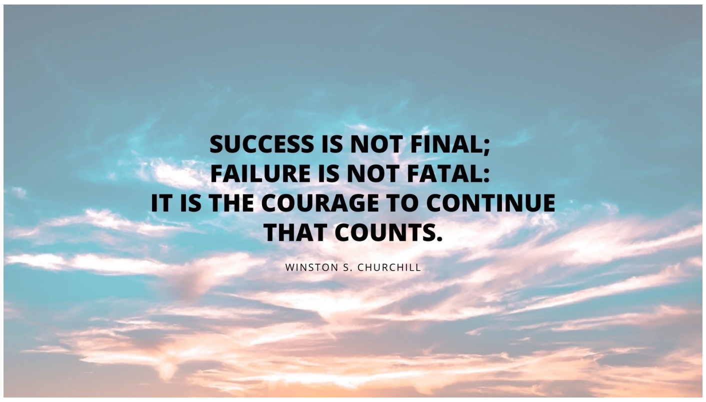
Modular Arithmetic



Today's content

→ % operator

→ Modular arithmetic % → {+, −, *, /}

→ 1 Google problem

% operator basics

$n \% a$ = Remainder when n divided by a.

$10 \% 4 = 2$

$13 \% 5 = 3$

Dividend = quo * div + rem

$$\text{rem} = \text{Dividend} - \underbrace{\text{div} * \text{quo}}_{\text{greatest mul of div} \le \text{dividend}}$$

$10 \% 4 = 10 - 8 = 2$

$13 \% 5 = 13 - \{\text{greatest mul of } 5 \le 13\}$

$= 13 - 10 = 3$

Quiz 1 :- $150 \% 11$

$\Rightarrow 150 - \{\text{greatest mul of } 11 \le 150\}$

$= 150 - 143 \Rightarrow 7$

Quiz 2 $= 100 \% 7$

$= 100 - \{\text{greatest mul of } 7 \leq 100\}$

$= 100 - 98 \Rightarrow 2$

Quiz 3 $= -60 \% 9$

$= -60 - \{\text{greatest mul of } \underbrace{9 \leq -60}\}$

$\Rightarrow -60 - (-63)$

$= -60 + 63 = 3$

Quiz 4 $= -40 \% 7$

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

$= -40 - \{-42\} \Rightarrow 2$

Remainder is something which is left

Remainder is always going to be positive

$a \% p$

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

$$-5 \xrightarrow{+7} 2$$

$$-6 \xrightarrow{+9} 3$$

$$-4 \xrightarrow{+9} 5$$

In Java, C++, C#, JS

```
if ( a < 0 )
    return a % p + p
}
```

* In Java

$\left(\frac{a}{b}\right) \rightarrow$ Integer divison

$100/7 \Rightarrow 14$

$100 \% 7 = 100 - \{\text{greatest mul of } 7 \leq 100\}$

$= 100 - \{7 * 14\} \Rightarrow 2$

$-40/7 = -5$

$-40 \% 7 = -40 - \{\text{greatest mul of } 7 \leq -40\}$

$= -40 - \{7 * -5\} \Rightarrow -5$

$-60/9 = -6$

$-60 \% 9 = -60 - (\text{greatest mul of } 9 \leq -60)$

$= -60 - (9 * -6) \Rightarrow -6$

* In python

$a/b \Rightarrow \text{floor}\left(\frac{a}{b}\right)$

$\frac{6}{4} = \text{floor}(1.5) \Rightarrow 1$

$\frac{7}{3} = \text{floor}(2.33) = 2$

$\frac{10}{6} = \text{floor}(1.6..) = 1$

$$floor\left(\frac{100}{7}\right) = floor(14.\ldots) \Rightarrow 1$$

$$100 \% 7 = 100 - \{\text{greatest mul of } 7 \le 100\}$$

$$= 100 - (7 * 14) \Rightarrow 2$$

$$floor(-40/7) = floor(-5.7) = -6$$

$$-40 \% 7 = -40 - \{\text{greatest mul of } 7 \le -40\}$$

$$= -40 - \{7 * -6\} = 2$$

$$floor(-60/9) = floor(-6.66) \Rightarrow -7$$

$$-60 \% 9 = -60 - (\text{greatest mul of } 9 \le -60)$$

$$= -60 - (9 * -7) \Rightarrow 3$$

* Why % ? → Limit the range of input in our required space

Hashing

Consistent hashing

LLD & HLD

$$\left.\begin{array}{l} 839 \\ 723 \\ 166 \\ 234 \\ -78 \\ 237 \end{array}\right\} \% 10 \quad \begin{array}{l} = 9 \\ = 3 \\ = 6 \\ = 4 \\ = 2 \\ = 7 \end{array}$$

$$\{0 - 9\}$$

$$\left.\begin{matrix}-\infty \\ \\ \infty\end{matrix}\right\} \% M \Rightarrow \boxed{\{0 \quad m-1\}}$$

