A = 240, 46 = B gcd(240, 46)

∴ extended_euclid (240, 46) = ?

	Index i	Quotient q_i	Remainder r	x_i	y_i
				$= x_{i-2} - q_i x_{i-1}$	$= y_{i-2} - q_i \times y_{i-1}$
	0			$1 \; x_2$	$0 \; y_2$
	1			$0 \; x_1$	$1 \; y_1$
240, 46	2	240/46 = 5	10	x_2 a x_1 $1 - 5 \times 0$ $x = 1$	$0 - 5 \times 1$ $y = -5$
46, 10	3	46/10 = 4	6	$0 - 1 \times 4$ $= -4$	$1 + 5 \times 4$ $= 21$
10, 6	4	10/6 = 1	4	$1 + 4 \times 1$ $= +5$	$-5 - 21 \times 1$ $= -26$
6, 4	5	6/4 = 1	2 Ans	$-4 - 5 \times 1$ $= -9$ x	$21 + 26 \times 1$ $= 47$ y
4, 2	6	4/2 = 2	0	$5 + 18$ $= 23$	$-26 - 47 \times 2$ $= -120$

when r = 0 stops

Pesudocode

```
extended_euclid (int A, int B, int *x, int *y)
{
    int x1 = 0, x2 = 1;
    int y1 = 1, y2 = 0;

    int x, y, r, q, r1, r2;

    for( r2 = A, r1 = B ; r1 != 0 ;
        ∴ q = r2 / r1;
          r = r2 % r1;

        ∴ x = x2 - (q x x1) ;
          y = y2 - (y1 x q) ;

        r2 = r1 ,
        r1 = r ,
        x2 = x1 ,
        x1 = x ,
        y2 = y1 ,
        y1 = y )

    *x = x2 ;
    *y = y2 ;

    ∴ return r2 ;
}
```

$x_i = x_{i-2} - q(x_{i-1})$

x | x2 | q | x1

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

Modular multiplicative inverse using extend euclid

∴ $AX \equiv 1 \pmod m$ ∴ X is modular Inverse of A modulo m

∴ $Ax + my = 1$ ∴ Hence $x \rightarrow MI$ of a

∴ suppose we have to find MI of (3)B modulo (5)A

∴ $5x + 3y = 1$ ∴ there value of y is our MI (ans)

A	B	Reminder, r	Quotient	y_2	y_1	y
r_2	r_1	r	Q	0	1	$y = y_2 - Q \times y_1$
5	(3)	5%3 = (2)	5/3 = 1	0	(1)	= 0 − 1×1
3	2	3%2 = 1	3/2 = 1	1	−1	= 1 − (−1)×1 = 2
2	1	2%1 = 0	2/1 = 2	−1	2	= −1 ÷ 2×2 = −5
1	0	×	×	(2)	−5	

$r_2 = r_1$, $r_1 = r$, $y_2 = y_1$, $y_1 = y$ = (−1)

$r_1 = 0$ loop breaks

value of y_2 is our ans MI

$3x + 5y = 1$ ∴ Here x is our mj of $\frac{3}{A}$ modulo $\frac{5}{B}$

A	B	R	Q	x_2	x_1	x
3	5	3 1.5 = 3	3 1 5 = 0	(1)	(0)	= 1 - 0 = 1
5	3	2	1	0	1	

Now it has become the same solution of

$5x + 3y = 1$

so betten do with

$5x + 3y = 1$

and find value y

Chinese Reminden theorem (weak form)

$X \equiv a_1 \bmod m_1$
$X \equiv a_2 \bmod m_2$
$\vdots$
$X = a_n \bmod m_n$

∴ Find value of X

Rule:-

$m_1, m_2 \cdots m_n$
all pair wise coprime
$\gcd(m_1, m_2) = \gcd(m_2, m_n)$
$= \gcd(m_1, m_n) = \cdots$
$= 1$

Proof

Suppose,

$X \equiv a_1 \bmod m_1$
$X \equiv a_2 \bmod m_2$

∵ we know m_1, m_2 pairwise coprime

∵ from Bezout' Identity,

$m_1 p + m_2 q = 1 \quad —①$
$(Ax + By = 1)$

using extended euclid, we can find p, q

∵ now we can say,

$$X = (a_1 m_2 q + a_2 m_1 p) \bmod m_1 m_2$$

এটা আমার existing মূত। এখন প্রমাণ করবো actually এই সূত্র যেমন $X \equiv a_1 \bmod m_1$, $X \equiv a_2 \bmod m_2$ থেকে কিভাবে

$$X = a_1 m_2 q + a_2 m_1 p$$

From (1)

$$= a_1 (1 - m_1 p) + a_2 m_1 p \quad \text{—— (1)}$$

$$= a_1 - a_1 m_1 p + a_2 m_1 p$$

$$X = a_1 + ((a_2 - a_1) p) m_1$$

$$\therefore X \equiv a_1 \bmod m_1$$

same ভাবে $X \equiv a_2 \bmod m_2$

(Proved)

$X = (a_1 m_2 q + a_2 m_1 p) \bmod m_1 m_2$

why mod with $m_1 m_2$?

