↳ Agenda → Revisit Euclid ↩

Modular Arithmetic

↳ ADA GCD SPOJ

Extended euclid algorithm

Multiplication modular inverse

Linear diophantine eqn]

Prerequisites → elementary maths

loops, if else, recursion

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

③

if b divides a with a remainder r

$lcm = \dfrac{ab}{gcd}$

$a = bq + r$? ? $r = a\%b$

$(a - bq = r)$ $O(\log_{\phi}(\min(a,b)))$

ϕ

$x^2 - x - 1 = 0$

golden ratio

Fibonacci

$x^2 = x + 1$

$x^3 = x \times x^2$

$= x \times (x+1) = x^2 + 1$

$= 2x + 1$

% → modulo

Modular Arithmetic

↪ You need to print ans % 10^9+7 → int 4byte

Q → L, B of a rectangle → area → 10^{24} ← long long int

$L \approx 10^{12}$ $B \approx 10^{12}$

O(1)

$L \rightarrow 10^{12}$ $\quad$ $B \rightarrow 10^{12}$

area % $10^9 + 7$

$(L \times B)$ % $10^9 + 7$

10^{24} % $10^9 + 7$

$\rightarrow$ modular arithmetic

Rules

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

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

$(1+1)\%2$

$2\%2$

0

0

number%m $\rightarrow$ $[0, m-1]$

$[0, 2-1]$

$5\%2 = 1$

$4\%2 = 0$

$3\%2 = 1$

$2\%2 = 0$

$$(a+b)\,\%\,c = (a\,\%\,c + b\,\%\,c)\,\%\,c$$

$$(a * b)\,\%\,c = (a\,\%\,c \times b\,\%\,c)\,\%\,c$$

$$(a-b)\,\%\,c = (a\,\%\,c - b\,\%\,c + c)\,\%\,c$$

post

$$(13-4)\,\%\,5 = (13\,\%\,5 - 4\,\%\,5 + 5)\,\%\,5$$

$$\Rightarrow (3 - 4 + 5)\,\%\,5$$

4 → 1

$4\,\%\,5$

4

$(13-12)\,\%\,5$

$(13\,\%\,5 - 12\,\%\,5 + 5)\,\%\,5$

$(3 - 2 + 5)\,\%\,5 \rightarrow 1$

$\left(\frac{9}{3}\right)\%\,c$??

$$\left(\frac{a}{b}\right) \% C = \left(\frac{a \% C}{b \% C}\right) \% \ldots$$

do

Extra work

$\to 0$

number % C $\longrightarrow$ [0, C-1]

Q → You are given 3 values a, b, c

return $(a^b) \% c$

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

→ a^b → Brute force $O(b)$

$$f(a, b) = f(a, b/2) * f(a, b/2)$$

if $b \% 2 == 0$

return a^b

recurrence ???

$b \to b/2 \to b/4$ ... $b/8$ c

$O(\log b)$

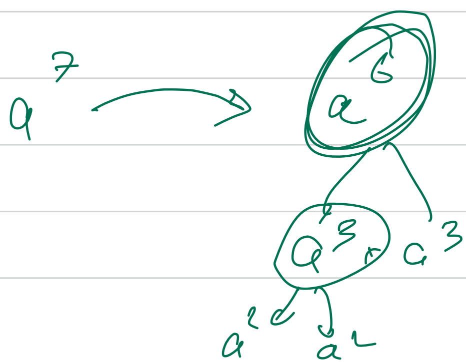
$\log b$

$$f(a,b,c) = \Big(\big(f(a, b/2, c)\big) \% c * \big(f(a, b/2, c)\big) \% c \Big) \% c$$

$\hookrightarrow$ b is even

$$f(a,b,c) = \big(a \% c * f(a, b-1, c) \% c \big) \% c$$

$\hookrightarrow$ b is odd



$$f(a,b,c) = a \times f(a, b/2) \; f(a, b/2)$$

$$a^7 = a \times a^3 \times a^3$$

$(a^b) \% c$ → iteration

→ $\log_2 b$ → operation

while (b → $b/2$ → $b/4$ - - - .)

→ $a \times$

$a \to a^2$ — a^4 - - - . .

$a^7 \longrightarrow$

	~~ans~~ = 1	$a = 3$	$b = 7$
ans = 1	3	3	7
	3	9	3
	27	9	3
	27	81	1
$3^3 \times 3^4$	27×81	81	1
3^7	27×81	81×81	0

Extended Euclid algorithm ??

Let say we have 2 number a and b & then

gcd is $\gcd(a, b) \rightarrow g$

$(ax + by) = g$ → True

$(ax) \% g == 0$

$by \% g == 0$

$g \% g == 0$

x, y

$$\longrightarrow ax + by = \gcd(a, b)$$

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

10^9

Ex $a = 35$ $b = 15$ $g = 5$

$$ax + by = 5$$

for som integ x & y

$x = 1$ $y = -2$

2 variables

$$ax + by = \gcd(a, b) \qquad x \,\&\, y$$

$$a x_1 + b y_1 = \gcd(b, a \% b) = \gcd(a, b) \qquad x_1 \,\&\, y_1$$

$$b x_1 + (a \% b) y = \gcd(b, a \% b)$$

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

$$b x_1 + \left(a - b \left\lfloor \frac{a}{b} \right\rfloor\right) y_1 = \gcd(b, a \% b)$$

$$13 \% 3 = 13 - 3 \times \left\lfloor \frac{13}{3} \right\rfloor$$

$$= 13 - 12$$

$$= 1$$

$x_1, y_1 \rightarrow \gcd(b, a\%b)$
$x, y \rightarrow \gcd(a, b)$

$$b x_1 + \left(a - b \times \left\lfloor \frac{a}{b} \right\rfloor\right) y_1 = \gcd(b, a\%b) = \gcd(a, b)$$

