Lecture : Modular arithmetic

Agenda

- % operator
- Modular arithmetic basics
- $a^n \% p$
- arr[ ] % p.

I will solve some mystery today and I will create some

class starts at 7:05 AM

Range

Approx

int: -2^{31} to $2^{31}-1$ — $-2 * 10^{9}$ to $2 * 10^{9}$

long: -2^{63} to $2^{63}-1$ — $-8 * 10^{18}$ to $8 * 10^{18}$

% basics:

$n \% a$ = remainder when n is divided by a.

$[0, a-1]$

Maths: Remainder is always +ve.

Another dimension of %

dividend = divisor * quotient + remainder.

remainder = dividend − divisor * quotient.

remainder → +ve

divisor * quotient → divisor * quotient <= dividend

divisor * quotient → multiple of divisor.

remainder = dividend − [multiple of divisor <= dividend]

multiple of divisor → greatest multiple.

Ex: $10 \% 4 = 10 - [\text{multiple of } 4 <= 10]$

$= 10 - 8 = 2.$

$13 \% 5 = 13 - [\text{multiple of } 5 <= 13]$

$= 13 - 10 = 3.$

rem = dividend − [greatest multiple of div <= dividend]

150 % 11 = 150 − [greatest multiple of 11 (<=150)]

= 150 − [143] = 7.

100 % 7 = 100 − [98] = 2.

−40 % 7 = −40 − [greatest multiple of 7 <= −40]

= −40 − [−42] = 2.

−60 % 9 = −60 − [−63] = 3.

Trivia

	Python	Java | C | C++ | C#
−40 % 7	2	−5
−60 % 9	3	−6

```
int calcRem(int n, int p) {
    int rem = n % p    // n = -60, p = 9, java: rem = -6
    if (rem < 0) {
        rem = rem + p; ] — Try to prove it why it works?
    }
    return rem;
}
```

Q Why % ? [return ans % $10^9 + 7$]

→ limit our output to required range.

Ex: find ($n!$ % $10^9 + 7$) → [0 , $10^9 + 7 - 1$]

1. int ans = $n!$

2. return ans % $10^9 + 7$.

$n = 10^6$.

$n! = 10^6!$ — int ✗, long ✗

Properties of % [Resolve issues such as n!]

1. $(a + b) \% p = (a \% p + b \% p) \% p$

a	b	p
8	6	10

LHS: $(a + b) \% p = (8 + 6) \% 10 = 4$

RHS $(a \% p + b \% p) = 8 \% 10 + 6 \% 10$

$= 8 + 6 = 14$ $\neq$ LHS

RHS $(a \% p + b \% p) \% p = 14 \% 10 = 4 =$ LHS.

2.) $(a * b) \% p = (a \% p * b \% p) \% p$

3.) $(a * b * c * d \text{ - - - -}) \% p =$

$[a \% p * b \% p * c \% p * d \% p \text{ - - - - - - - - - -}] \% p$

4) $(a - b) \% p$

5.) $(a / b) \% p$ — Advanced Module

6.) $(a \wedge b) \% p$

* $(a \% p) \% p = a \% p$

Lets say $\Rightarrow a \% p = x$

<u>RHS</u> $a \% p = x \quad [0 - p-1]$

<u>LHS</u> $(a \% p) \% p$

$\uparrow$

$\underbrace{x}_{\text{less than } p} \% p = x$

LHS = RHS, Hence proved.

$10 \% 20 = 10$

$5 \% 82 = 5.$

$a \% b = a$

$\uparrow$

$a < b$

* $(a \% p * \underbrace{b}_{b \% p \text{ is missing}}) \% p = (a * b) \% p$

Lets say $a \% p = x$

$b = y.$

<u>LHS</u> $(x * y) \% p$

$(x \% p * y \% p) \% p$

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

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

$(a * b) \% p = RHS.$

$(100 \% 50) \% 50$

$\downarrow$

$100 \% 50$

Divisibility rules

1.) $\% 3 \Rightarrow$ (sum of all digits) $\% 3 == 0$

divisible by 3.

Ex: $(2853) \% 3$

Check $2+8+5+3 = 18 \% 3 == 0$, divisible by 3.

Proof: $(2853) \% 3$

$\Rightarrow [2 * 10^3 + 8 * 10^2 + 5 * 10^1 + 3 * 10^0] \% 3$

$\Rightarrow [(2 * 10^3) \% 3 + (8 * 10^2) \% 3 + (5 * 10^1) \% 3 + (3 * 10^0) \% 3] \% 3$

$\Rightarrow [(2 \% 3 * 10^3 \% 3) \% 3 + (8 \% 3 * 10^2 \% 3) \% 3 +$

$(5 \% 3 * 10^1 \% 3) \% 3 + (3 \% 3 * 10^0 \% 3) \% 3] \% 3$

observation

$10^0 \% 3 = 1$

$10^1 \% 3 = 1$

$10^2 \% 3 = 1$

$10^3 \% 3 = 1$

⋮

$10^n \% 3 = 1$.