→ to find the (smallest solution and Unique) among Infinite solutions

How to sure solution is unique?

suppose we have two solution of x is x_1, x_2

$x_1 \equiv a_1 \bmod m_1$

$x_2 \equiv a_1 \bmod m_1$

we can say $\therefore x_1 \equiv x_2 \bmod m_1$

$\therefore x_1 - x_2 \equiv 0 \bmod m_1$ | $(x_1 - x_2)$ is divisible by m_1

same $x_1 - x_2 \equiv 0 \bmod m_2$ | " " " " m_2

if $(x_1 - x_2)$ is divisbly by both m_1 and m_2 and m_1, m_2 coprime

that means $x_1 - x_2$ is alo divisble by $m_1 \times m_2$

$\therefore x_1 - x_2 \equiv 0 \bmod m_1 m_2$

$\therefore x_1 \equiv x_2 \bmod m_1 m_2$

Hence there exist only one solution

$\therefore x$ is unique to modulo $m_1 m_2$

(proved)

PseudoCode

```
pair<int, int> chinese remainder theorm
                (vector<int> A, vector<int> m)
{
    if (A.size() != m.size())
            { Invalid Input }

    int n = A.size();

    int a1 = A[0]
    int m1 = m[0]
for (int i = 1 ; i < n ; i++ {
    int a2 = A[i], m2 = m[i];
    int p, q;
    extended_euclid (m1, m2, &p, &q);

    int x = (a1 * q * m2 + a2 * p * m1) % m1 * m2

    a1 = x
    m1 = m1 * m2
}
    if (a1 < 0) a1 = a1 + m1

    return { a1, m1 }
```

Chinese Reminden Theonem – Strong

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$x \equiv a_n \bmod m_n$

$m_1, m_2 \ldots m_n$ not copnime

(*) How to sure thene a solution exists?

$\therefore \gcd(m_1, m_2) = g$

we know,

$x \equiv a_1 \bmod m_1$

$x - a_1 \equiv 0 \bmod m_1$ | m_1 divide $x - a_i$

divisor of m_1 like(g) also divides $x - a_i$ (*)

$\therefore x - a_1 = 0 \bmod g$

same $x - a_2 = 0 \bmod g$

$\therefore x - a_1 \equiv x - a_2 \pmod g$

$\therefore a_1 \equiv a_2 \bmod g$

if ~~sta~~ satisfy this condition then thene exist a solution of x

Now solution

∴ we know

$$GCD(m_1, m_2) = g$$

Bezout's Identity

$$\therefore \quad m_1 p + m_2 q = g$$

$$\therefore \quad \frac{m_1}{g} p + \frac{m_2}{g} q = 1 \quad -(1)$$

using ext_gcd we can find p, q

$$\therefore \boxed{X = a_1 \frac{m_2}{g} q + a_2 \frac{m_1}{g} p}$$

now same stykpnoof

$$\therefore \quad x = a_1 \left(1 - \frac{m_1}{g} p\right) + a_2 \frac{m_1}{g} p \quad -(1)$$

$$= a_1 - a_1 \frac{m_1}{g} p + a_2 \frac{m_1}{g} p$$

$$= a_1 + \frac{(a_2 - a_1)}{g} m_1 p$$

$$\therefore \quad x \equiv a_1 \bmod m_1$$

(Same) $$\therefore \quad x = a_2 \bmod m_2$$

proved

$$X = \left(a_1 \frac{m_2}{g} a + a_2 \frac{m_1}{g} p \right) \bmod lcm(m_1, m_2)$$

Pseudocode

Same like weak form

Just some changes

Same

∴ int g = GCD(m1, m2)

∴ if (a1 %. g != a2 %. g) → No solution

int p, q

ext-gcd (m1/g, m2/g, &p, &q)

∴ int mods = m1 / g * m2

$$X = \left(a_1 q \frac{m_2}{g} + a_2 p \frac{m_1}{g} \right) \text{ ~~mod~~ } \%. \text{ mods}$$

a1 = X

if (a1 < 0) a1 += mod

m1 = mod