modulo operator : %

$\Downarrow$

finds the remainder.

Dividend = Divisor * Quotient + Remainder.

→ closest value to dividend

150 = 7 * x + y → 3

12

13

14

.

.

→ 20

21 → 147

$\boxed{150 \,\%\, 7 = 3}$

150 − 7 * 21 = y

150 − 147 = y

3

Divisor * Quotient → ≤ Dividend

Less than or equal to

Remainder = Dividend − Divisor * Quotient

① closest.

② Less than / equal to

① Remainder is always >= 0 ✓

② Max value of Remainder < Divisor !

49 % 7 = 0
50 % 7 = 1
51 % 7 → 2
52 % 7 → 3
53 % 7 → 4
54 % 7 → 5
55 % 7 → 6
56 % 7 → 0
57 % 7 → 1

Keeping modulo fixed.

⇒ Range of remainders

[0, Div-1]

⇓

Remainders,

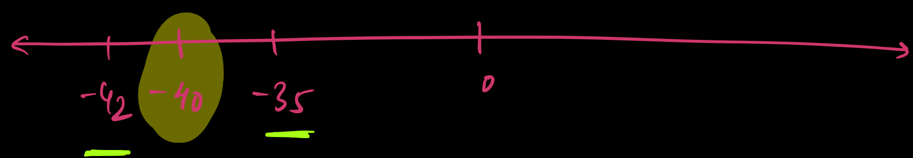
wrap around!

0 1 2 3 4 5 6

-40 % 7 → 2

→ -5

⇒ closest value less than or equal to !



$-40 = \cancel{-35} / -42 + \text{Remainder}$

$42 - 40 = \text{Remainder}$

2 ⇒ Remainder

$-60 = 9 * (\quad) + \text{Remai-}$

-63 / -54

3 -6

Applications of modulus operation

- → Rotate Matrix (k time Rotation)
- → Even or odd
- → Hashing
- → Cryptography

RSA

MD5

→ In DSA

↳ Limiting values.

$100^{10} \% x$

Modular Arithmetic

↓

Arithmetic operators

↓

+ - * /

Addition with modulo

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

$(29 + 100000) \% 10$ → 9

$29 \% 10 = 9$ $\qquad \% 10 = 0$

$(9+0)\% \rightarrow 9$

$a = x_1 + M^* y_1$

$b = x_2 + M^* y_2$

$a \% M = x_1$

$b \% M = x_2$

$(a+b) \% M$

$= (x_1 + My_1 + x_2 + My_2) \% M$

$= ((x_1 + x_2) + M(y_1 + y_2)) \% M$

$= (x_1 + x_2) \% M$

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

$$\boxed{(a+b) \% M = (a \% M + b \% M) \% M}$$

2) ✓ Linearity on modular addition!

$$(17 + 9) \% 5 = 26 \% 5 = 1$$

$$17 \% 5 = 2 \quad + \quad 9 \% 5 = 4$$

$$(2 + 4) \% 5$$
$$= 1$$

$$(a + b + c) \% M \rightarrow (a \% M + b \% M + c \% M) \% M$$

Modular Multiplication

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

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

$$(\boxed{69 * 75}) \% 7$$
$$\Downarrow$$
$$2$$

2, 3, 4, 6

$$(6 * 5) \% 7$$

$$= 30 \% 7 = 2$$

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

$$\downarrow$$

$$(x_1 + M * y_1) * (x_2 + M y_2)$$

$$(x_1 x_2 + \cancel{M y_1 x_2} + \cancel{M y_2 x_1} + \cancel{M^2 y_1 y_2}) \% M$$

$$= x_1 x_2 \% M$$

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

$$\boxed{76! \ \% \ 9} \rightarrow \underline{0}$$

$10^9 + 7$

$$\boxed{76! \ \% \ (10^9 + 7)}$$

POWER FUNCTION

100^{100} ← % MOD ~ generally 10^9+7

100^{100} % MOD

⇒ $\boxed{a^b \ \% \ M}$ ⇒ find the most efficient way of doing this

a^b ⇒ a * a * a ___ b times!

```
ans = 1
for i in range(b):
    ans = ((ans % M) * (a % M)) % M
return ans
```

a^b

⇒ TC → O(b)

a^b % MOD

(ans % M) % M

= ans % M

for

ans = ((ans % M) * (a % M)) % M

ans

[0 ... M-1]

TC → O(b)

5 mins Break

POWER FUNCTION → Powerful

$a^{99} \times a$

$a^{100} = a \times a \times a \ldots \ldots a$ 100 times

O(100)

