% ⇒ Modulus ⇒ Remainder

$n \% a$ ⇒ Remainder when we divide n by a

Eg ⇒ 1) $10 \% 4 = 2$

$$\begin{array}{r} 2 \\ 4 \overline{)10} \\ 8 \\ \hline 2 \end{array}$$

2) $13 \% 5 = 3$

Divisor ← 5) 13 (2 ⇒ Quotient

10

3 ⇒ Ans

Divident → Remainder

$$\begin{array}{r} 3 \\ 5 \overline{)15} \\ 15 \\ \hline 0 \end{array}$$

Remainder

$0 \leq \text{Remainder} < \text{Divisor}$

Divident = Quotient × Divisor + Remainder

$$\boxed{\text{Remainder} = \text{Divident} - (\text{Quotient} \times \text{Divisor})}$$

greatest multiple of divisor ≤ divident

Quiz

150 % 11

$$\begin{array}{r} 13 \\ 11 \overline{)150} \\ 11 \\ \hline 40 \\ 33 \\ \hline 7 \end{array}$$

150
143
7

11 × 11 = 121
11
132
11
143
11
> 150

Q

-100 > -200

Quiz 3

-40 % 7 ⇒ Remainder

- 40 - (greatest multiple of 7 ≤ -40)

-7, -14, -21, -28, -35, -42, -49, -56

-40 - (-42) = 2

Quiz

$-60 \% 9 = 7$

$-60 - ($greatest multiple of 9 which is less than $-60)$

+ve

$9, 18, 27, 36, 45 < -60$ ✗

$-9, -18, -27, -36, -45, -54, -63$

$-72, -81, -90$

$-60 - (-63) = 3$

$$\boxed{a \% m \Rightarrow [0, m-1]}$$

$m = 5$

$a = 5$	Modulo $=$	0
$a = 6$	" $=$	1
$a = 7$		2
$a = 8$		3
$a = 9$		4
$a = 10$		0
"		1

12	2
13	3
14	4
15	0

(C/C++/Java/JS) ⇓ Python ⇓

$-(40 \% 7) = -5 + 7 = 2$

$-(60 \% 9) = -6 + 9 = 3$

$-(30 \% 4) = -2 + 4 = 2$

-30

%

$a \% m$ s.t. $m > a$

$= a$

1
2
3
4
5
⋮
10

$\%\ 5$

0
1
2
3
4

$5 \% 15$

$5 - \underline{0 \times 15} = 5$

$-\infty$

$\vdots$

∞

$\% 5$ — $[0, 4]$

$[0 - 100]$

350

349

348

$\vdots$

550

$350 \% 101$

Applications of %

1) HashMap / HashTable / dict / unordered_map
2) Consistent Hashing

3) Encryption

* Modular Arithmetic $(+ - \times \div)$

1) $\underbrace{(a+b) \% M}_{\text{Range} \Rightarrow [0, M-1]} = (\underbrace{a \% M + b \% M}_{0-m-1}) \% M$

$0-m-1$

$[0, 2m-2]$

$a \% m$ $a < m$

Eg ⇒ 1) $12 \% 5 \Rightarrow 2$

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

$= 1+1 = 2$

2) $a = 4$
$b = 4$

$(a+b) \% 5$

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

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

$= (4 + 4)$

[0-4]   [0-4]

$= \quad 8 \% 5 = 3$

[0 - 8]

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

$(a+b) \% m \Rightarrow [0, m-1]$

$a \% m \Rightarrow [0, m-1]$ $b \% m \Rightarrow [0, m-1]$

$[0, 2(m-1)] \% m$

$a = 4$

$b = 4$

$m = 5$

[0 - 4]

$(a+b) \% m$

Overflow

$\frac{8}{5} = 3$

$\left(\frac{4}{5}\right) + \left(\frac{4}{5}\right) \Rightarrow 4+4$

$a = $ INT_MAX

$b = $ INT_MAX

$(a+b) \quad \% m$

$2 \times$ INT_MAX   32 bits ✗

$a \% m + b \% m$ ✓

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

Q Implement power function which takes 3 argument

a, n, p

$power(a, n, p) \Rightarrow a^n \% p$

Eg 1) $a = 2, n = 5, p = 7$

$2^5 \% 7 = 32 \% 7 = 4$

2) $a = 3, n = 4, p = 6$

$(3^4) \% 6 = 81 \% 6 = 3$

Sol^n a^n $1 \times a \times a \times a \times a \times a \times a \times a ..$ n times

a^n

```
int power (a, n) {
    ans = 1;
    for (i = 0; i < N; i++) {
```

i	ans_b	ans_a
0	1	a^2
1	a	a^2
2	a^2	a^3

ans = ans × a;

}

return ans;

}

N-1 | a^{N-1} | a^N

a = 10
n = 40

$(10^{40}) \% P$

10^9+7 ⟹ Prime no.

