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 multiple of a <= dividend)

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

10 - 8 = 2

13 % 5 = 3 13 - 5 × 2 = 13 - 10 = 3

remainder = dividend - divisor × quotient

$150 \% 11 = r$

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

$11 \times 13 = 143$

$11 \times 14 = 154 > 150$

$= 150 - 143 = 7$

$100 \% 7 = r$

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

$= 100 - 98 = 2$

$7 \times 14 = 98$

$-40 \% 7 = r$

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

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

$7 \times -6 = -42 <= -40$

$r = -40 - (-42)$

$\therefore -40 + 42 = 2$

$-60 \% 9 = r$

$r = -60 - (-63)$ (not -54)

$= -60 + 63 = 3$

Modulo always returns a positive value

Why %?

% limits input data to a required range.

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

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

$[0, 9]$

$\left.\begin{matrix} +\infty \\ -\infty \end{matrix}\right\} \% p = [0, p-1]$

Popular application: Hashing

&

future class

Modular arithmetic

$(a+b)\%p \quad \neq \quad (a\%p + b\%p)$

$(a+b)\%p$ → $[0, p-1]$

$(a\%p + b\%p)$ → $[0, p-1]$ $[0, p-1]$ ⇒ $[0, 2p-2]$

$$\boxed{(a+b)\%p = (a\%p + b\%p)\%p}$$

$(a\%p + b\%p)\%p$ → $[0, p-1]$

Eg $p=10 \quad a=29, \; b=13$

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

$(a\%p + b\%p) = (29\%10 + 13\%10) = 9+3 = 12$

$(a\%p + b\%p)\%p = 12\%10 = 2$

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

$[0, p-1]$ = $(a\%p \times b\%p)$ ✗ ⇒ $[0, (p-1)^2]$

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

eg $p=10 \quad a=9 \quad b=8$

$(a \times b) \% p = (9 \times 8) \% 10 = 72 \% 10 = 2$

$(a\%p \times b\%p) = (9\%10 \times 8\%10) = 9 \times 8 = 72$

$(a\%p \times b\%p)\%p = 72\%10 = 2$

$(a-b)\%p$
$(a/b)\%p$
} → Advance batch

CHECK ?

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

$(a\%p)$ → $[0, p-1]$; $\%p$ → $[0, p-1]$

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

$(a\%p \times b)\%p$ ⇓

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

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

$(a \times b)\%p$ ⇓

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

↔

Number Not Divisible by 3 ?

231 , 4562 , 7821 , 1026

sum of digits should be multiple of 3.

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

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

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

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

Proof for %3 → sum of all digits

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

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

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

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

observation:

$10^0 \%3 = 1$

$10^1 \%3 = 1$

$10^2 \%3 = 1$

⋮

Proof for %4 → last 2 digits

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

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

($(2\times10^3)\%4 \to 0$, $(4\times10^2)\%4 \to 0$)

$= [50+7]\%4 = 57\%4$

observations:

$10^0\%4 = 1$

$10^1\%4 = 2$

$10^2\%4 = 0$

$10^3\%4 = 0$

⋮

Proof for %8 → last 3 digits

$10^0\%8 = 1$

$10^1\%8 = 2$

$10^2\%8 = 4$

$10^3\%8 = 0$

$10^4\%8 = 0$

⋮

$(2457)\%8 = 457\%8$

Proof for %.9 → sum of digits

$10^0 \%.9 = 1$

$10^1 \%.9 = 1$

$10^2 \%.9 = 1$

⋮

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

Divisibility Rules

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

6 → 2 & 3

7 → TODO

Question1

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

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

$1 <= p <= 10^9$

$1 <= n <= 10^5$

$a^n \%.p = (a \times a \times a \ldots \times a) \%.p$

n times

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

$ans = a^n$

$= (10^9)^{10^5}$

$= 10^{9 \times 10^5}$

overflow

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

ans: max 10^9

a: max 10^9

result: $[0, p-1]$

$max\ p = 10^9$

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

Can't be stored in integer

Use long

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

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

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

Question 2

Given a number in an array format.

Calculate a[] % p.

↳ each a(i) represent a single digit of a number.

