long
ans = 1
for (i=0; i<n; ++i) {
    ans = (ans * a) % p
}
return ans
```

$p = 10^9$

max value

$10^9 \times 10^9 = 10^{18}$

[0, p-1]

[0, p-1]

TC: O(N) SC: O(1)

Question 2

Given a number in an array format.

Calculate a[] % p. → each a[i] represents a single digit of a number.

Constraints: $1 <= N <= 10^5$

$0 <= a[i] <= 9$

$2 <= p <= 10^9$

eg N = 5 a[5] = | 6 | 2 | 3 | 4 | 5 | p = 49

(62345) % 49

Ideal : Convert a[] → number and take % p

N = 2 : 9 9 $= 10^2 - 1$

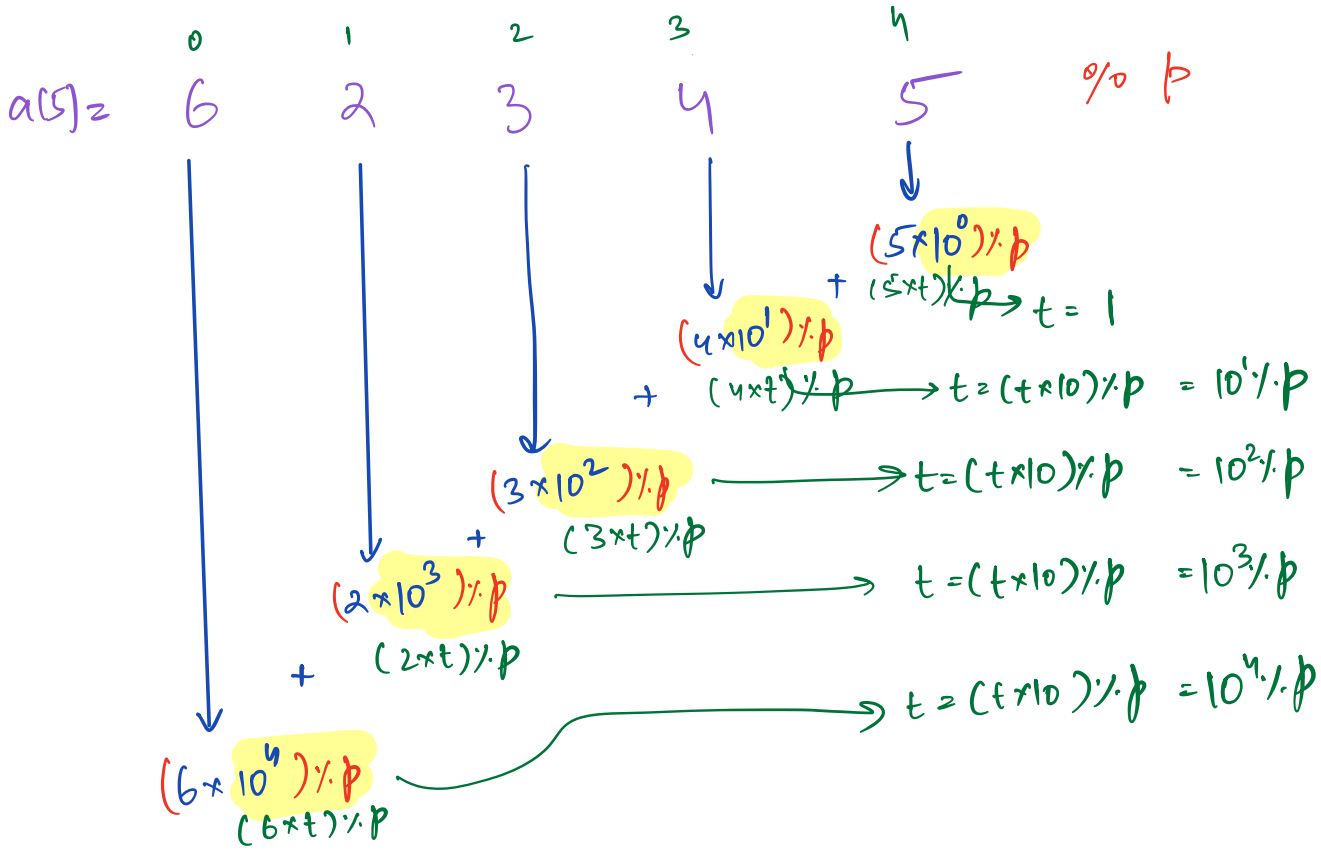
N = 3 : 9 9 9 $= 10^3 - 1$

⋮

N = 10^5 : $10^{10^5} - 1$

↳ storing in int/long not possible

Hint : Calculate modulo digit by digit



Code

```
def arrmod(a[], p) {
    n = a.length
    long ans = 0
    long t = 1
    for(i=n-1; i>=0; --i) {
        int x = (t * a[i]) % p        // [0,p-1] -> 9
        ans = (ans + x) % p           // [0,p-1] -> [0,p-1]
        t = (t * 10) % p
    }
    return ans
}
```

Max values

$\Rightarrow 9 \times (p-1) = 9 \times 10^9$

$\Rightarrow 10^9 + 10^9 \approx 2 \times 10^9$

$\Rightarrow 10^9 \times 10 = 10^{10}$

TC: O(N)

SC: O(1)

a = [1 3 4 5] p = 20

ans = (0 + 5) % 20 = 5

ans = (5 + 4 × 10) % 20

= (5 + 40 % 20) % 20 = 5 % 20

ans = (5 + (3 × 100) % 20) % 20

= (5 + 0) % 20 = 5