Int ≤ 10^9

INT   ans % (10^9+7) ⟹ $x+1$

ans > INTMAX ⟶ (0 — ~~x~~)

var a = max (40)

var (1 bytes) = 8 bits = 255

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

$2^{8}-1$ 255

var a = 200
var b = 250

var c = (a+b) % 256 = (450)

[0, 255]

(Overflow)

$255 \Rightarrow (0, 254)$

$a \% 5$

11

21

31

41

0
1
2
3
4

clashes

collisions

$$a^n \% p = (\underbrace{a \times a \times a \times a \times \ldots a}_{n \text{ times}}) \% p$$

$$= ((a \% p) \times (a \% p) \times (a \% p) \ldots n\text{times}) \% p$$

Code

$a^n \% p$

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

~~int~~ long ans = 1;

$\Rightarrow$ for (i=1; i ≤ N; i++) {

// ans = ans × a

$$\underbrace{ans}_{[0,\,p-1]} = \Big(\underbrace{(ans \% p)}_{(0-p-1)} \times \underbrace{(a \% p)}_{(0-p-1)} \Big) \% p$$

$(p-1)^2$

$[0,\ (p-1)^2]$

}

return ans;

}

Divisibility Rules

1) Rule for 3 $\Rightarrow$ Sum of digits has to be divisible by 3

$(4372) \% 3 = 0$

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

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

$$\left(\left(4\times 10^3\right)\%3 + \left(3\times 10^2\right)\%3 + \left(7\times 10^1\right)\%3 + \left(2\times 10^0\right)\%3\right)\%3$$

$$(a\times b)\%M = \left((a\%M)\times(b\%M)\right)\%M$$

$$\left[\left((4\%3)\times\left(\cancel{10^3\%3}\right)^{1}\right)\%3 + \left((3\%3)\times\left(\cancel{10^2\%3}\right)^{1}\right)\%3 + \left((7\%3)\times\left(\cancel{10^1\%3}\right)^{1}\right)\%3 + (2\%3)\right)\%3\right]$$

$10\%3 \rightarrow 1$

$10^2\%3 \rightarrow 1$

$10^3\%3 \Rightarrow 1$

$$\forall i_{\geq 0} \quad (10^i)\%3 = 1$$

$$\left((4\%3) + (3\%3) + (7\%3) + (2\%3)\right)\%3$$

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

$$= \underbrace{(4+3+7+2)}\%3$$

Sum of digits % 3

$(a+b)\%M$

$=$

$\left((a\%M) + (b\%M)\right)\%M$

$a = 3$ $\quad M = 5$ $\quad a = 1$

$b = 4$ $\quad\quad\quad\quad b = 2$

$(3 + 4)$

$= 7 \% 5$

$\left(\frac{a \% m}{1} + \frac{b \% m}{2} \right)$

$3 \% 5 = 3$

Rule for 4 ⇒ Last 2 digits divisible by 4

$(3484) \% 4 = (3\times10^3 + 4\times10^2 + 8\times10^1 + 4) \% 4$

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

$\Downarrow$

$\left((3) \% 4 \times (10^3) \% 4 \right) \% 4$

$0 \quad 0 \quad 0 \quad 0$

$\left((8\times10) \% 4 + (4 \% 4) \right) \% 4$

$(8\times10 + 4) \% 4$

$\Downarrow$

Last 2 digit

$10 \% 4 \Rightarrow 2$

$100 \% 4 \Rightarrow 0$

$1000 \% 4 \Rightarrow 0$

$10^4 \% 4 \Rightarrow 0$

$\forall i \geq 2 \quad 10^i \% 4 = 0$

H.W: 9, 11

Doubts

$(-40 \% 7) \Rightarrow$ Not defined

power (a, N, P) {

INT

$a = 25$

$N = 325$

ans = 1

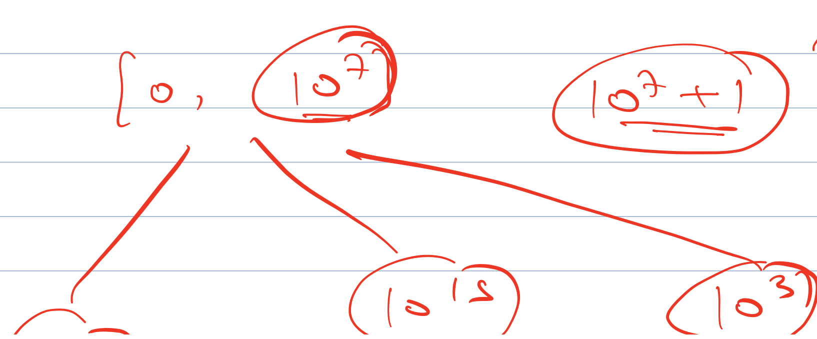
$10^{11} \% P \Rightarrow [0, P-1]$

10^{25} 10^{55}

Return the ans as mod $(10^9 + 7)$

P

PM



10^6

$\left(\frac{a}{b}\right) \% m$

$\Downarrow$

Fermat's theorem

$(a \times b^{-1}) \% m$

$(a \% m) \times (b^{-1} \% m) \Rightarrow$ prime no

$\Downarrow$

coprime

Inverse modulo

Max

MSR

1

1

1

1

1

< 4

> 4

a && b && c && d $\Rightarrow$ S

1 0 0 0   MSB   LSB

0 1 1 1 1

N ⇒ X 1 ≥ 4

Y ⇒ 0 X X

1 0 1 0 1

1 0 0 0 1

≥ 4