Solution of linear congruence equations

Remember $ax \equiv b \pmod m \iff (a,m) \mid b$ [$\because (a,m) =$ g.c.d of a & m, no of solu's $= (a,m)$.]

Solve ① $9x \equiv 12 \pmod{15}$ — ①

Here $a = 9$, $m = 15$, $b = 12$

$(a,m) = (9,15) = 3$ and $3 \mid 12$

$\therefore$ ① has solution

no of solu's of ① (incongruent) $= (a,m) = 3$

$9x \equiv 12 \pmod{15}$

$\Rightarrow x = \dfrac{12+15k}{9}$

For $k=1$, $12+15k = 27$ and $\dfrac{12+15k}{9} = 3$ for $k=1$

$\therefore x = 3$ is a solu of ① say x_0

$\therefore$ no of solu's (incongruent) of ① are

$x_0,\ x_0 + \dfrac{m}{d},\ x_0 + 2\cdot\dfrac{m}{d}$

$3,\ 3 + \dfrac{15}{3},\ 3 + 2\cdot\dfrac{15}{3}$

$\Rightarrow 3, 8, 13$

i.e $x_1 = 3$, $x_2 = 8$, $x_3 = 13$ are 3 incongruent solu's of $9x \equiv 12 \pmod{15}$.

② **Solve** $6x \equiv 15 \pmod{21}$ — (Ex)

Solu Given $6x \equiv 15 \pmod{21}$ — ①

$d = (6,21) = 3$ & $3 \mid 15 \Rightarrow$ ① has solution

Total no of incongruent solu's of ① are $(6,21) = 03$

namely $x_0,\ x_0 + \dfrac{m}{d},\ x_0 + 2\cdot\dfrac{m}{d}$ where $m = 21$, $d = 3$

To find x_0:

$6x \equiv 15 \pmod{21}$

$\Rightarrow x = \dfrac{15+21k}{6}$, k is an integer, search x as positive integer, for any k

यहाँ पर k की वो value choose करेंगे जो $(15+21k)$ को 6 से भाग देने पर शेष शून्य आवे

$15+21k = 36$ for $k=1$ and $6 \mid 36$

$\therefore x = 6 = x_0$ say

$\therefore$ Total incongruent solutions are $\qquad$ $\because$ Total incongruent solu's are

$$6,\ 6+\frac{21}{3},\ 6+2\times\frac{21}{3} \qquad \left[x_0,\ x_0+\frac{m}{d},\ x_0+2.\frac{m}{d}\right]$$

i.e 6, 13, 20 are three incongruent solu's of (1).

(3) Solve $9x \equiv 21 \pmod{23}$

Given equation is

$$9x \equiv 21 \pmod{23} \quad \text{——— (1)}$$

Here $(9, 23) = 1$ [g.c.d of 9 & 23]

and 1 divides 21

$\Rightarrow$ Equ. (1) has solution

$$(1) \Rightarrow \quad x = \frac{21+23k}{9}$$

[यहां पर हम x की value positive integer search करेंगे

for any integer k, $21+23k$ = multiple of 9

$k=1$, $x = \frac{44}{9} \notin I$, $k=2$, $x = \frac{21+46}{9} = \frac{67}{9} \notin I$

$k=3$, $x = \frac{21+69}{9} = \frac{90}{9} = 10$]

$\therefore$ $x = 10 = x_0$, say

. Equ (1) has only one solu as $(9,23) = 1$

$\therefore$ $x_0 = 10$ is only solution of (1).

(4) Solve $9x \equiv 21 \pmod{30}$

Solution. Given equation is

$$9x \equiv 21 \pmod{30} \quad \text{——— (1)}$$

$(9, 30) = 3$ and $3 \mid 21$

$\Rightarrow$ Equation (1) has solution

As $(9,30) = 3 \Rightarrow$ Equ (1) has (3) incongruent solu's

namely $x_0,\ x_0+\frac{m}{d},\ x_0+2.\frac{m}{d}$ ——— (2)

$$(1) \Rightarrow \quad x = \frac{21+30k}{9}$$

$$x = \frac{21+30\times 2}{9} = 9 \Rightarrow x_0 = 9$$

$\therefore$ Required solutions of (1) are

$$9,\ 9+\frac{30}{3},\ 9+2\times\frac{30}{3}$$

i.e, 9, 19, 29. Ans

(3) Solve $49x \equiv 47 \pmod{81}$

Solution. Given equation is (or Linear congruence eqn)

$$49x \equiv 47 \pmod{81} \quad \text{--- (1)}$$

Here $(49, 81) = 1$ and $1 | 47 \Rightarrow$ (1) has only one solution [as $d = 1$ ie g.c.d of $(49, 81) = 1$]