$\Rightarrow [(2 \% 3) \% 3 + (8 \% 3) \% 3 + (5 \% 3) \% 3 + (3 \% 3) \% 3] \% 3$

$\Rightarrow [2 \% 3 + 8 \% 3 + 5 \% 3 + 3 \% 3] \% 3$

$(a \% p + b \% p + c \% p + d \% p) \% p = (a + b + c + d) \% p$

$\Rightarrow [2 + 8 + 5 + 3] \% 3$

Hence proved

H|W: % 9 [sum of all digits should be divisible by 9]

2.) % 4 [last two digits should be divisible by 4]

Ex: 24 → Yes

124 → Yes

8008 → Yes

proof: $(2853)\ \%\ 4 = $ NO

$[2 * 10^3 + 8 * 10^2 + 53]\ \%\ 4$

$[(2 * 10^3)\ \%\ 4 + (8 * 10^2)\ \%\ 4 + 53\ \%\ 4]\ \%\ 4$

$[(2\ \%\ 4 * 10^3\ \%\ 4)\ \%\ 4 + (8\ \%\ 4 * 10^2\ \%\ 4)\ \%\ 4 + 53\ \%\ 4]\ \%\ 4$

observation

$100\ \%\ 4 = 0$

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

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

⋮

$10^n\ \%\ 4 = 0$

$[n >= 2]$

$\Rightarrow [0 + 0 + 53\ \%\ 4]\ \%\ 4$

$\Rightarrow (53\ \%\ 4)\ \%\ 4$

$\Rightarrow 53\ \%\ 4$

Hence proved.

Qu1 Given a, n, p, calculate $a^n \% p$.

Constraints: Do not use inbuilt func.

$1 <= a <= 10^9$

$1 <= p <= 10^9$

$1 <= n <= 10^5$

Ex:

a	n	p
3	4	7

$= 3^4 \% 7 = 81 \% 7 = 4.$ Ans

straight forward approach

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

Issues

$a = 10^9$, $n = 10^5$

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

out of range [ans]

$ans = (a * a * a * a ----- n \text{ times}) \% p$

$ans = [\underbrace{(a \% p)}_{\substack{p-1 \\ 10^9}} * \underbrace{(a \% p)}_{\substack{p-1 \\ 10^9}} * \underbrace{(a \% p)}_{\substack{p-1 \\ 10^9}} * \underbrace{(a \% p)}_{\substack{p-1 \\ 10^9}} .... n \text{ times}] \% p$

Overflow

ans = 1.

1st itr   ans = (ans * a) % p $\in [0, p-1]$

2 itr   ans = $(\underbrace{ans}_{p}$ * $\underbrace{a}_{10^9}$) % p

10^9

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

$[0, p-1]$ a $\simeq 10^9 * 10^9 = 10^{18}$

suggestion   If in any doubt, apply % [condition :- Question demands it]

TC : O(n)

SC : O(1)

Qu Given arr[n], calculate arr[] % p

arr[] — represents a number.

arr[5] = [6 2 3 4 3] , p = 49

62343 % 49 = $\boxed{15}$ Ans.

Constraints

$1 <= n <= 10^5$

$1 <= arr[i] <= 9$

$1 <= p <= 10^9$

$$\begin{array}{cccccc} & 4 & 3 & 2 & 1 & 0 \\ arr[\,] = & [\,6 & 2 & 3 & 4 & 3\,] \end{array}$$

$num = 6 * 10^4 + 2 * 10^3 + 3 * 10^2 + 4 * 10^1 + 3 * 10^0.$

overflow

arr[i] * mul

$\boxed{mul * 10}$

num + arr[i] * mul.

mul = 1

$(1*10) \% 10^9$

$(100) \% 10^9$

$(1000) \% 10^9$

$(100000) \% 10^9$

```
int arrMod( int[] arr, int p) {
    long ~~int~~ num = 0;
    long ~~int~~ mul = 1;
        for( i= arr.length-1; i>=0; i--) {
            num = [num + (arr[i] * mul) % p] % p;
            mul = (mul *10) % p
        }
    return (int)num % p;
}
```

p   10 = p*10(long range)

$\underbrace{mul}_{[0,\, p-1]} = (mul * 10) \% p \longrightarrow$ mul * 10 ← mul

mul % p ← mul

p

$10^9 * 10 = \boxed{10^{10}}$

Thankyou :)

Doubts

$(3^{20}) \% 4$ $\quad (3^4)^5 \% 4$

$(3^2)^{10} \% 4$ $\quad (81)^5 \% 4$

$(9)^{10} \% 4 = 9 \% 4$

1

$[\overset{0}{8} \quad \overset{1}{2} \quad \overset{2}{4}] \Rightarrow 824 \% p$

$[8 * 10^2 + 2 * 10^1 + 4 * 10^0] \% p \Rightarrow 824 \% p$

$8000 \; 2224 - 20 \quad + \quad 4) \% p$

$[arr[0] * mul + arr[1] * mul + arr[2] * mul] \% p \Rightarrow 824 \% p$

$[(arr[0] * mul) \% p + \text{- - - - -}] \% p \Rightarrow 824 \% p$

$[0, p-1) \quad (p-1]$

$[p-4) \longrightarrow 824 \% p$