

$$(1) \rightarrow 1 \times 2 \times 3 \times 4 \rightarrow 24$$

$$(2) \quad 36$$

$$(3) \quad 30$$

$$\underline{\underline{\text{gcd}(24, 36, 30)}}$$

A, B

Big Oid

$B = 10^{250}$ \rightarrow Cannot be stored in long long int

this no. as a string.

$A = 12$ $B = "25369"$

if $A > B$ $\gcd(A, B) \rightarrow$ euclid's algo

$$B > A \rightarrow \text{gcd}(B, A)$$

$$\text{gcd.}(\underbrace{A}, \underbrace{B \div A})$$

$$\underline{\underline{A \leq 4 \times 10^7}}$$

$$A > B \div A$$

$$\underline{\underline{\leq 4 \times 10^7}}$$

$$A \div B \div A$$

reading the bits

$$25369$$

$$2 \times 10^4 + 5 \times 10^3 + 3 \times 10^2 + 6 \times 10^1 + 9 \times 10^0 \div A$$

modulo answer.

28369

ans = 0

ans += (9 × 10⁰) 9₀₁₂ → 9

ans += (6 × 10¹) 6₀₁₂ → 5 + 9 → 14

ans += (3 × 10²) 3₀₁₂ → 0 + 14 → 14

⋮

Extended Euclid's algo \rightarrow

$$ax + by = \underline{\underline{\gcd(a, b)}} \rightarrow \underline{\underline{eq^n}}$$

$1eq^1$ is given
for a pair (a, b)

Calc x & y

$$ax + by = \gcd(a, b) \quad \text{--- ①}$$

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

$$\text{w.r.t eq}^n \text{ ①}$$

$$bx_1 + \underbrace{(a \% b)}_y = \gcd(b, a \% b)$$

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

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

$$bx_1 + (a - b \lfloor \frac{a}{b} \rfloor) y_1 = \gcd(b, a \% b)$$

from eq ① $ax + by = \underline{\underline{\gcd(b, a \% b)}}$

$$bx_1 + (a - b \lfloor \frac{a}{b} \rfloor) y_1 = ax + by$$

$$ay_1 + b(x_1 - \lfloor \frac{a}{b} \rfloor y_1) = ax + by$$

$$x = y_1 \quad y = \underline{\underline{x_1 - \lfloor \frac{a}{b} \rfloor y_1}}$$

if ($b == 0$)

$$\text{gcd}(a, b) = a$$

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

$$ax = a$$

$$\boxed{x = 1} \leftarrow$$

$$\underline{\underline{y = 0}}$$

(Multiplicative modulo inverse)

$$\text{number} \rightarrow \underline{\underline{2}}$$

$$\text{Invers} \rightarrow \frac{1}{2}$$

$$\boxed{2 \times \frac{1}{2} = 1}$$

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

so, for a given a and m we need to calc
 b viz inverse modulo of a over m .

$$a = 5 \quad m = 12$$

$$(5 \times 1) \% 12 \rightarrow 5$$

$$(5 \times 2) \% 12 \rightarrow 10$$

$$(5 \times 5) \% 12 \rightarrow 3$$

$$(5 \times 5) \% 12 \rightarrow 8$$

$$(5 \times 5) \% 12 = 1$$

$$(A \cdot B) \bmod m = 1$$

Congruency \rightarrow Given a pair x, y

then if $x - y$ is integrally divisible by m , then we say x & y are congruent modulo m .

$$(A \cdot B) \not\equiv 1 \pmod{m}$$

congruent

$$(A \cdot B) \equiv 1 \pmod{m}$$

$AB - 1$ is a multiple of m .

$$AB - 1 = mq \rightarrow \text{some multiple of } \underline{m}$$

$$AB - mq = 1$$

$$AB - mq = 1$$

$$\text{but } -q \approx \phi$$

$$B = x \quad y = q = -q$$

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

$$AB + m\phi = 1 \rightarrow Ax + my = 1$$

unusable

involved

$$Ax + By = \gcd(A, m)$$

$$\gcd(A, m)$$

Extended euclid algo.

Q →

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{n}$$

$$1 \leq n \leq 10$$

$a, b \rightarrow$ integer

$a \neq 0$ $b \neq 0$

find the no. of pairs a, b that satisfy
the abv eq.

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{n}$$

$$\frac{b + a}{ab} = \frac{1}{n}$$

$$na + nb = ab$$

$$ab - na - nb = 0$$

add n^2 on both sides.

$$\begin{aligned} n &\leq 10^6 \\ n^2 &\leq 10^{12} \end{aligned}$$

$$ab - na - nb + n^2 = n^2$$

$$a(b-n) - n(b-n) = n^2$$

$$(b-n)(a-n) = n^2$$

$$\begin{aligned} O(\sqrt{n^2}) \\ \downarrow \\ O(n) \end{aligned}$$

$$n^2 = \underline{x \cdot y} \quad \forall \text{ all factors of } \underline{n^2}$$

$$(a-n)(b-n) = f_1 \times \frac{n^2}{f_1}$$

$$\begin{aligned} a-n &= f_1 \\ b-n &= n^2 / f_1 \end{aligned}$$

$$\begin{aligned} n^2 &\rightarrow f_1 \\ &f_2 \\ &f_3 \\ &\vdots \end{aligned}$$

$$a - n = f_1$$

$$b - n = \frac{n^2}{f_1}$$

$$\left(\begin{array}{l} a = f_1 + n \\ b = \frac{n^2}{f_1} + n \end{array} \right)$$