Now (1) $\Rightarrow$ $x = \dfrac{47 + 81k}{49}$

$x = 77$

$49 \times 2 = 98$
$49 \times 3 = 147$
$49 \times 4 = 196$
$49 \times 5 = 245$
for $k = 46$
$47 + 3726$
$81 \times 46 = 3726$

$47 + 81 = 128$
$47 + 162 = 209$
$47 + 243 = 290$
$47 + 324 = 371$
$47 + 405 = 452$

Second method After converting into Diophantine form

$$49x - 81y = 47$$

$$49x = 81y + 47 = (49 \times 2 - 17)y + (49 - 2)$$

$$x = \frac{(49 \times 2 - 17)y + (49 - 2)}{49}$$

$$x = 2y + 1 - \frac{17y - 2}{49}$$

$$x = 2y + 1 - \left(\frac{17y + 2}{49}\right)$$

$$\frac{17y + 2}{49} = u$$

$$17y + 2 = 49u$$

$$y = \frac{49u - 2}{17}$$

$$y = \frac{(51 - 2)u - 2}{17}$$

$$y = 3u - \left(\frac{2u + 2}{17}\right)$$

$\dfrac{2u + 2}{17} = v$, Take $v = 0 \Rightarrow 2u + 2 = 0$
$\Rightarrow u = -1$

$$17y + 2 = 49(-1)$$

$$17y = -2 - 49 = -3 \Rightarrow y = -3$$

$\therefore x = 2y + 1 - u = -6 + 1 + 1$ $\left[\begin{matrix} y = -3 \\ u = -1 \end{matrix}\right]$

$x = -4$

$\therefore -4 \pmod{81} = 4 \pmod{81} \Rightarrow x = 77$

Scanned with CamScanner

CH-04 (26) Number Theory
Pdf-02 Dr Sahsh Kumar

(6) Solve $12x \equiv 44 \pmod{59}$

Solution. Given linear congruence equation is

$$12x \equiv 44 \pmod{59} \quad \text{——} (1)$$

Here $(12, 59) = 1$ and $1 \mid 44$

$\Rightarrow$ (1) has one incongruent solution [as $d=1$]

(1) $\Rightarrow$ $x = \dfrac{44 + 59k}{12}$

For $k=8$

$x = 43$

Table of 12

$12, 24, 36, 48, 60, 72, 84, 96$

$\underset{9}{108}, \underset{10}{120}, \underset{11}{132}, \underset{12}{144}, \underset{13}{156}, \underset{14}{168}$

$\underset{15}{180}, \underset{16}{192}, \underset{17}{204}, \underset{18}{216}, \underset{19}{228}, \underset{20}{240}$