$= a^{50} \times a^{50}$

O(50)

$a^{49} \times a$

$a^{25} \times a^{25}$

$a^{12} \times a^{13}$

$a^{12} \times a^{12} \times a$

100

50

25

12 $a^6 \times a^6$

6 $a^3 \times a^3$

3 a^3

1

Log n

Even
power $(x/2)$ * power$(x/2)$

power (x)

Odd
power $(x/2)$ * power $(x/2)$ * x

$a^b \to a^{b//2}$

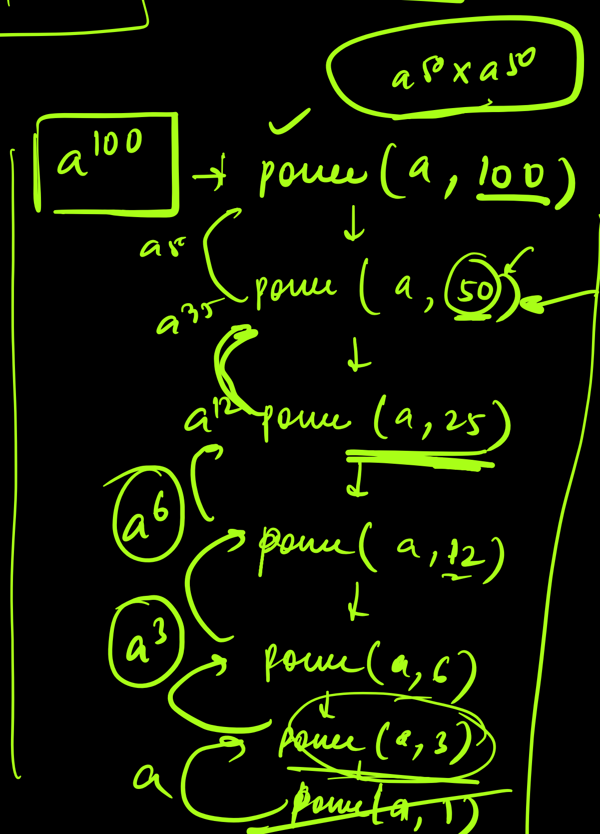
```
def power(a, b):
    if b == 1:
        return a
    x = power(a, b//2)
    if b % 2 == 0:
        return x * x
    else:
        return x * x * a
```

$a^{b//2}$

a^1

ML

$\to O(\log b)$



power(a, 6)

Divisibility Rules

% 2   % 4   % 3   % 9

Divisibility Rule by 2

last digit → even or odd

$(abcde)_{10}$ divisible by 2

⇓ Expand

$10^4 * a + 10^3 b + 10^2 c + 10^1 d + e$ % 2

divisible by 2

$\boxed{e \% 2}$

Divisibility Rule by 4

a b c d e

$$(10^4 * a + 10^3 * b + 10^2 * c + \underline{10^1 d + e}) \% 4$$

$$\underbrace{(10^4 * a) \% 4}_{\checkmark} + \underbrace{(10^3 * b) \% 4}_{\checkmark} + \underbrace{(10^2 * c) \% 4}_{\checkmark}$$

0

100, 1000, 10000

$\boxed{10d + e}$

$\boxed{(de)_{10}}$

it divisible by 4

(abcde) ✓

Divisibility by 3

$(a\,b\,c\,d\,e)_{10} \% 3$

$\underline{(10^4 \times a + 10^3 \times b + 10^2 \times c + 10^1 d + e) \% 3}$

$\Downarrow$

$(10^4 \times a) \% 3 + (\cancel{10^3} \times b) \% 3 + (10^2 \times c) \% 3$

$+ (10^1 d) \% 3$

$(e \% 3)$

$(\underbrace{\cancel{10^4 \% 3}}_{1} \times (a \% 3)) \% 3$

$= \underline{(a \% 3 + b \% 3 + c \% 3 + d \% 3 + e \% 3) \% 3}$

$10 \% 3 = 1$

$100 \% 3 = 1$

$1000 \% 3 = 1$

$10000 \% 3 = 1$

Sum of digits should be divisible by 3

$10 \% 9 = 1$

$100 \% 9 = 1$

$1000 \% 9 = 1$ =

For 9 also → sum of digits

$\underline{10^4} \times 9$ 100 10 $\square$

Last digit should be divisible $\underline{5}$

~~Do~~: Doubts

$\cancel{a_1}$ $\cancel{b_1}$ $\cancel{c_1}$ $\cancel{a_1}$ x $\cancel{b_1}$ $\cancel{c_1}$ y

(1) Take XOR of all no.s in the array ⇓ $x \wedge y$

↓ ↓
1 0 1 0 1
1 1 0 1

⇒ 1 1 0 0 0 (bit positions 3 2 1 0)

& (1 << i) — i: 0 → 1 → 2.

