Modular Arthimetic Introduction

Vinay Neekhra

Senior Instructor & Mentor

Reachable in Scaler Lounge 

"Everything in moderation; including moderation!"

Today's content:

- → % operator
- → modular arithmatic
- → One easy problem
- → one hard problem.

int range : $[-2 \times 10^9, 2 \times 10^9]$ $[-2^{31}, 2^{31}-1]$
(4 bytes)

long range : $[-8 \times 10^{18}, 8 \times 10^{18}]$

% Basics:

n % a = remainder when n is divided by a

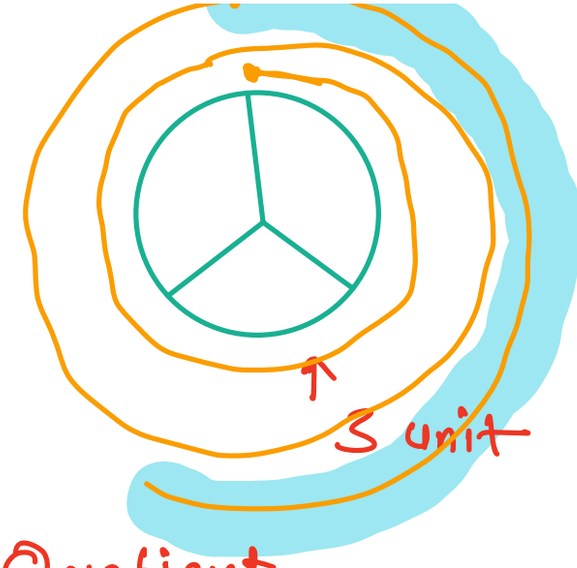
r = dividend − (greatest multiple of divisor <= dividend)

dividend → $\frac{A}{B}$ ← divisor , $Q + R$ (Q: Quotient, R: remainder)

$8 \% 3 = 8 - (3*2) = 2$

$13 \% 5 = 13 - (10) = 3$

(0, 5, 10, 15)



Remainder = dividend − divisor * Quotient

(greatest multiple of divisor <= dividend)

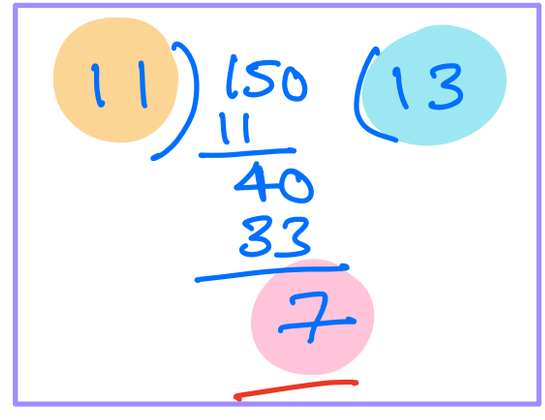
Quiz $150 \% 11 = ?$

$= 150 - (\text{greatest multiple of } 11 \leq 150)$

$= 150 - (143)$

$= 7$

$\Rightarrow \frac{150}{11} =$



Quiz 2 $100 \% 7 = ?$

$$7)\overline{100}\,(14$$
$$\underline{7}$$
$$30$$
$$\underline{28}$$
$$2$$

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

$= 100 - (98)$

$= 2$

Quiz 3 $-40 \% 7 = ?$

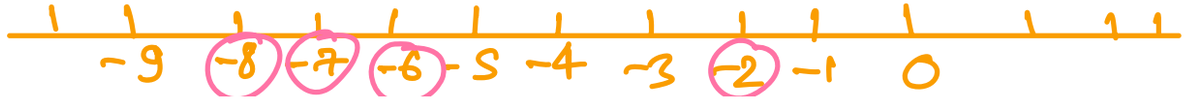
$= -40 - (\text{greatest multiple of } 7 <= -40)$

