Let's start at 9:02 PM

L51
Modular Arithmetic & Euclid's GCD Algorithm

Join Discord - https://bit.ly/ly-discord

RECAP

What is this Modulo Operator? (%)

$a \% b \Rightarrow$ remainder when a is divided by b.

$$a = q * b + r$$

$$r = a - q * b$$

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

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

15

$10 \% 3 = 1$

$13 \% 2 = 1$

$18 \% 5 = 3$

$5 \% 10 = 5$

$-6 \text{ rem } 3 = 0$

$-18 \text{ rem } 5 = 2$

$-25 \text{ rem } 7 = 3$

Weird behaviour on negative numbers

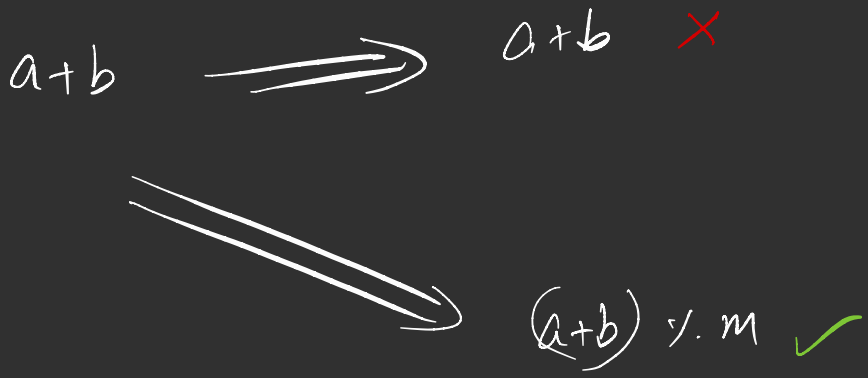
$\frac{13}{5} = 2.\overline{6}$

$-2.\overline{6}$

$\frac{13}{5} \Rightarrow 2$

$\frac{-13}{5} \Rightarrow -2$

What is Modulo Arithmetic?



Why Modular Arithmetic?

Eg. given N, find fact(N).

$1 \le N \le 1000$

ans = 5.4229...168 * 10^{30}

ans % mod => 501253 1

[0, mod-1]

mod = 1000000007

ans % mod.

$1 * 2 * 3 * 4 \ldots \ldots \ldots N$

ans = 1;

```
for(i=2; i<=N; ++i)
    ans = (ans * i) % mod;
```

Addition

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

$a = q_1 * m + r_1 \quad (a \% m \Rightarrow r_1)$

$b = q_2 * m + r_2 \quad (b \% m = r_2)$

$$q_1 m + r_1 + q_2 m + r_2 \Rightarrow (q_1 + q_2)\, m + r_1 + r_2$$

$a = 10^{18} + 5$, $b = 10^{30} + 5127$

$m = 10$

$(a+b) \% 10$

$(r_1 + r_2) \% 10$

$(5+7) \% 10 \Rightarrow 2$

Subtraction

$$(a - b) \% m \Rightarrow ((a \% m) - (b \% m) + m) \% m$$

$a = q_1 * m + r_1$

$b = q_2 * m + r_2$

$\Rightarrow a - b \Rightarrow (q_1 - q_2) * m + \underbrace{r_1 - r_2}$

$r_1 \in [0, m-1]$, $r_2 \in [0, m-1]$

$r_1 - r_2 \in [-(m-1), m-1]$

$a = 10^{31} + 5$, $b = 10^{30} + 5127$

$m = 10$

$(a - b) \% 10$

$(r_1 - r_2 + 10) \% 10$

$(5 - 7 + 10) \% 10$

$\Rightarrow 8 \% 10 \Rightarrow 8$

Multiplication

$$(a * b) \% m \implies ((a \% m) * (b \% m)) \% m$$

$$a = q_1 m + r_1$$

$$b = q_2 m + r_2$$

$$a * b = (q_1 m + r_1) * (q_2 m + r_2)$$

$$= q_1 q_2 m^2 + q_1 r_2 m + q_2 r_1 m + r_1 r_2$$

$$\Rightarrow \underbrace{(q_1 q_2 m + q_1 r_2 + q_2 r_1) * m}_{\text{Irrelevant}} + \underbrace{r_1 * r_2}_{\text{Relevant}}$$

$a = 10^{31} + 5$, $b = 10^{30} + 5127$

$m = 10$

$(a * b) \% 10$

$\Downarrow$

$(r_1 * r_2) \% 10$

$\Downarrow$

$(5 * 7) \% 10$

$\Rightarrow 35 \% 10 \Rightarrow 5$

Find a^n under modulo

Given a & n, find a^n.

$1 \le a \le 10^9$

$1 \le n \le 10^{18}$

Since answer may be large print ans % (10^9+7).

Introduction to GCD

Also called HCF (Highest common factor)

↳ stands for greatest Common Divisor

The largest such numbers which divides both A & B.

