(1) → 1 × 2 × 3 × 4 → 24

(2) 36

(3) 30

gcd (24, 36, 30)

Big GCD

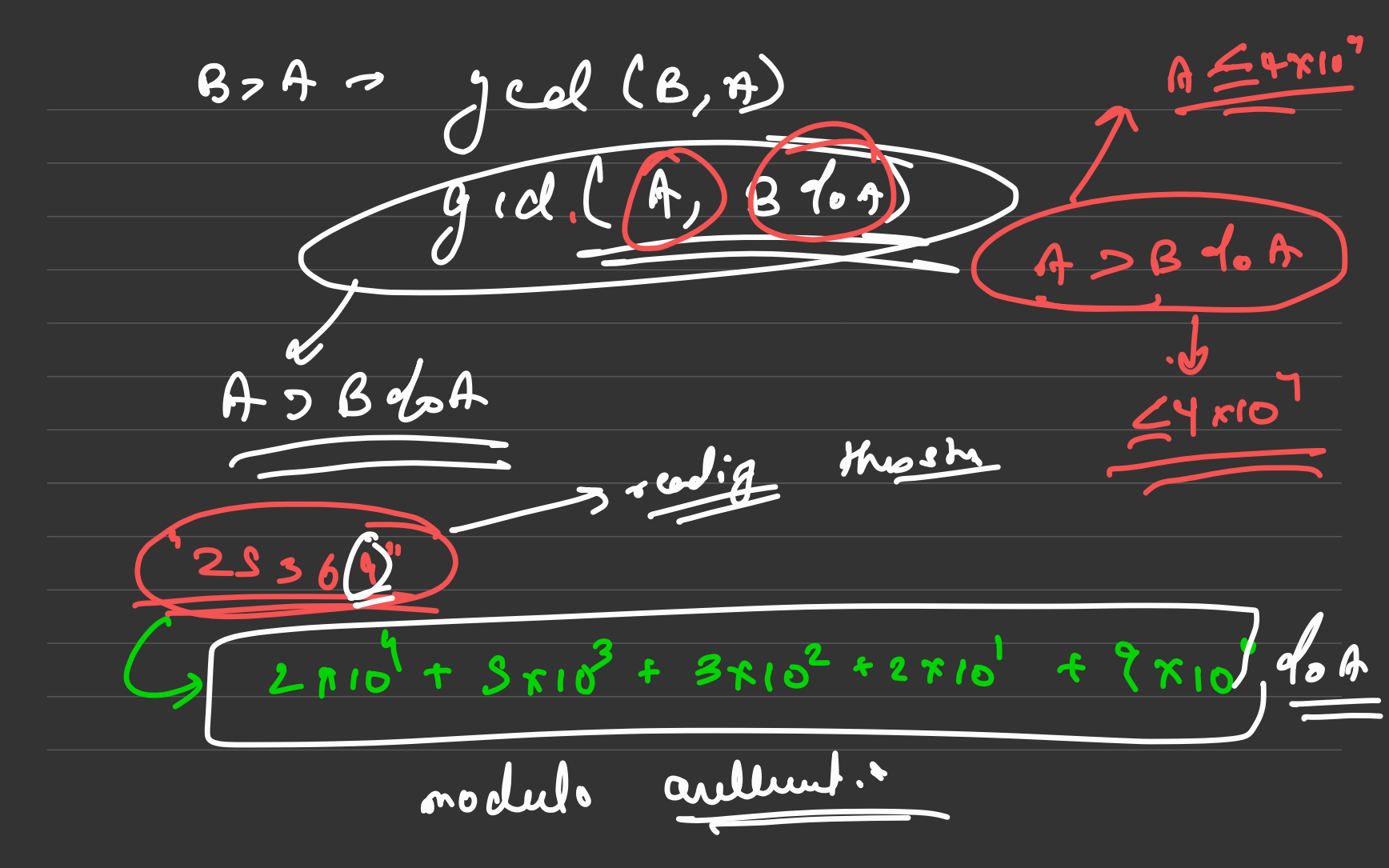
A, B

B ≈ 10^{250} → Cannot be stored in long long int

thus no. as a string.

A = 12 B = "2536 9"

if A > B gcd(A, B) → euclid's algo


B > A → gcd (B, A)
gcd (A, B % A)
A > B % A
A ≤ 4x10^7
≤ 4x10^7
A > B % A
reading
2536
2x10^4 + 5x10^3 + 3x10^2 + 2x10^1 + 6x10^0
% A
modulo arithmetic

23369

ans = 0

ans += $(9 \times 10^0)\ 9_{012}$ → 9

ans += $(6 \times 10^1)\ 9_{012}$ → 5+9 → 14

ans += $(3 \times 10^2)\ 9_{012}$ → 0 + 14 → 14

⋮

Extended Euclid's algo →

$ax + by = gcd(a, b)$ → eqⁿ

eqⁿ is given for a pair (a, b)

Calc x & y

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

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

w.r.t eq^n (1)

$$bx_1 + (a \% b) y_1 = gcd(b, a \% b)$$

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

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

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

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

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

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

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

if (b == 0)

gcd(a, b) = a

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

$ax = a$

$x = 1$

$y = 0$

Multiplicative modulo inverse

number → 2

Inverse → $\frac{1}{2}$

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

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

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

a = 5 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 → Given a pair x, y

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

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

congruent

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

$AB - 1$ is a multiple of m.

$AB - 1 = mq$ → some multiple of m

$AB - mq = 1$

$AB - mq = 1$

but $-q$ as ϕ

$B = x$

$q = \phi = -q$

$AB + m(-q) = 1$

$AB + m\phi = 1$ → $Ax + mY = 1$

multiplicative inverse

$Ax + By = gcd(A, 0)$

$gcd(A, m)$

Extended euclid algo.

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

$1 \le n \le 10^9$ $\quad a, b \to$ integers $\quad a \neq 0 \quad b \neq 0$

find the no. of pairs a, b that satisfy the above eq^n.

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

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

$$na + nb = ab$$

$$ab - na - nb = 0$$

adding n^2 on both sides.

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

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

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

$n \leq 10^6$

$n^2 \leq 10^{12}$

$O(\sqrt{n^2})$

$O(n)$

$n^2 = x \cdot y$ ∀ all factors of n^2

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

$a - n = f_1$

$b - n = n^2 / f_1$

$n^2 \to f_1, f_2, f_3, \ldots$

$$a - n = f_1$$

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

$$a = f_1 + n$$

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