$(-63, -56, -49, -42, -35, -28, -21, -14, -7, 0, 7, 21$

$= -40 - (-42)$

$= 2.$

Quiz 4



Quiz. 5. $-60 \% 9 = ?$

$= -60 - ($ greatest multiple of 9 $<= -60)$

$(-90, -81, -72, -63, -54, -45 \ldots\ldots$

$= -60 - (-63)$

$= 3.$

⊛ '%' operator in programming languages

$-40 - (-35)$
$= -5$

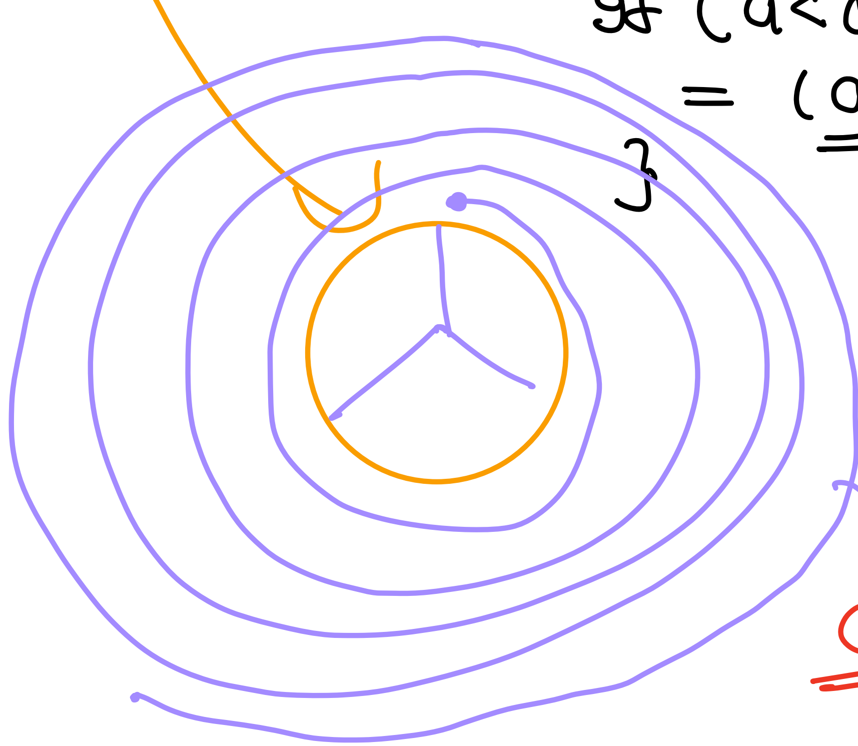
ex.	Python		Java / C / C++ / C# / JS	
$-40 \% 7$	2	⟷	-5	$(-5+7)$
$-60 \% 9$	3	⟷	-6	$(-6+9)$
$-40 \% 9$	5	⟷	-4	$(-4+9)$

Obsⁿ: difference is equal to the divisor

$a \% p$

in these languages

```
if (a<0) {
    = (a%p) + p
}
```



$40 \% 7 = 5$

$\Rightarrow -40 \% 7$

$\Rightarrow 2$

Quiz: $-40 \% (-7)$

(*) Why? → limit the scope of our data.

$\left.\begin{matrix} -\infty \\ \vdots \\ +\infty \end{matrix}\right] \% 10 = [0, 9]$

club ⇒ A, B, C

↓ serial number % 3 ↑

$-\infty \rceil \% p = [0, p-1]$

+∞

Hashing (DSA)

consistent (NLD, LLD) Hashing

5. Properties.

① $(a+b) \% M = ((a \% M) + (b \% M)) \% M$

a	b	M	(a+b)%M	((a%M)+(b%M))%M
8	6	10	4	(8+6)%10 = 4
18	11	10	9	(8+1)%10 = 9
18	36	10	4	((8+6))%10 = 4

(8 ← 18%10, 6 ← 36%10)

② $(a * b) \% M = ((a \% M) * (b \% M)) \% M$

a	b	M	(a*b)%M	(a%M)*(b%M)%M
8	7	6	2	((2)*1)%M

5 4 6 2 (5 * 4) % 6

(a - b) % M

(a / b) % M → Inverse modulo

→ advanced module

③ $(a \% p) \% p = a \% p$

$[0, p-1] \% p = [0, p-1]$

(16 % 10) % 10

(6) % 10 ⇒ 6

(16 % 10)

