Number theory : Steps to find the Solution of x linear Congruence

(*) Rules for finding x, in linear Congruence:

General format : $ax \equiv b \pmod{n}$

1) Find $GCD(a, n) = d$ (let)
2) $b/d \rightarrow$ if possible $\rightarrow$ solution exists.
3) Find $d \bmod n$ ($d \% n$) $\rightarrow$ These no. of solution are possible
4) Divide both the sides by d.
5) Multiply both the sides by "Multiplicative inverse of a" i.e. $(a \cdot a^{-1})x = b \cdot a^{-1} \pmod{n}$
6) General eq^n is :

$$x_K = x_0 + K\left(\frac{n}{d}\right)$$

where $K = \{0, 1, 2, \ldots (d-1)\}$

Number theory : Steps to find the Solution of x linear Congruence

(*) Rules for finding x, in linear Congruence:

General format : $ax \equiv b \pmod{n}$

1) Find $GCD(a, n) = d$ (let)
2) $b/d \rightarrow$ if possible $\rightarrow$ solution exists.
3) Find $d \bmod n$ $(d \% n) \rightarrow$ These no. of solution are possible
4) Divide both the sides by d.
5) Multiply both the sides by "Multiplicative inverse of a" i.e. $(a \cdot a^{-1})x = b \cdot a^{-1} \pmod{n}$
6) General eq^n is :

$$x_K = x_0 + K\left(\frac{n}{d}\right)$$

where $K = \{0, 1, 2, \ldots (d-1)\}$

Linear Congruence Example 2 | Number theory | Finding solution of x

Q: $14x \equiv 12 \pmod{18}$ ———— (1)

$ax \equiv b \pmod{n}$ ———— (2)

From eq^n (1) & (2), we can write,

$a = 14$, $b = 12$, $n = 18$

1st step: $GCD(14, 18) = 2 = d$

2nd step: $b/d = 12/2 = 6$ (sol^n exist)

3rd step: $d \bmod n = 2 \bmod 18$ (2 sol^n exist, means at the end we will get 2 values of x)

4th step: $14x \equiv 12 \pmod{18}$

or, $\frac{14}{2} \equiv \frac{12}{2} \left(\bmod \frac{18}{2}\right)$ [Dividing both the sides by d.]

or, $7 \equiv 6 \pmod{9}$

5th step: Multiply by mul. inverse of a

$7x \equiv 6 \bmod 9$

or, $\cancel{7}.\cancel{7}^{-1} x \equiv 6.7^{-1} \bmod 9$

$x \equiv 6.7^{-1} \bmod 9$

$x \equiv 6.4 \bmod 9$

$= 24 \bmod 9$

$\boxed{\therefore x_0 = 6}$

which is the 1 value of x

$(7 \times c) \bmod n = 1$

$(7 \times c) \bmod 9 = 1$

$c = 1)$ $7 \bmod 9 \neq 1$

$c = 2)$ $14 \bmod 9 \neq 1$

$c = 3)$ $21 \bmod 9 \neq 1$

$c = 4)$ $28 \bmod 9 = 1$

6th step : $x_k = x_0 + k\left(\frac{n}{d}\right)$

$$x_1 = 6 + 1\left(\frac{18}{2}\right)$$
$$= 6 + 9$$
$$= 15$$

(Ans)

Chinese Remainder Theorem

Theorem: The Chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots\cdots$$
$$x \equiv a_n \pmod{m_n}$$

Statement: CRT states that the above equations have a unique solution of the moduli are relatively prime.

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \dots + a_n M_n M_n^{-1}) \bmod M$$

Example 1: Solve the following equations using CRT

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Solution:

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

Here,

$x \equiv a_1 \pmod{m_1}$	$x \equiv 2 \pmod 3$
$x \equiv a_2 \pmod{m_2}$	$x \equiv 3 \pmod 5$
$x \equiv a_3 \pmod{m_3}$	$x \equiv 2 \pmod 7$

Given		To Find	
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$ M
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$ =105

$\therefore M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times M_1^{-1} = 1 \bmod 3$

$35 \times 2 = 1 \bmod 3$

$\therefore M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times M_2^{-1} = 1 \bmod 5$

$21 \times 1 = 1 \bmod 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$15 \times M_3^{-1} = 1 \bmod 7$

$15 \times 1 = 1 \bmod 7$

$M_3^{-1} = 1$

$\therefore X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= 233 \bmod 105$

$= 23$

(Ans)