19/12/22

Linear congruence :

A congruence of the form $ax \equiv b \pmod{m}$ where a, b and $m \in z^+$ and x is an unknown integer is said to be a "linear congruence" in one variable.

Eg:- $2x \equiv 3 \pmod{4}$

$3x \equiv 4 \pmod{6}$

*The values of x that satisfy the linear congruence is said to be the solution of the linear congruence.

Ex:- $3x \equiv 4 \pmod{2}$.

$x=2$, $x=4$, $x=6$, etc

particularly, $\{\ldots -4, -2, 0, \underline{2}, 4, \ldots\}$ is a sol'n.

i.e; sol'n is $x \equiv 2 \pmod{2}$

2.

2. $4x \equiv 8 \pmod{6}$

$x=2$, $x=5$, $x=8$, $x=11$, $x=14$, $x=17$

sol'ns are, $\{\ldots -10, -4, \underline{2}, 8, 14, 20, \ldots\}$ i.e; $x \equiv 2 \pmod{}$

$\{\ldots -7, -1, \underline{5}, 11, 17, \ldots\}$ i.e; $x \equiv 5 \pmod{}$

48/12/36

3. $6x \equiv 12 \pmod{9}$

$x=2$, $x=5$, $x=8$, $x=11$, $x=14$, $x=17$

sol'ns are, $\{\ldots -16, -7, \underline{2}, 11, 20, \ldots\}$ i.e; $x \equiv 2 \pmod{9}$

$\{\ldots -13, -4, \underline{5}, 14, 23, \ldots\}$ i.e; $x \equiv 5 \pmod{9}$

$\{\ldots -10, -1, \underline{8}, 17, 26, \ldots\}$ i.e;; $x \equiv 8 \pmod{9}$

4. $7x \equiv 3 \pmod{6}$

$x \not\in$ This congruence has no solution.

Statement: If $a, b \in z$ & $m \in z^+$ and $(a, m) = d$ then

(i) if $d \nmid b$ then $ax \equiv b \pmod{m}$ has no sol'n.

(ii) if $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d incongruent (distinct) solns

Statement-2 : If $x \equiv x_0 \pmod m$ is a solution of the linear congruence $ax \equiv b \pmod m$ then the list of all incongruent solutions are,

$$x = x_0 + \frac{m}{d}t \text{ for } t = 0, 1, 2, \ldots, d-1$$

Ex:- 1. $4x \equiv 8 \pmod 6$

$a = 4, b = 8, m = 6$

$(a, m) = (4, 6) = 2 = d$ as $2 | 8$ i.e., $d | b$

$\therefore$ system has 2 solutions.

Here, $x = 2$ is a sol'n

i.e., $x \equiv 2 \pmod 6$

Now, $x_0 = 2$

the other sol'n is,

$x = x_0 + \frac{m}{d}t$ where $t = 1$

$= 2 + \frac{6}{2}(1)$

$= 5$

$\therefore x = 5$ is the other sol'n. $x \equiv 5 \pmod 6$

2. $6x \equiv 18 \pmod 9$

$a = 6, b = 18, m = 9$

$(a, m) = (6, 9) = 3$ as $3 | 18$

system has 3 sol'ns.

$x = 0$, is a sol'n

i.e., $x \equiv 0 \pmod 9$

other sol'ns are,

$x = x_0 + \frac{m}{d}t$ where $t = 1, 2$

$x = 0 + \frac{9}{3}(1)$, $x = 0 + \frac{9}{3}(2)$

$x = 3$, $x = 6$

$\Rightarrow x \equiv 3 \pmod 9$, $\Rightarrow x \equiv 6 \pmod 9$

H/W 19/12/22

1) show that each of the following congruences holds.

