Let's begin by 9:03 PM

L53
Modulo Inverse and more Problem Solving

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

Contest tomorrow

Topics from March.

Time ⇒ 3:45 PM to 6:15 PM.

Link will be shared on Discord.
(in #imp-announcements)

RECAP

Modulo Inverse - Intuition

Additive Inverse $\Rightarrow$ $(x \Rightarrow -x)$

$5 \Rightarrow -5$

$0 \Rightarrow 0$

$-10 \Rightarrow 10$

Multiplicative Inverse $\Rightarrow$ $(x \Rightarrow 1/x)$

$5 \Rightarrow 1/5$

$-10 \Rightarrow 1/-10$

$0 \Rightarrow$ not defined

Introduction

Modulo Inverse of a number a (under a given modulo m) is basically the number x such that:

1) $0 \leq x \leq m-1$

2) $a * x \equiv 1 \pmod{m}$

$a = 2 \qquad m = 15$

$x = 1 \Rightarrow 2 \% 15 = 2$

$x = 2 \Rightarrow 4 \% 15 = 4$

$x = 3 \Rightarrow 6 \% 15 = 6$

$\vdots$

$x = 7 \Rightarrow 14 \% 15 = 14$

$x = 8 \Rightarrow 16 \% 15 \Rightarrow 1$

$inv(a) = 8$

Why is it needed?

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

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

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

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

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

$\Rightarrow {}^{n}C_r = \frac{n!}{r!\,(n-r)!}$

$$\frac{num}{den} \pmod m$$

$$\left[\frac{num}{\cancel{den}} \cancel{* den} * inv(den)\right] \pmod m$$

$$\Rightarrow \left[num * inv(den)\right] \pmod m$$

$$\Rightarrow \left[(num \% mod) * inv(den \% mod)\right] \% m$$

$$(a * x) \,\%\, m = 1$$

$$\Downarrow$$

$$\left((a \,\%\, m) * (x \,\%\, m)\right) \,\%\, m$$

$$\Rightarrow \quad inv(a) = inv(a \,\%\, m)$$

How to find?

Extended Euclid's Algorithm

$$x * a + y * b = gcd(a, b)$$

x, y are integers

Eg $a = 10, \quad b = 15 \quad \Rightarrow g = 5$

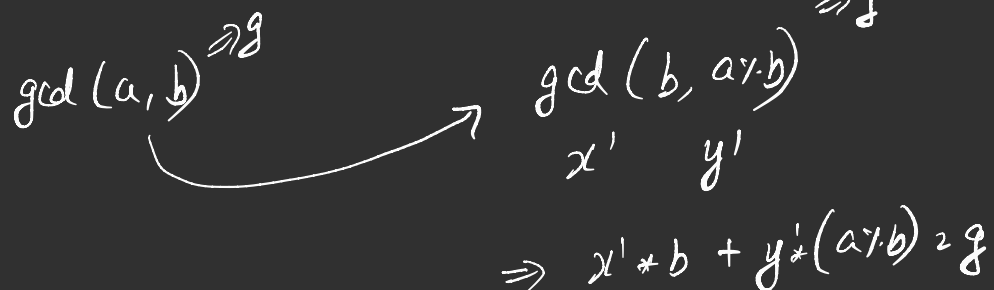
$$2 * 10 + (-1) * 15 = 5 \Longrightarrow$$

$x = 2$

$y = -1$

Is it always possible?

$a, b = 0 \Rightarrow gcd = a$ $\quad x = 1, \quad y = 0$



Solution

$$\Rightarrow x' * b + y' * (a \% b) = g$$

$$\Rightarrow x' * b + y' * \left(a - \left\lfloor \frac{a}{b} \right\rfloor * b\right) = g$$

$$\Rightarrow y' * a + \left(x' - y' * \left\lfloor \frac{a}{b} \right\rfloor\right) * b = g$$

$$x_{new} = y' \qquad y_{new} = x' - y' * \left\lfloor \frac{a}{b} \right\rfloor$$

In brief about LDE

Linear Diophantine equation

$x * a + y * b = c$

Integral Solutions of this equation exist if & only if (a or b is non-zero) & c is a multiple of gcd(a,b)

Let's come back to Modulo Inverse

given a & m, find integral x s.t.

$$(a * x) \% m = 1$$

$$\Rightarrow x * a = k * m + 1$$

(k can be any integer)

$$\Rightarrow x * a + (-k) * m = 1$$

Let $y = -k$

$$\Rightarrow x * a + y * m = 1$$

iff 1 is a multiple of $gcd(a, m)$

For modulo inverse of a to exist,

gcd (a, m) should be 1.

Connecting the dots

$$x * a + y * m = 1$$

$$\Rightarrow x * a + y * m = \gcd(a, m)$$

$$(x \,\%\, m + m) \,\%\, m \Longrightarrow [0, m-1]$$

Let’s implement

1 problem?

Given a string S where 1 <= len(s) <= 10^5.
Find the number of distinct anagrams of
the given string.

Since the answer may be large,
print ans (mod 10^9 + 7)

Eg. abc ⟹ abc, acb, bac, bca, cab, cba ($3!$)

Eg 2. $b_1 a b_2$ ⟹ $a b_1 b_2$, ~~$a b_2 b_1$~~, $b_1 a b_2$, $b_1 b_2 a$, ~~$b_2 a b_1$~~, ~~$b_2 b_1 a$~~

3

10 diff. characters

$f_1, f_2, f_3 \ldots f_{10}$

$$Ans = \frac{(N)!}{f_1! \times f_2! \times f_3! \ldots f_{10}!}$$

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!