④ $(a \% p * b) \% p = (a * b) \% p$

$x = a \% p$, $y = b$

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

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

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

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

Quiz: $/3 = ?$

232	4560	238	4333
✗	✓	✗	✗

✱ Divisibility rules:

/2 = (If the last digit is (0,2,4,6,8) is divisible by 2)

/3 = sum of digits divisible by 3

/4 = last 2 digits / divisible by 4

/8 = last 3 digits / divisible by 8

/9 = sum of digits divisible by 9

H.W. $\Rightarrow$ $\underline{17 = ?}$

$\Rightarrow$ $4563\%13 = ?$

$= (4000 + 500 + 60 + 3)\%13$

$= ((4000\%13) + (500\%13) + (60\%13) + (3\%13))\%13$

$= ((4*1000)\%13) + \text{——}$

$= ((4\%13) * (1000\%13)\%13) + \text{——}$

$= (1*1\%13) + \text{——}$

$= 1 + ((5\%13) * (100\%13))\%13 + \text{——}$

$= 1 + (2*1)\%13 + \text{——}$

$= (1 + 2 + ((6\%13) * (10\%13)\%13 + 3\%13)\%13$

$= (1 + 2 + (0 * 1) \% 3) + 3 \% 3) \% 3$

$= (1 + 2 + 0 + 0) \% 3$

$= 0$

Obsⁿ:

$= ?$ divisibility rule for 3 $=$

$10 \% 3 = 1$	$10 \% 4 != 0$
$100 \% 3 = 1$	$100 \% 4 = 0$
$1000 \% 3 = 1$	$1000 \% 4 = 0$
⋮	⋮
$10^n \% 3 = 1$	$10^n \% 4 = 0 \quad n \geq 2$

10 ; 13

(*) 2347 13 = ?

$= ((2 * 1000) \% 3 + (3 * 100) \% 3 + (4 * 10) \% 3 + (7 * 1) \% 3) \% 3$

$= ((2 \% 3) + (3 \% 3) + (4 \% 3) + (7 \% 3)) \% 3$

$= (2+3+4+7) \% 3$

$= 16 \% 3$

$= 1$

⊛ divisibility by 2

$2457 \% 2 = ?$

$= [(2*1000) \% 2 + (4*100) \% 2 + (5*10) \% 2 + (7*1) \% 2) \% 2$

$= (0 + 0 + 0 + (7 \% 2))$

$= \underline{7 \% 2}$

$(5*10) \% 2$

⇒ $(5\%2 * 10\%2)\%2$

⇒ $(1 * 0)\%2 = 0$

(*) divisibility by 4.

$2457 \% 4 = ?$

$= ((2 * 1000)\%4 + (4 * 100)\%4 + (57\%4))\%4$

$\because \quad (57)\%4$

= If the last 2 digit num is divisible by 4, then the given number is divisible by 4.

Q. Given a, n, p, calculate $a^n \% p$ without using inbuilt function.

Constraints
$1 \le a \le 10^9$
$2 \le p \le 10^9$
$1 \le n \le 10^5$

ex:1 $a = 3, n = 4, p = 7$

⇒ $3^4 \% 7$ ⇒ $(3 \times 3 \times 3 \times 3)\%7$

⇒ $81 \% 7$ ⇒ 4

Ex. $a=4, n=5, P=6$

$\Rightarrow (4^5) \% 6$ $\Rightarrow (16*16*4) \% 6$

$\Rightarrow (256*4) \% 6$

$= (1024) \% 6$

$= 4$

* Brute force:

idea: ① calculate a^n (build pow fn)

② $a^n \% P = ans$.

```
int modulo (a, n, P) {
    int ans = 1
    for(i=1; i<=n; i++) {
```