* Modular Arithmetic $\quad \% \rightarrow \{+, *, -, /\}$

Q: $(a+b) \% p = (a \% p + b \% p) \% p$

$a = 8$

$b = 6$

$p = 10$

$(8+6) \% 10 = (8 \% 10 + 6 \% 10)$

$14 \% 10 = 8 + 6$ * Wrong

$4 = 14$

$a = 5$

$b = 4$

$p = 6$

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

$(5+4) \% 6 = (5 \% 6 + 4 \% 6) \% 6$

$9 \% 6 = (5 + 4) \% 6$

$3 = 3$

$a = 7$ $\quad (7+10)\,\%\,3 = (7\,\%\,3 + 10\,\%\,3)\,\%\,3$

$b = 10$ $\quad 17\,\%\,3 = (1+1)\,\%\,3$

$p = 3$ $\quad \boxed{2} = 2\,\%\,3$

$= \boxed{2}$

02. $(a * b)\,\%\,p = (a\,\%\,p * b\,\%\,p)\,\%\,p$

$a = 10$ $\quad (10 * 7)\,\%\,3 = (10\,\%\,3 * 7\,\%\,3)\,\%\,3$

$b = 7$ $\quad = 70\,\%\,3 = (1 * 1)\,\%\,3$

$p = 3$ $\quad \Rightarrow 1 = 1$

03. $(a-b)\,\%\,p$

04. $(a/b)\,\%\,p$

Advance content + Inverse modulo

$*\quad \underbrace{(a\,\%\,p)}_{[0 \quad p-1]}\,\%\,p = \underbrace{a\,\%\,p}_{[0 \quad p-1]}$ → Correct

$\underbrace{[0 \quad p-1]\,\%\,p}_{[0 \quad p-1]}$

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

$x = a \% p$

$y = b$

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

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

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

$= (a * b) \% p$

* Divisibility Rules

01. Numbers divisible by 3

% 3 = sum of digits should be divisible by 3

01. $2475 \% 3$

$(2000 + 400 + 70 + 5) \% 3$

$= (2000 \% 3 + 400 \% 3 + 70 \% 3 + 5 \% 3) \% 3$

$= ((2 * 10^3) \% 3 + (4 * 10^2) \% 3 + (7 * 10^1) \% 3 + (5 * 10^0) \% 3) \% 3$

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

$\Rightarrow (\underbrace{2+4+7+5}_{\text{sum of all digits}})\ \%\ 3$

Observation

$10^0\ \%\ 3 = 1$

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

$10^2\ \%\ 3 = 1$

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

$\vdots$

$10^x\ \%\ 3 = 1$

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

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

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

$10^4\ \%\ 9 = 1$

$\vdots$

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

% 9 = sum of digits divisible by 9.