$\underset{21}{252}, \underset{22}{264}, \underset{22}{276}, \underset{22}{288}$

$\dfrac{59 \times 1 + 44}{12}$ × ~~216+33~~ 62.66

$\dfrac{59 \times 2 + 44}{12} = \dfrac{162}{12}$ ×

$\dfrac{59 \times 3 + 44}{12} = \dfrac{221}{12}$ ×

$\dfrac{59 \times 4 + 44}{12} = \dfrac{280}{12}$ ×

$\dfrac{59 \times 5 + 44}{12} = \dfrac{339}{12}$ ×

$\dfrac{59 \times 6 + 44}{12} = \dfrac{398}{12}$ ×

$\dfrac{59 \times 7 + 44}{12} = \dfrac{457}{12}$ ×

$\dfrac{59 \times 8 + 44}{12} = \dfrac{516}{12} = 43$

Second method

$$12x \equiv 44 \pmod{59}$$

$$\Rightarrow 12x - 59y = 44$$

$$12x = 59y + 44$$

$$x = \frac{(60-1)y + (48-4)}{12}$$

$$x = 5y + 4 - \left(\frac{y+4}{12}\right)$$

$$y + 4 = 12u$$

$$y = 12u - 4$$

Take $u = 0$ $\Rightarrow$ $y = -4$

$$x = 5y + 4 - 0 = 5(-4) + 4 = -20 + 4$$

$$x = -16 \pmod{59}$$

$$x = -16 + 59k \Rightarrow x = -16 + 59$$

$$x = 43 \pmod{59}$$

$\therefore$ Req. Solution is $x \equiv 43 \pmod{59}$.

(7) Solve $47x \equiv 11 \pmod{249}$

Sol

Soln. Given $47x \equiv 11 \pmod{249}$ — (1)

Here $(47, 249) = 1$ and $1 \mid 11$

$\Rightarrow$ (1) has solution

and no of solution of (1) is only one as $d = 1$ $[d = (47, 249)]$

(1) $\Rightarrow$ $47x - 249y = 11$

$[47 \times 5 = 235$ ✓, $47 \times 6 = 282$

$47x = 249y + 11$

$x = \frac{(47 \times 5 + 14)y + 11}{47}$

$x = 5y + \frac{14y + 11}{47}$

$\frac{14y+11}{47} = u$

50 ✓, $49 = 14 \times 3 + 5$, $47 = 14 \times 4 + 9$

$14y = 47u - 11$

$y = \frac{(14 \times 3 + 5)u - [14 - 3]}{14}$

$y = 3u - 1 + \frac{5u + 3}{14}$

$\frac{5u+3}{14} = v$

$[3 = 5 - 2$

$5u = 14v - 3$

$u = \frac{(15-1)v - 3}{5}$

$u = \frac{(15-1)v - (5-2)}{5}$

$u = 3v - 1 - \left(\frac{v-2}{5}\right)$

$\frac{v-2}{5} = w$ Take $w = 0 \Rightarrow v = +2$

$\frac{5u+3}{14} = v \Rightarrow 5u + 3 = 14(+2)$

$5u = -3 + 28 \Rightarrow u = 5$

$14y + 11 = 47u \Rightarrow 14y = 47 \times 5 - 11 = 235 - 11$

$\Rightarrow 14y = 224 \Rightarrow y = 16$

$x = 5y + u \Rightarrow x = 5 \times 16 + 5$ $[u = 5]$

$x = 85$

ii Req solution of $47x \equiv 11 \pmod{249}$ is

$$x \equiv 85 \pmod{249}.$$

State and prove Chinese Remainder theorem.

Statement. Let $m_1, m_2, m_3, \ldots, m_r$ be pairwise prime numbers such that $(m_i, m_j) = 1$ for $i \neq j$.

Then, the system of linear congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_r \pmod{m_r}$$

has a Unique Solution.

Proof. Let $m_1, m_2, m_3, \ldots, m_r$ be pairwise prime numbers such that $(m_i, m_j) = 1$ for $i \neq j$.

To prove
$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_r \pmod{m_r} \end{aligned}\right\} \quad \text{—} \ (1)$$

has unique solution.

Let $m = (m_1)(m_2)(m_3)\cdots(m_r)$

Let for each $k = 1, 2, 3, \ldots, r$

$$M_k = \frac{m}{m_k}$$

Since it is given $(m_i, m_j) = 1$

$$\Rightarrow (M_k, m_k) = 1$$

$\Rightarrow \exists$ linear congruence equation — (2)

$$M_k x \equiv 1 \pmod{m_k}$$

which will have a unique solution as $(M_k, m_k) = 1$ and 1 divide 1.