// a*a*a*a.. n time

a^n

```
    ans *= a
  }
  return ans %p;
}
```

T.C. = O(N)
S.C. = O(1)

No TLE

Partial correct ⇒ WRONG

* a = 2, n = 30, p = 45

  ⇒ a^n ⇒ 2^{30} (we can store this in int)

  won't overflow $(-2^{31}, 2^{31})$

* a = 2, n = 60, p = 45

  ⇒ a^n ⇒ 2^{60} (we can NOT store this in int)

  Sol^n ⇒ instead of int we long

* a = 2, n = 100, p = 45

$\Rightarrow \quad a^n = 2^{100} \Rightarrow$ (No data structure can hold this value)

3. optimal approach:

idea: take modulo.

$$(a * a) \% p \Rightarrow \left((a\%p) * (a\%p)\right)\%p$$

this might overflow

this won't overflow

$a^{n}\%p$

$((1 * a\%p) * (a\%p))\%p$

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

```
int modulo (a, n, p) {
    a = a%p
    int ans = 1

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

```
    return ans;
}
```

(ans is always b/n (0, p-1))

Dry Run: a, p, n = 5 — 10^9, 10^9 — No overflow

ans	i	i<=5
1	1	✓
a%p	2	✓

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

$ans = a \% p$ ← no overflow

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

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

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

$= (a * a) \% p$

$= a^2 \% p$ → no overflow

$a^2 \% p$ 3 ✓ $ans = ((a^2 \% p) * a) \% p$

$= a^3 \% p$ → no overflow

$a^3 \% p$ 4 ✓ $ans = (a^3 \% p * a) \% p$

$= (a^3 * a) \% p$

$= a^4 \% p$ → no overflow

$a^4 \% p$ 5 ✓ $ans = ((a^4 \% p) * a) \% p$

$= a^5 \% p$ → no overflow

$a^5 \% p$ 6 ✗ ⇒ return ans

Q. Given a number in array format, calculate a % P.

$1 \leq$ Array size $\leq 10^5$ → N

$0 \leq A[i] \leq 9$

$2 \leq P \leq 10^9$

ex: N = 5, A = [6, 2, 3, 4, 3], P = 49

⇒ (62343) % 49 = 15 = ans

ex: ② N = 4, A = [2, 4, 3, 7], P = 16

⇒ (2437) % 16 = 5 = ans

Brute force soln:

idea: ① construct the number num

② num % P

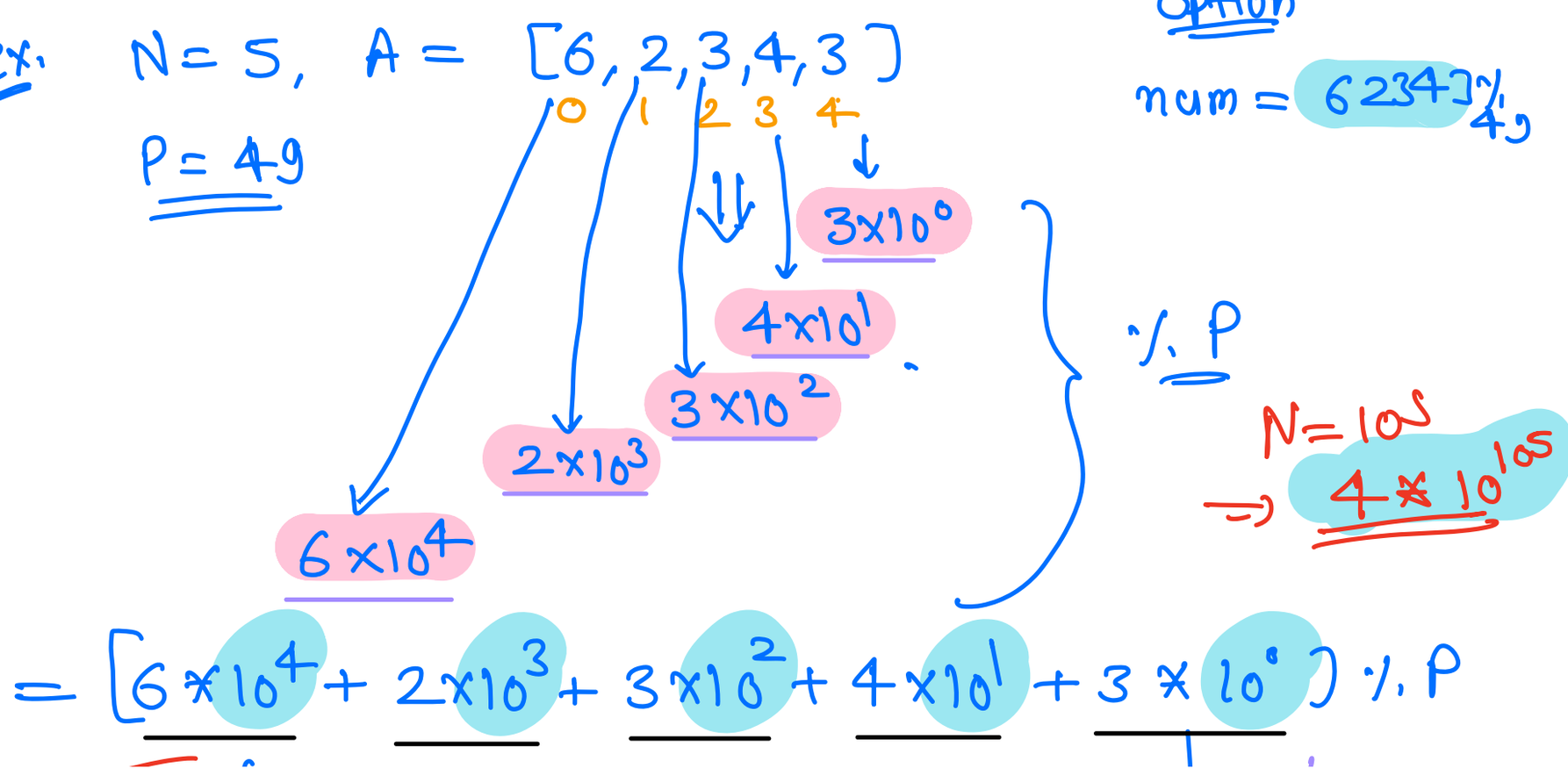
flaw: (1) overflow

⊛ Optimised approach:

(1) take modulo inside

ex. N = 5, A = [6, 2, 3, 4, 3]

P = 49

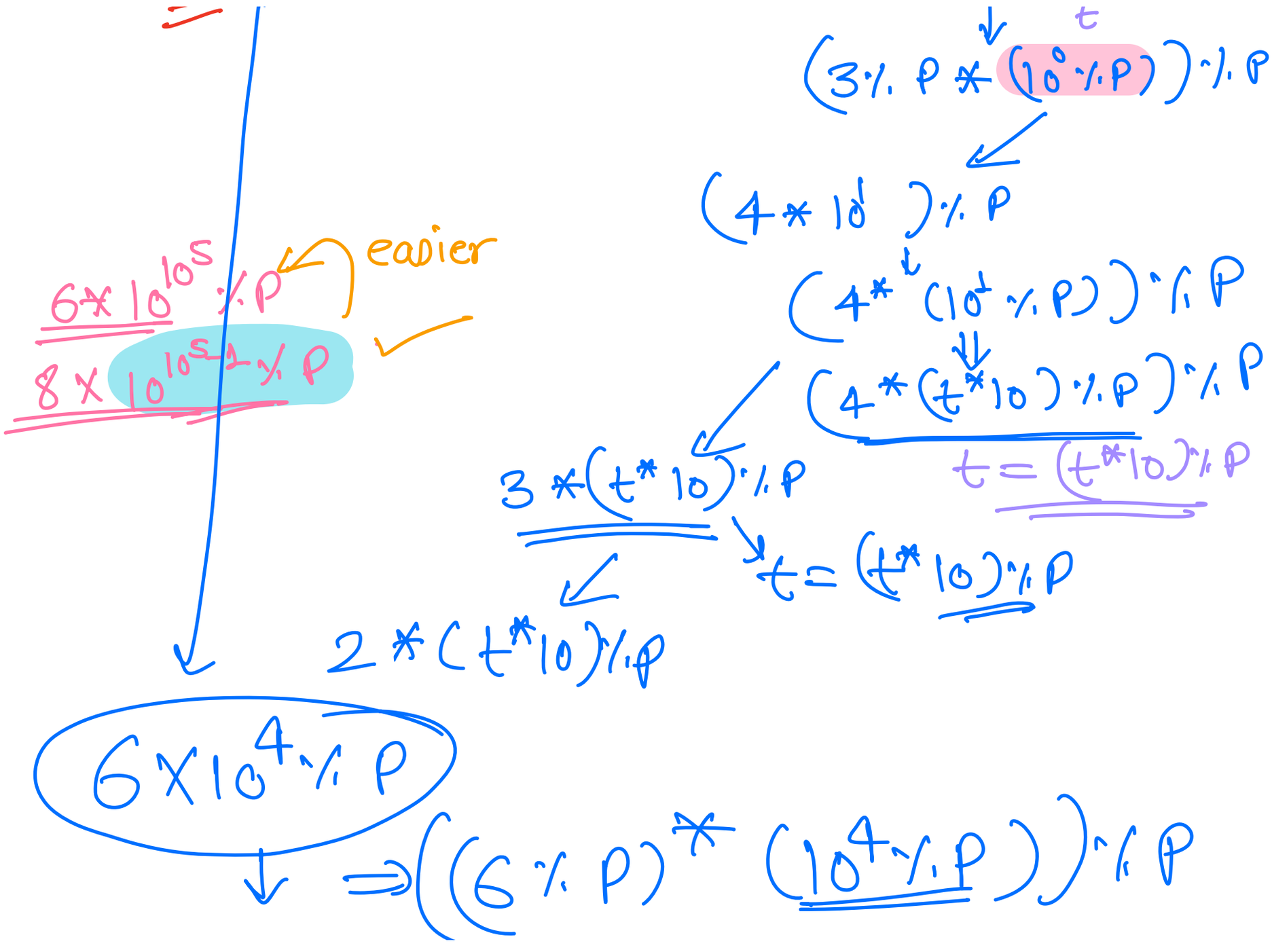