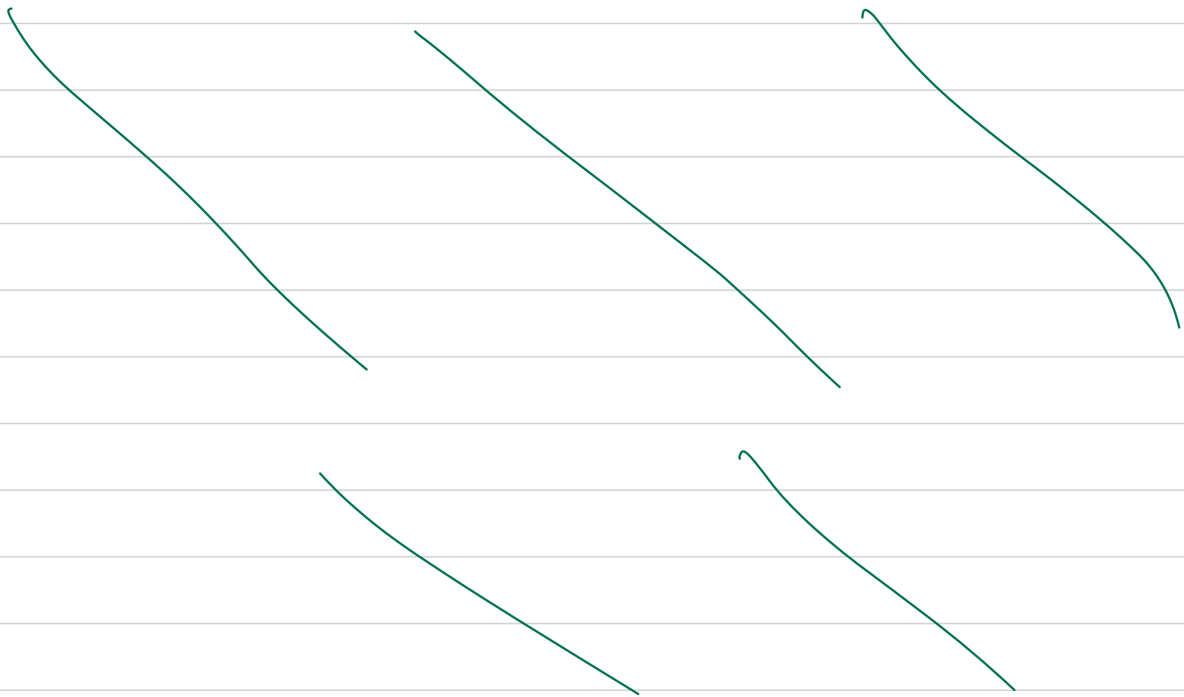
$$b x_1 + \left(a - b \times \left\lfloor \frac{a}{b} \right\rfloor\right) y_1 = a x + b y$$

$$b x_1 + a y_1 - b \times \left\lfloor \frac{a}{b} \right\rfloor y_1 = a x + b y$$

$$b \left(x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1 \right) + a y_1 = a x + b y$$

Comparing coefficients of a & b

$$\boxed{x = y_1} \qquad \boxed{y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1}$$



$x = y_1 \qquad y = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1$

$$ax + by = \gcd(a, b)$$

$$\boxed{a x_1 + b y_1 = \gcd(b, a \% b)}$$

recur relat

any step

3

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

Base Case

$b == 0 \longrightarrow a$

$ax + by = gcd(a, b)$

$ax = a$

$x = 1$

$y = 0$

one of the key application of extended Euclid algo

→ multiplication modular inverse ✓

modular congruency

$$a \cdot b \equiv 1 \pmod{m}$$

b is the multiplicative modular inverse of a

$x \equiv y \pmod{2}$

x is congruent to y on mod 2

$(x-y)/2 \rightarrow$ no remainder

$x \% 2 = y$

$13 \equiv 2 \pmod{11}$

$13 \% 11 = 2$

$(13-2)/11 \Rightarrow$ no rem

$a = 3$
$m = 5$

$b = 2$

$(a \times b) = 1$

$(a \times b) \% m = 1$

b is the multiplicat modular inv

$(3 \times 2) \% 5 = 1$

$(a \times b) \% m = 1$

b is the multiplicative modulo inverse

↳ if $a \times b \equiv 1 \pmod{m}$ → congruency

Q: Given the value of a & m find b

↳ $ab - 1$ (multiple of m)

$ab - 1 = mq$ → multiple of m

$ax + by = \gcd(a, b)$

gu

m

mod Inv

$$ab - 1 = mq$$

$$ab - mq = 1$$

$$ab + m(-q) = 1$$

$$(ab + m\,q' = 1) \rightarrow \text{extended euclid algo}$$

$\gcd(a, m)$

$\gcd(a, m) = 1$

$(ab) \equiv 1 \pmod{m}$

multiplicative mod inverse

$ax + by = c$ → linear diophantine eqn

$c = K * gcd(a, b)$

ADAGCD