Introduction To Modular Arithmetic

↳ overflow ← of value

C, C++, Java → limitation on the max

integer that we can store

long long int → factorial ← large

↳ let's say → $\underbrace{g \% c}$ → ~~range ??~~

↳ $[0, c-1]$

no matter how big g is → it will reduce to $[0, c-1]$

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

ii) $(a * b) \% c \rightarrow ((a \% c) * (b \% c)) \% c$

iii) $(a-b) \% c \rightarrow (a \% c - b \% c + c) \% c$

⇒ Calc → a^b and print your ans modulo

$10^9 + 7$.

$a = 2$ $b = 4$

ans → 16

$a^b \longrightarrow a^{b-1} \times a \longrightarrow$ not an effect on

$\hookrightarrow a^{b-2} \times a$

$\hookrightarrow a^{b-3} \times a \ldots\ldots$

$O(b)$

$$a^b \rightarrow a^{b/2} \times a^{b/2}$$

$$\hookrightarrow a^{b/4} \times a^{b/4}$$

$$T(b) = T\left(\frac{b}{2}\right) + T\left(\frac{b}{2}\right) + O(1)$$

$$T(b) = 2T\left(\frac{b}{2}\right) + O(1)$$

$$\hookrightarrow O(b)$$

$$a^b = \left(a^{b/2}\right)^2$$

$$\hookrightarrow \left(a^{b/4}\right)^2$$

$$\hookrightarrow \left(a^{b/8}\right)^2$$

$$\hookrightarrow \ldots$$

$$O(\log b)$$

$$b \to \frac{b}{2} \to \frac{b}{4} \to \frac{b}{8} \cdots \frac{b}{2^k}$$

$$k = \log_2 b$$

$a^b \% c \rightarrow \left(\left(a^{b/2}\right) \% c \times \left(a^{b/2}\right) \% c \right) \% c$

Recursively $\rightarrow$ TC $\rightarrow$ $O(\log b)$

SC $\rightarrow$ $O(\log b)$

$\gcd(x, y) \rightarrow$ greatest common divisor

↳ highest common factor

$x = p_1^{a} \; p_2^{b} \; \cdots\cdots$

$y = p_1^{a_1} \; p_2^{b_1} \; \cdots\cdots$

$\rightarrow$ common factors exact

p_1	a
p_2	b

$p_1 \rightarrow a_1$

result $p_1^{\min(a, a_1)}$

$30 \rightarrow 2 \times 3 \times 5 \rightarrow 2^1 \times 3^1 \times 5^1$

$18 \rightarrow 2 \times 3 \times 3 \rightarrow 2^1 \times 3^2$

6

$$\begin{array}{l} 2 - 1 \\ 3 - 1 \\ 5 - 1 \end{array}$$

$res = 1 \times 2^{\min(1,1)}$

$\hookrightarrow 2 \times 3^{\min(2,1)}$

$\hookrightarrow 2 \times 3^1$

$\hookrightarrow 6$

gcd → <u>Euclid's algorithm</u>

- → what is ?
- → implementation
- → Intuition
- → Time Comp → proof ?

↳ Let's say we have 2 integers a, b

$a / b \to$ quotient $\to q$

remainder $\to r$

$a > b$

$$\boxed{a = bq + r}$$

Let's assume 'g' is the gcd of a, b

then $\boxed{a \% g == b \% g == 0}$

$a \mid g$ and $b \mid g$ → g divides a and b.

$a = bq + r$

$a - \underbrace{bq}_{} = r$

equality

a is divisble by g

if b is divisible by g then $(b \times q)$ is also divisible by g.

$a - bq = r$

LHS is divisible by g

implies $\Longrightarrow$

is also divisible by g

$\boxed{r = a \% b}$

$a \mid g$ and $b \mid g$ then $(a\%b) \mid g$

consider $a > b$ then

$\gcd(a, b) = \gcd(b, a\%b)$

recursive relation

if $b == 0$ ans is a → base case

$x^2 - x - 1 = 0$ sol^n ??

$D \rightarrow b^2 - 4ac$

$\rightarrow 1 - 4(1)(-1)$

$\rightarrow 1 + 4 \rightarrow \underline{\underline{5}}$

sol^n $\longrightarrow \dfrac{-b \pm \sqrt{D}}{2a}$

roots $\Rightarrow \left.\dfrac{1 \pm \sqrt{5}}{2}\right\}$ special

$$x^2 - x - 1 = 0$$

$$x = x + 0$$

$$x^2 = x + 1$$

$$x^3 = 2x + 1$$

$$x^4 = 3x + 2$$

$$x^5 = 5x + 3$$

$$x(x^4)$$

$$\rightarrow 3x^2 + 2x$$

$$3x + 3 + 2x$$

$$5x + 3$$

0, 1, 1, 2, 3, 5, 8, 13 . . . . .

0 1 2 3 4 5 6 7

$\hookrightarrow \quad x^n = f_n x + f_{n-1}$

$f_n \rightarrow n^{th}$ fib

$$x = \frac{1+\sqrt{5}}{2}, \quad \frac{1-\sqrt{5}}{2}$$

$\alpha \qquad \beta$

$$x^n = f_n x + f_{n-1}$$

$$\hookrightarrow \alpha^n = f_n \alpha + \cancel{f_{n-1}} \quad \text{--- } 1$$

$$\beta^n = f_n \beta + \cancel{f_{n-1}} \quad \text{--- } 2$$

1 - 2

$$\alpha^n - \beta^n = f_n \alpha - f_n \beta$$

$$\alpha^n - \beta^n = f_n (\alpha - \beta)$$

$$\boxed{f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}} \longrightarrow \text{Binet's formula}$$

golden ratio $\phi = \frac{1+\sqrt{5}}{2}$

$f_n \propto \phi^n$

proportion

↳ if we use euclids algorithm to calc $\gcd(a, b)$ → assume we require 'n' steps to calculate $\gcd(a, b)$

Claim $a \geq f_{n+2}$ where f_n is the n^{th} fibonacci

$b \geq f_{n+1}$

$\gcd(a, b) = \gcd(b, a \% b)$

converges in n steps

converges in $(n-1)$ steps

$\underline{\underline{a > b}}$

$a = bq + r$

$r \rightarrow a \% b$

$q \rightarrow \left\lfloor \frac{a}{b} \right\rfloor$

$a = b \times \left\lfloor \frac{a}{b} \right\rfloor + a \% b$

gcd(b, a % b) converges in (n-1) steps

and if we assume this holds true,

$b \geq f_{n-1+2} \longrightarrow b \geq f_{n+1}$ → half part proved

$a \% b \geq f_{n-1+1} \longrightarrow a \% b \geq f_n$

assum → $\left\lfloor \frac{a}{b} \right\rfloor \geq 1$

$a = b \left\lfloor \frac{a}{b} \right\rfloor + a \% b$

$\hookrightarrow \geq 1$

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

$a \geq f_{n+1} + f_n$

$\boxed{a \geq f_{n+2}}$ → fibonacci relation

$$f_n \propto \phi^n$$

$$n \propto \log_\phi f_n$$

$$\left(\begin{array}{l} a \geq f_{n+2} \\ b \geq f_{n+1} \end{array} \right)$$

a, b are also proportional to fibonacci of 1

$$n \approx \log_\phi \min(a, b)$$

steps

$$O(\log \min(a, b))$$