$gcd(2, 8) \Rightarrow 2$

$gcd(24, 32) \Rightarrow 8$

$gcd(11, 15) \Rightarrow 1$

$gcd(0, 10) \Rightarrow 10$

Brute Force

```
for( i = min(a,b); i >= 1; --i)
    if (a%i == 0 && b%i == 0)
        return i;
```

Time $\Rightarrow O(\min(a,b))$

A better method

$a = 10590 = 2^2 * 3^1 * 5^3 * 7$

$b = 198 = 2^1 * 3^2 * 11$

$O(\sqrt{\max(a,b)})$

$gcd = 2^1 * 3^1 \Rightarrow 6$

Euclid’s GCD Algorithm

(a > b)

Observation 1

(a, b)

⇓

{f1, f2, f3}

(a-b , b)

⇓

{f1, f2, f3 ——}

If a number is a divisor of both a, b.

$\Rightarrow$ It will be a divisor of a-b also.

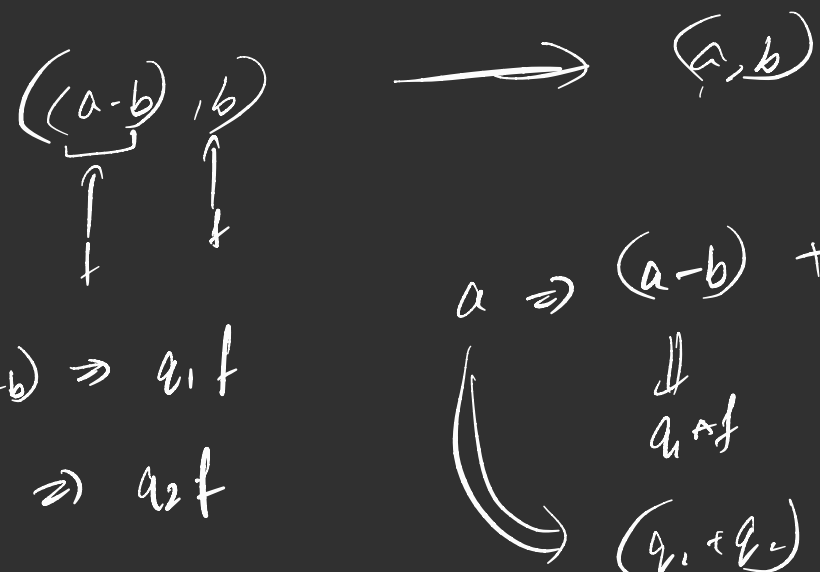
a b

(21, 8) $\Rightarrow$ 1, 2, 4,

a-b, b

(20, 8)

Observation 2



If a number is a divisor of both $(a-b)$ & b, then it will a divisor of a.

$\Longrightarrow$ Common divisors a, b & $a-b, b$ will be same set of numbers.

a = 28 b = 8

(a-b, b)

↓

(20, 8) ⟹ 1, 2, 4

(28, 8) ⟹ 1, 2, 4

$$gcd(a,b) = gcd(a-b, b)$$

$$gcd(28, 8) \Longrightarrow gcd(20, 8)$$

$a > b$

Observation 3

$$gcd(a, b) = gcd(a-b, b)$$

$$gcd(a-b, b) = gcd(a-2b, b)$$

$$gcd(a-2b, b) = gcd(a-3b, b)$$

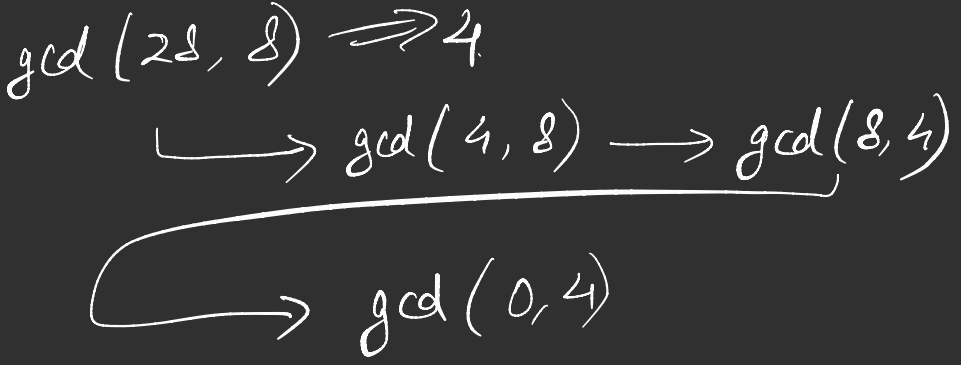
$$\Downarrow$$

$$a - \lfloor \frac{a}{b} \rfloor * b$$

$$\Downarrow$$

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

Example



$(a > b)$

$gcd(a, b)$

$\downarrow$

$(b, a \% b)$

Let's implement

```
int gcd (a, b) {
    if (min(a, b) == 0)
        return max(a, b);
    int mx = max(a, b), mn = min(a, b);
    return gcd (mn, mx % mn);
}
```

Time Complexity

cb algorithm euclid's algorithm.

$\Rightarrow \quad \log(\min(a, b))$

gcd (a, b)

Thank You!

Reminder: Going to the gym & observing the trainer work out can help you know the right technique, but you'll muscle up only if you lift some weights yourself.

So, PRACTICE, PRACTICE, PRACTICE!