* Divisibility rule for 4 → Last 2 digits must be divisible by 4

01. $(2457)\ \%\ 4 = (2400 + 57)\ \%\ 4$

$= (2400\ \%\ 4 + 57\ \%\ 4)\ \%\ 4$

$(0 + 57\ \%\ 4)\ \%\ 4$

↓

NO

$\Rightarrow (57 \% 4) \% 4$

$= (57 \% 4)$

Observation

$10^0 \% 4 = 1$

$10^1 \% 4 = 2$

$10^2 \% 4 = 0$

$10^3 \% 4 = 0$

$10^4 \% 4 = 0$

$10^5 \% 4 = 0$

All multiples of 100 are divisible by 4

* Divisibility rules for 8 →

Last 3 digits of the no. are divisible by 8

Q1. $(2457 \% 8)$ → No

$= (2000 + 457) \% 8$

$= (\cancel{2000 \% 8} + 457 \% 8) \% 8$

$= (0 + 457 \% 8) \% 8$

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

$= (457 \% 8)$

Obs

$10^0 \% 8 = 1$

$10^1 \% 8 = 2$

$10^2 \% 8 = 4$

$10^3 \% 8 = 0$

$10^4 \% 8 = 0$

$10^5 \% 8 = 0$

All multiples of 1000 are divisible by 8

Todo → { divisibility rules for 7 }

10:10 → 10:21 pm

Q1. Given a, n, p. Calculate $a^n \% p$, without using inbuilt functions

Constraints → $1 \leq a \leq 10^9$

$2 \leq p \leq 10^9$

$1 \leq n \leq 10^5$

pown (int a, int n, int p)

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

✗

$a = a$ $\quad n = 4$

i	$i \le 4$	$a = a * a$	$i = i + 1$
1	$1 \le 4$	$a = a^2$	2
2	$2 \le 4$	$a = a^2 * a^2$ a^4	3
3	$3 \le 4$	$a = a^4 * a^4$ a^8	4
4	$4 \le 4$	$a = a^8 * a^8$ a^{16}	5

$5 \le 4 \rightarrow \boxed{a^{16}}$

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

a	n	p	→ $a^n \% p$
2	10	20	→ $2^{10} \% 20$
2	30	45	→ $2^{30} \% 45$
2	60	45	→ $\underbrace{2^{60}}_{\text{long}} \% 45$
2	100	45	→ $\underbrace{\boxed{2^{100}}}_{\text{overflow}} \% 45$

Range of int $= -2^{31}$ to $2^{31}-1$

Issue → Trying to calculate the a^n first & then applying the modulus

Apply modulus at every multiplication step

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

Given

$a = a$

$n = 4$

$p = p$

$a^4 \% p$

ans	i	$i \le n$
1	1	$1 \le 4$
$a \% p$	2	$2 \le 4$
$a^2 \% p$	3	$3 \le 4$

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

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

$ans = \boxed{a \% p \rightarrow \text{No overflow}}$

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

$= (\underbrace{(a \% p) \% p}_{} * a \% p) \% p$

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

$= (a * a) \% p$

$= \boxed{a^2 \% p \rightarrow \text{No overflow}}$

Max value of $a = 10^9$

$= (10^9)^2 \% p$

$= \underbrace{10^{18}}_{\text{long}} \% p$

$ans = [0 \quad p-1]$

$ans = (\underbrace{a^2 \% p}_{[0 - p-1]} * \underbrace{a}_{[1 \quad 10^9]}) \% p$

$= \underbrace{p}_{} * \underbrace{10^9}_{}$

$= 10^9 * 10^9 = 10^{18} \% p$

$\boxed{ans = a^3 \% p \rightarrow [0 \quad p-1]}$

$a^3 \% p$ 4 $4 \le 4$

$ans = (\underbrace{a^3 \% p}_{[0 \;\; p-1]} * \underbrace{a}_{[1 \;\; 10^9]}) \% p$

$\underbrace{[0 \;\; p-1]}_{p} * \underbrace{[1 \;\; 10^9]}$

$p * 10^9$

$[10^9 * 10^9] \% p$

$[10^{18}] \% p$

$ans = a^4 \% p = [0 \;\; p-1]$

$a^4 \% p$ 5 $5 < 4$ $\longrightarrow$ return ans

Q2. Given a number in ar[] format. Calculate arr[] % p

Each ar[i] represents a single digit of a no.

Constraints

$1 \le n \le 10^5$

$0 \le ar[i] \le 9$

$2 \le p \le 10^9$

$arr[\,] =$

6	2	3	4	5

$p = 45$

return $(62345 \% 45) \Rightarrow \boxed{20}$

Eg:- $n = 4$

2	4	3	7

$p = 16$

return $\underline{\underline{2437 \% 16}} \rightarrow 5$

* Convert ar[] into a no & then %p ✗

$n = 1 \quad \underline{9} \quad = 10^1 - 1$

$n = 2 \quad \underline{9} \quad \underline{9} \quad = 10^2 - 1$

$n = 3 \quad \underline{9} \quad \underline{9} \quad \underline{9} \quad = 10^3 - 1$