For each k, equation (2) will have a unique solution

i.e for $k=1$ we shall have $M_1 x \equiv 1 \pmod{m_1}$

$k=2$ we shall have $M_2 x \equiv 1 \pmod{m_2}$

$\vdots$

$k=r$ we shall have $M_r x \equiv 1 \pmod{m_r}$

Each the above linear congruence equation will have unique solution namely $x_1, x_2, \ldots, x_r$

So the required solution of the system (1) will be

$$\bar{x} = (a_1 x_1 M_1 + a_2 x_2 M_2 + \cdots + a_r x_r M_r) \pmod m$$

Uniqueness: suppose $\bar{x_1}$ and $\bar{x_2}$ be any two different solutions of the given system (1) then

$$\bar{x_1} \equiv \bar{x_2} \pmod m$$

$$\Rightarrow m \mid (\bar{x_1} - \bar{x_2})$$

$$\Rightarrow \{(m_1)(m_2)\cdots(m_r)\} \mid (\bar{x_1} - \bar{x_2}) \qquad [(m_i, m_j) = 1]$$

which is possible only when $(\bar{x_1} - \bar{x_2}) = 0$

as $(\bar{x_1} - \bar{x_2}) < \{(m_1)(m_2)\cdots(m_r)\}$

[Here $m = (m_1)(m_2)\cdots(m_r)$]

$$\Rightarrow \bar{x_1} = \bar{x_2}$$

$\therefore$ The solution must be unique.

Example. 1 solve
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solution Given
$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}\right\} \quad \text{—— } (1)$$

Here $m_1 = 3,\ m_2 = 5,\ m_3 = 7$ Clearly $(m_i, m_j) = 1$, $i = 1,2,3$, $j = 1,2,3$

$m = 3 \times 5 \times 7 = 105$

Given $a_1 = 2,\ a_2 = 3,\ a_3 = 2$

$$M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$$
$$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$$
$$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$$

Now, we have
$$M_k x \equiv 1 \pmod{m_k}$$

$$\left.\begin{aligned} \text{For } k=1 \quad & M_1 x \equiv 1 \pmod{m_1} \\ k=2 \quad & M_2 x \equiv 1 \pmod{m_2} \\ k=3 \quad & M_3 x \equiv 1 \pmod{m_3} \end{aligned}\right\} \quad \text{—— } (2)$$

system (2) $\Rightarrow$
$$35x \equiv 1 \pmod{\overset{3}{\cancel{7}}} \quad \text{—— } (3)$$
$$21x \equiv 1 \pmod 5 \quad \text{—— } (4)$$
$$15x \equiv 1 \pmod 7 \quad \text{—— } (5)$$

(3) $\Rightarrow$ $x = \dfrac{1+3k}{35} \Rightarrow x_1 = 2$ for $k = 23$

(4) $\Rightarrow$ $x = \dfrac{1+5k}{21} \Rightarrow x_2 = 1$ for $k = 4$

(5) $\Rightarrow$ $x = \dfrac{1+7k}{15} \Rightarrow x_3 = 1$ for $k = 2$

$\therefore$ Req. solution is
$$\bar{x} \equiv (x_1 a_1 M_1 + x_2 a_2 M_2 + x_3 a_3 M_3) \pmod m$$
$$\equiv (2 \times 2 \times 35 + 1 \times 3 \times 21 + 1 \times 2 \times 15) \pmod{105}$$
$$\equiv (2\times 70 + 63 + 30) \pmod{105}$$
$$\equiv 233 \pmod{105}$$
$$\bar{x} \equiv 23 \pmod{105}, \quad \text{Req. answer.}$$

140
63
30
233

(2) **Solve** Solve $x \equiv 3 \pmod{11}$
$x \equiv 5 \pmod{19}$
$x \equiv 10 \pmod{29}$

Solution. Given

$$\left.\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{19} \\ x &\equiv 10 \pmod{29} \end{aligned}\right\} \quad \text{--- (1)}$$

Here $m_1 = 11$, $m_2 = 19$, $m_3 = 29$

$a_1 = 3$, $a_2 = 5$, $a_3 = 10$

clearly $(m_i, m_j) = 1$, $i = 1, 2, 3$. $j = 1, 2, 3$

$$m = 11 \times 19 \times 29$$

$$M_1 = \frac{m}{m_1} = 19 \times 29$$

$$M_2 = \frac{m}{m_2} = 11 \times 29$$

$$M_3 = \frac{m}{m_3} = 11 \times 19$$

Now, we have

$$\left.\begin{aligned} M_1 x &\equiv 1 \pmod{m_1} \\ M_2 x &\equiv 1 \pmod{m_2} \\ M_3 x &\equiv 1 \pmod{m_3} \end{aligned}\right\} \quad \text{--- (2)}$$

$$\Rightarrow \begin{aligned} (19 \times 29)\, x &\equiv 1 \pmod{11} \quad \text{--- (3)} \\ (11 \times 29)\, x &\equiv 1 \pmod{19} \quad \text{--- (4)} \\ (11 \times 19)\, x &\equiv 1 \pmod{29} \quad \text{--- (5)} \end{aligned}$$