Bit which is different in both the no.s

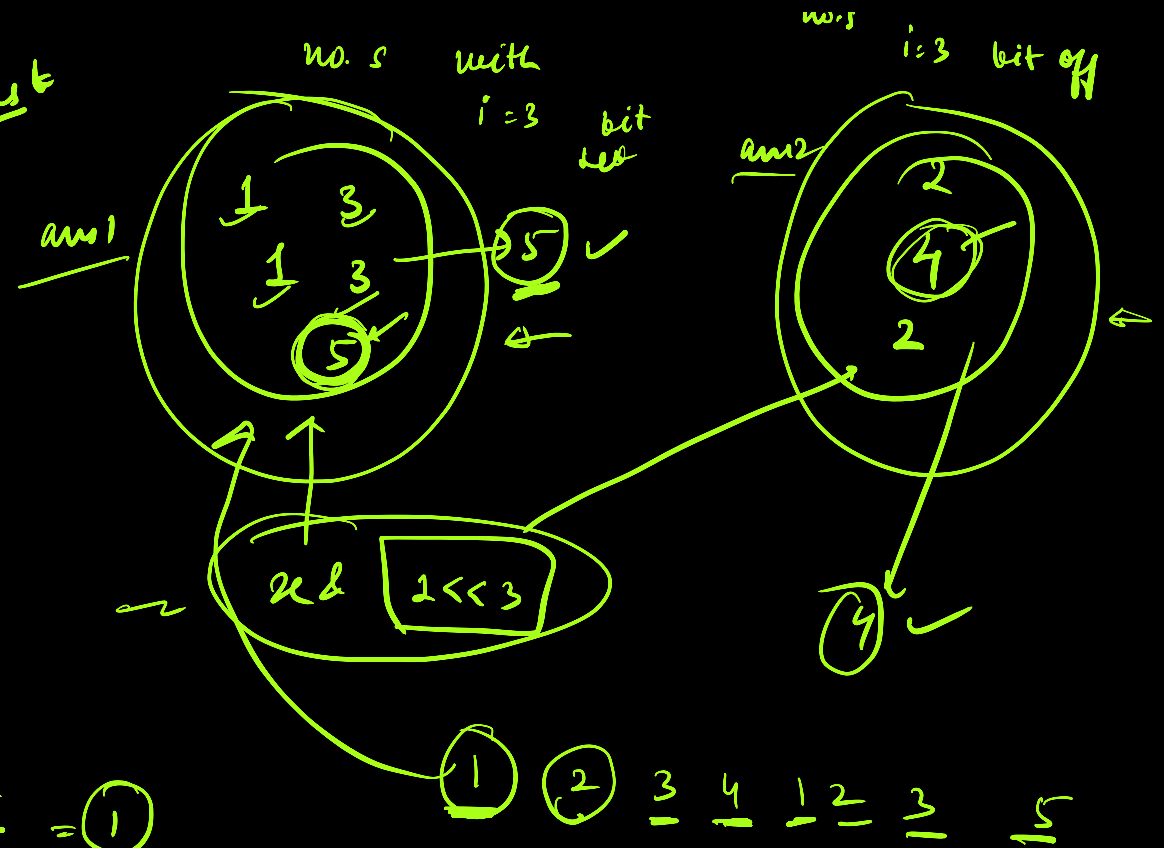
If a bit is SET in XOR value

It means both no.s have that bit different

(2) Find bit that is ON in XOR

⇒ Lets says i = 3 $x \wedge y$

Hardest



4 ^ 5 = 1

~~001~~

i = 0

Maximum satisfactin.

[ ]

Max (a & b & c & d) →

10 11

5

3

1 1 0 0

0 1

for 31 → 0

if 4 no.s are there which have this bit ON ans = 0

31 → 0

I

4 3 2 1 0

0 → 1 0 1 0 1 — & (10000)

→ 1 1 0 0 0

1 0 0 0 0 &

1 0 1 1 1

1 1 0 0 0

1 1 1 0 0

1 1 1 1 1

0 0 0 1 1

1<<4

1<<3

7

ans = 1 1 0 0 0

11000

11 100 → 11010 ← O(N)

& = 11100