⋮

n digit $= 10^n - 1$

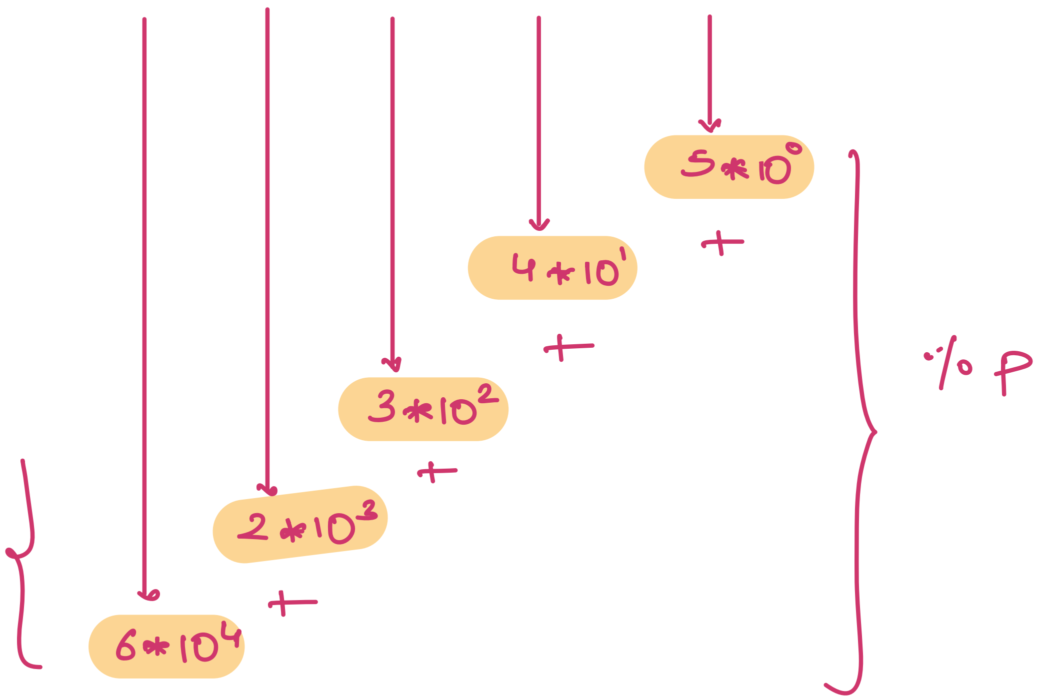
As per constraints max $n = 10^5$

no. $= \boxed{10^{10^5} - 1}$ } Not possible to store the number

Idea 2 → Split the no. digit by digit & then generate our answer

arr[] =

6	2	3	4	5



$$= \{ (6 * 10^4) + (2 * 10^3) + (3 * 10^2) + (4 * 10^1) + 5 * 10^0 \} \% p$$

$(5 * 10^0) \% p$

$x = 1 * 5$

$x = (x * 10) \% p$

$(4 * 10^1) \% p$

$x = 10 \% p * 4$

$x = (x * 10) \% p$

$(3 * 10^2) \% p$

$x = 10^2 \% p * 3$

$x = (x * 10) \% p$

$(2 * 10^3) \% p$

$x = 10^3 \% p * 2$

$x = (x * 10) \% p$

$(6 * 10^4) \% p$

$x = 10^4 \% p * 6$

```
int arrmod (int [] ar, int p)
{
    long sum=0
    long x=1
    for (i=n-1; i≥0; i--)
    {
        sum = (sum + ar[i] * x) % p
        x = (x * 10) % p
    }
    return sum;
}
```

$[0 \quad p-1] * 10 = 10p$ max product

$= 10 * 10^9 = 10^{10} \rightarrow$ long

Doubts

$1 \le n \le 10^5$

$0 \le ar[i] \le 9$

$2 \le p \le 10^9$

$\underbrace{[0 \quad p-1]}$

1	2	3

$123 = 100 + 20 + 3$

10^2 10^1 10^0

10^5

10

Reverse bits

0 0 0 0 0 0 0 0 1 1 1 $\boxed{1}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ 0

1 _ _ _ _ _ _ _ _ _ _ _

31

idx = 0 , long res = 0

check if (n, idx) == set

res = res | (1 << 31 - idx);

* Set bit

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ 4 3 2 1 0

num = 0 0 0 0 0 0 0 0 0 0 0 0 0

A = 2

B = 4