(3) $\Rightarrow$ $x \equiv \dfrac{1 + 11k}{19 \times 29} = \dfrac{1 + 11k}{551} \Rightarrow x_1 = 1$ for $k = 50$

(4) $\Rightarrow$ $x = \dfrac{1 + 19k}{11 \times 29} = \dfrac{1 + 19k}{319} \Rightarrow x_2 = 14$ for $k = 235$

(5) $\Rightarrow$ $x = \dfrac{1 + 29k}{11 \times 19} = \dfrac{1 + 29k}{209} \Rightarrow x_3 = 5$ for $k = 36$.

$\therefore$ Req. soln is $\bar{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 \pmod{m}$

$$\bar{x} = 3 \times 551 \times 1 + 5 \times 319 \times 14 + 10 \times 5 \times 209 \pmod{6061}$$

$$\bar{x} \equiv 34433 \pmod{6061} \Rightarrow \bar{x} \equiv 4128 \pmod{6061}$$

(3) Find an integer which leaves remainder 5 when divided by 11 and 2 when divided by 19.

Hint. $x \equiv 5 \pmod{11}$
$x \equiv 2 \pmod{19}$

Ans $x = 192 \pmod{209}$

(4) Solve $x \equiv 3 \pmod 6$
$x \equiv 5 \pmod 7$
$x \equiv 2 \pmod{11}$

Ans $x \equiv 453 \pmod{462}$

(5) Remember

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{n} \end{aligned}\right\} \quad \text{—(1)}$$

System (1) is solvable iff $(m_i, m_j) \mid (a_i - a_j)$

ex
$$\left.\begin{aligned} x &= 5 \pmod 8 \\ x &\equiv 9 \pmod{12} \\ x &\equiv 3 \pmod{18} \end{aligned}\right\} \quad (I)$$

System (1) is solvable as $(8,12) \mid (5-9) \Rightarrow 4 \mid 4$
$(8,18) \mid (5-3) \Rightarrow 2 \mid 2$
$(12,18) \mid (9-3) \Rightarrow 6 \mid 6$.

(11) Solve $f(x) = (x^3 + x^2 + 4x + 29) \equiv 0 \pmod{125}$ is satisfied by $x = 109$. —(1)

Soln. Given $f(x) = x^3 + x^2 + 4x + 29$

To show $f(109) \equiv 0 \pmod{125}$

Now $f(109) = [(109)^3 + (109)^2 + 4 \times 109 + 29]\ [\bmod (125)]$
$= (109)^3 \pmod{125} + (109)^2 \pmod{125} + \cancel{4x \bmod}$
$+ (4 \times 109) \bmod 125 + 29 \pmod{125}$ —(2)

$29 \equiv 29 \pmod{125}$ —(3)
$4 \times 109 \equiv -64 \pmod{125}$ —(4)
$(109)^2 \equiv 6 \pmod{125}$ —(5)
$(109)^3 \equiv 29 \pmod{125}$ —(6)

$109 \times 4 = 436 \pmod{125}$
$109 \equiv -16 \pmod{125}$
$(109)^2 \equiv 256 \pmod{125}$
$(109)^3 \equiv 654 \pmod{125}$
$125 \times 5 = 625$

$$\{(109)^3 + (109)^2 + 4\times 109 + 29\} \equiv (29 - 64 + 06 + 29) \bmod (125)$$
$$\equiv 0 \pmod{125}$$

$\Rightarrow f(109) \equiv 0 \pmod{125}$

ii $f(x) = (x^3 + x^2 + 4x + 29) \equiv 0 \pmod{125}$ is satisfied by 109.