Maths - Modular Arithmetic

%

Modulo

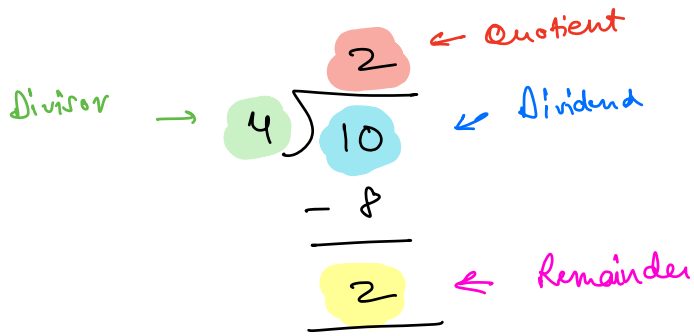
Agenda

- Modular Operator
- Modular Arithmetics
- Divisibility Rules
- Problems

Revision

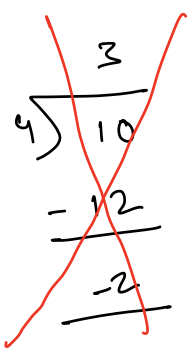
Modulo Operator % → Remainder

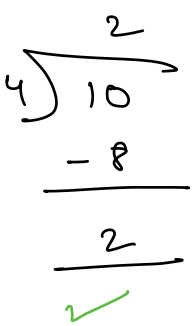
Dividend = Divisor * Quotient + Remainder

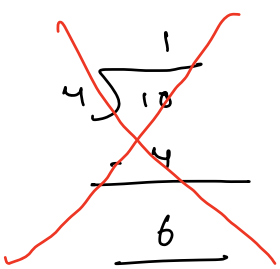


⇒ Remainder = Dividend − (Divisor * Quotient)

highest multiple of divisor ≤ dividend







Quiz 1

150 % 11

$150 - 143 = 7$

Quiz 2

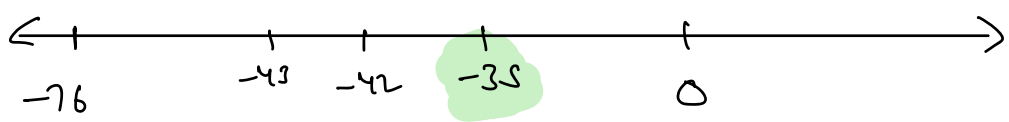
100 % 7

$100 - 98 = 2$

Quiz 3

Pick the largest

-76, -35, -43, -42



Quiz 4

-40 % 7

$$\text{Rem} = -40 - \{\text{greatest multiple of } 7 \leq -40\}$$

$$= -40 - (-42)$$

$$= -40 + 42$$

$$= 2$$

35 < -40? No
-35 < -40? No
-42 < -40? Yes

Java = -5
Python = 2 ↙ +7

-80 % 9

$$\text{Rem} = -80 - \{\text{greatest multiple of } 9 \leq -80\}$$

$$= -80 - (-81)$$

$$= -80 + 81$$

$$= 1$$

Java = -9
Python = 1 ↙ +9

Quiz 5

-60 % 9

Rem = -60 − { greatest multiple of 9 ≤ -60 }

= -60 − (-63)

= -60 + 63

= 3

Java = -6

Python = 3 ↙ +9

---

res = a % b

if(res < 0)

res = res + b

Range

N % 10

↓

$(-\infty, \infty)$

Min = 0
Max = 9

$\Rightarrow$ Range $[0, 9]$

N = 100 → 100 % 10 → 0

N = 99 → 99 % 10 → 9

N % 6

Min = 0
Max = 5

Range $[0, 5]$

N % M

Min = 0
Max = M−1

Range $[0, M-1]$

Why modulo ?

Modulo operator allows us to get the result in a specific range.

Usecases

1) Dare to Dream → Consistent hashing

long

-9×10^{18} to 9×10^{18}

2) Hashmaps / Dictionary

↳ Hashing

3) Cryptography

4) Sharding in DBMS

Modular Arithmetic

$(a + b) \% M = (a \% M + b \% M) \% M$

Quiz 6

Range = $[0, M-1]$

Example

$a = 10$

$b = 8$

$M = 4$

$LHS = (10 + 8) \% 4 = 18 \% 4 = 2$

$RHS = (10 \% 4 + 8 \% 4) \% 4$

$= (2 + 0) \% 4$

$= (2) \% 4$

$= 2$

Example

$a = 6$

$b = 13$

$M = 7$

$LHS = (6 + 13) \% 7 = 19 \% 7 = 5$

$RHS = (6 \% 7 + 13 \% 7) \% 7$

$= (6 + 6) \% 7$

$= (12) \% 7$

$= 5$

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

Range $= [0, M-1]$

Example

$a = 6$

$b = 7$

$M = 4$

$LHS = (6 * 7) \% 4 = 42 \% 4$

$= 2$

$RHS = (6 \% 4 * 7 \% 4) \% 4$

$= (2 * 3) \% 4$

$= 6 \% 4$

$= 2$

(a - b) % M

(a / b) % M

} Covered in the Advanced Batch

Problems

Q1. Given a, n, p. Compute a^n %p.