option

num = 62343 % 49

N = 10^5

⇒ 4 * 10^5


$6*10^{10^5}\ \%P$
easier
$8\times 10^{10^5-1}\ \%P$
$(3\%P * (10^0\%P))\%P$
t
$(4*10^1)\%P$
$(4*(10^1\%P))\%P$
$(4*(t*10)\%P)\%P$
$t=(t*10)\%P$
$3*(t*10)\%P$
$t=(t*10)\%P$
$2*(t*10)\%P$
$6\times 10^4\%P$
$\Rightarrow((6\%P)*(10^4\%P))\%P$

$$\Rightarrow ((6\%P) * (10 * 10^{3}\%P)\%P$$

$$\Rightarrow ((6\%P) * (10 * t)\%P)$$

$$\boxed{t = 10^{x}\%P}$$

Brute force:

```
int arrModulo ( A , P) {
  int power = 1;  int answer = 0
  for (i = N-1; i >= 0; i++) {
      answer = (answer + A[i] * power) % P
```

6 2 3 4]

↓

4 %P

3 X 10 %P

(2 X 100) %P

(6 * 1000) %P

power = power * 10 ✗ power = 10^{10}

→ Overflow

```
    }
}
```

Optimal solution

```
int arrModulo(
    int t = 1;          // 10^0 % P = 1 % P = 1
    int answer = 0;
    for (i = N-1; i >= 0; i--) {
        answer = (answer + ((A[i] % P) * t) % P   // No overflow
        t = (t * 10) % P                          // No overflow
    }
    return answer;
```

T.C = O(N)
S.C. = O(1)