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

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

$1 <= p <= 10^9$

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

$\Downarrow$

$(62345) \% 49$

Idea 1 : Convert a[] → number and take % p

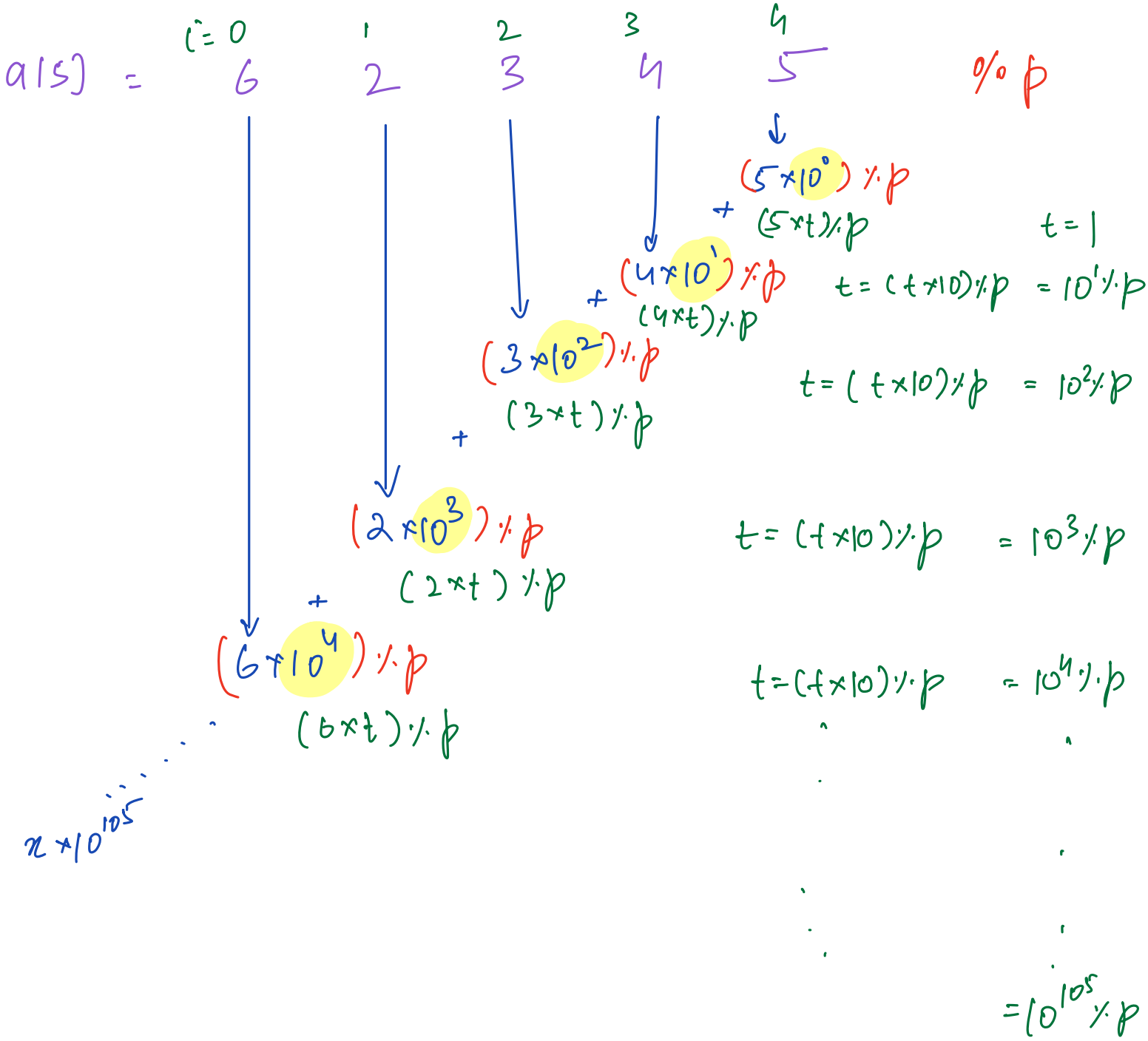
$n=2$: 9 9 $= 10^2 - 1$

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

⋮

$n=10^5$: $10^{10^5} - 1$ ⇒ storing in int / long is NOT POSSIBLE

Hint: Calculate modulo digit by digit



Code

```
def arrMod(a[], p) {
    n = a.length
    int ans = 0
    long t = 1

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

max values

$\Rightarrow 9 \times 10^9$ → need long

$\Rightarrow 10^9 + 10^9 \Rightarrow 2 \times 10^9$ → int is fine

$\Rightarrow 10^9 \times 10 = 10^{10}$ → need long

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

Doubt

$A \wedge X + B \wedge X$ A, B given

X to minimize

$a =$ 1 0 0 0 1 1 0 1

$b =$ 0 0 1 1 0 1 1 0

$X =$ 1,0 0 0,1 0,1 0,1 1 0,0 0,1

$=$ 0 0 0 0 0 1 0 0 ✓

$=$ 1 0 1 1 1 1 1 1 ✓

$a \wedge b =$ 1 0 1 1 1 0 1 1

$a \& b =$ 0 0 0 0 0 1 0 0