Note: No inbuilt functions allowed

Example

a = 3

n = 4

p = 7

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

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

Assume no overflow

TC: O(N)

SC: O(1)

How to handle the overflow problem ?

a = 10
n = 100
p = 30

$a^n \% p$

long - 10^{18}

$10^{100} \% 30$

```
power(int a, int n, int p) {

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

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

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

n times

Dry Run

a, n = 5, p, ans = 1

i	ans = (ans * a) % p	ans
1	ans = (1 * a) % p	$a \% p$
2	ans = ($a \% p$ * a) % p	$a^2 \% p$
3	ans = ($a^2 \% p$ * a) % p	$a^3 \% p$
4	ans = ($a^3 \% p$ * a) % p	$a^4 \% p$
5	ans = ($a^4 \% p$ * a) % p	$a^5 \% p$

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

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

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

= $a^2 \% p$

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

Divisible by 3

✓ 789 → 7+8+9 = 24

✗ 8215 → 8+2+1+5 = 16

Sum of all digits is divisible by 3

Quiz 7

Which of these numbers is divisible by 3?

4351 (13), 3521 (11), 7326 (18), 8236 (19)

$10 \% 3 = 1$

$10^2 \% 3 = 1$

$10^3 \% 3 = 1$

$10^4 \% 3 = 1$

$10^n \% 3 = 1$

Why does this work?

Property:

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

(a + b) % m = (a%m + b%m) % m

$$3458 = 3\times10^3 + 4\times10^2 + 5\times10^1 + 8\times10^0$$

$$3458\,\%3 = \left(3\times10^3 + 4\times10^2 + 5\times10^1 + 8\times10^0\right)\%3$$

$$= \left((3\times10^3)\%3 + (4\times10^2)\%3 + (5\times10^1)\%3 + (8\times10^0)\%3 \right)\%3$$

$$= \left(3\%3 + 4\%3 + 5\%3 + 8\%3 \right)\%3$$

Sum of digits →

$$= (3 + 4 + 5 + 8)\%3$$

$$= 2$$

$$(3\times10^3)\%3 = (3\%3 \times 10^3\%3)\%3$$

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

$$= 3\%3$$

$$(4\times10^2)\%3 = (4\%3 \times 10^2\%3)\%3$$

$$= (4\%3 \times 1)\%3$$

$$= 4\%3$$

Divisible by 4

Last two digits are divisible by 4.

Quiz 8

25 424 , 13960 , 44838 , 55552

✓ ✓ ✗ ✓

N = 3294

$$3294 = 3\times10^3 + 2\times10^2 + 9\times10^1 + 4\times10^0$$

$$3294 \,\%4 = (3\times10^3 + 2\times10^2 + 9\times10^1 + 4\times10^0)\,\%4$$

$$= ((3\times10^3)\%4 + (2\times10^2)\%4 + (9\times10^1)\%4 + (4\times10^0)\%4)\,\%4$$

$$= (0 + 0 + (9\times10^1)\%4 + (4\times10^0)\%4)\,\%4$$

$$= (9\times10^1 + 4\times10^0)\,\%4$$

$= (94) \% 4$ ← Last two digits

$(3 \times 10^3) \% 4 = (3 \% 4 \times 10^3 \% 4) \% 4$

$10^3 \% 4 = 0$

$= 0$

TODO

1) Divisibility rule of 9

2) " " " 8

Q. Given 1 number in arr[N], calculate number % p.

↳ Each digit of the number is given in arr[i]

78962

arr[5] =

7	8	9	6	2
0	1	2	3	4

p = 5

78962 % 5 = 2

3264

N=4

3	2	6	4
0	1	2	3

3264 % 5 = 4

Constraints

N = No of digits in the number $\leq 10^5$

$p \leq 10^5$

$0 \leq arr[i] \leq 9$ ← Implied

Largest number

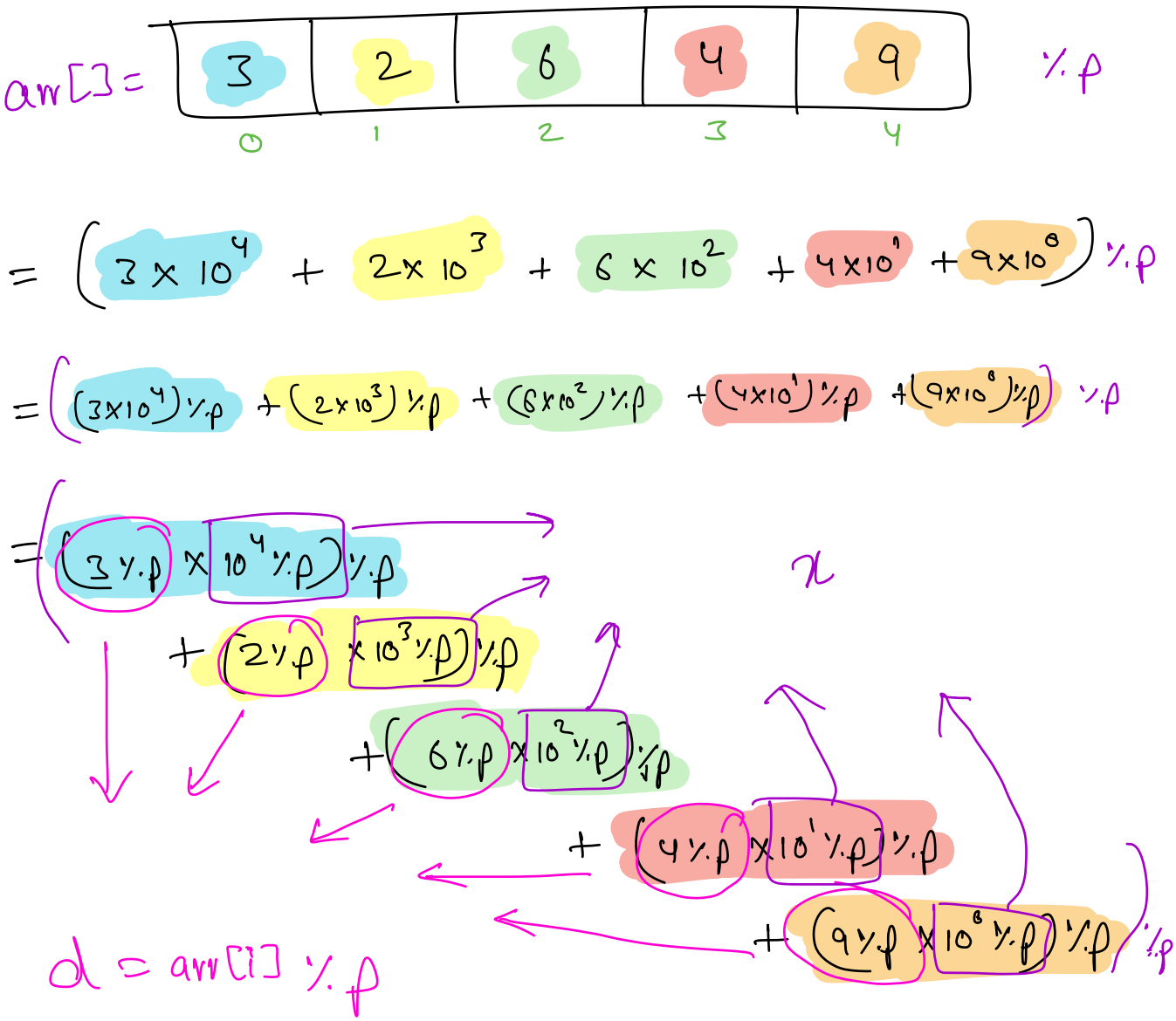
If N=2 | 9 | 9 | $= 10^2 - 1$

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

N=4 9 9 9 9 $= 10^4 - 1$

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

$= 10^{100000} - 1$



x = 1 %p

x = (x x 10) %p = 10 %p

x = (x x 10) %p = 10^2 %p

x = (x x 10) %p = 10^3 %p

Using power equation

ans = (ans*a) %p

Put a = 10

ans = x

Pseudocode

```
int arrayMod(int arr[], int p) {
        n = arr.length
        res = 0
        x = 1
        for (i=N-1 ; i >= 0 ; i--) {
                d = arr[i] % p
                res = (res + (d * x) % p) % p
                x = (x * 10) % p
        }
        return res
}
```

Doubts

Thank You

Competitive

- → Probability
- → Permutation / Combination } Advanced
- → Matrices
- → Inequality
- → Logarithm } Already covered
- → Prime Sieve ← Advanced
- → Data structures & algorithms ↗

Good Night

Thank You

Monday