(a) $13 \equiv 1 \pmod 2$

$a = 13, b = 1, m = 2$

$a - b = 12$

$2 | 12$

$\therefore 13 \equiv 1 \pmod 2$

(d) $69 \equiv 62 \pmod 7$

$a = 69, b = 62, m = 7$

$a - b = 7$

$7 | 7$

$\therefore 69 \equiv 62 \pmod 7$

(b) $22 \equiv 7 \pmod 5$

$a = 22, b = 7, m = 5$

$a - b = 15$

$5 | 15$

$\therefore 22 \equiv 7 \pmod 5$

(c) $91 \equiv 0 \pmod{13}$

$a=91, b=0, m=13$

$a-b=91$

$13 \mid 91$

$\therefore 91 \equiv 0 \pmod{13}$

(e) $-2 \equiv 1 \pmod{3}$

$a=-2, b=1, m=3$

$a-b=-3$

$3 \mid -3$

$\therefore -2 \equiv 1 \pmod{3}$

$a=-3, b=20,$

$a-b=-33$

$11 \mid -33$

$\therefore -3 \equiv 20 \pmod{11}$

(g) $111 \equiv -9 \pmod{40}$

$a=111, b=-9, m=40$

$a-b=120$

$40 \mid 120$

$\therefore 111 \equiv -9 \pmod{40}$

(h) $666 \equiv 0 \pmod{37}$

$a=666, b=0, m=37$

$a-b=666$

$37 \mid 666$

$\therefore 666 \equiv 0 \pmod{37}$

2) For each of these pairs of integers, determine whether they are congruent modulo 7.

(a) 1, 15

$a=1, b=15, m=7$

$a-b=-14$

$7 \mid -14$

$\therefore 1 \equiv 15 \pmod{7}$

(b) 0, 42

$a=0, b=42, m=7$

$a-b=-42$

$7 \mid -42$

$\therefore 0 \equiv 42 \pmod{7}$

(c) 2, 99

$a=2, b=99, m=7$

$a-b=-97$

$7 \nmid -97$

$\therefore 2 \not\equiv 99 \pmod{7}$

(d) $-1, 8$

$a=-1, b=8, m=7$

$a-b=-9$

$7 \nmid -9$

$\therefore -1 \not\equiv 8 \pmod{7}$

(e) $-9, 5$

$a=-9, b=5, m=$

$a-b=-14$

$7 \mid -14$

$\therefore -9 \equiv 5 \pmod{7}$

(f) $-1, 699$

$a=-1, b=699, m=$

$a-b=-700$

$7 \mid -700$

$\therefore -1 \equiv 699 \pmod{}$

3) Find the least non-negative residue modulo 13 of each of the following integers.

Given, $m=13 \Rightarrow r = \{0, 1, 2, \ldots, 12\}$

(a) 22

$22 = 13(1) + 9$

$\therefore r = 9$

(b) 100

$100 = 13(7) + 9$

$\therefore r = 9$

(c) 1001

$1001 = 13(77) + 0$

$\therefore r = 0$

(d) -1

$-1 = 13(-1) + 12$

$\therefore r = 12$

(e) -100

$-100 = 13(-8) + 4$

$\therefore r = 4$

(f) -1000

$-1000 = 13(-77) + 1$

$\therefore r = 1$

4) Find the least non-negative residue modulo 28 of each of the following integers.

Given, $m = 28 \Rightarrow r = \{0, 1, \ldots, 27\}$

(a) 99

$99 = 28(3) + 15$

$\therefore r = 15$

(b) 1100

$1100 = 28(39) + 8$

$\therefore r = 8$

(c) 12,345

$12,345 = 28(440) + 25$

$\therefore r = 25$

(d) -1

$-1 = 28(-1) + 27$

$\therefore r = 27$

(e) -1000

$-1000 = 28(-36) + 8$

$\therefore r = 8$

(f) $-54,321$

$-54,321 = 28(-1941) + 27$

$\therefore r = 27$

20/12/21

5) Find all solutions of the linear congruence $9x \equiv 12 \pmod{15}$

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

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

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

$\therefore$ The given linear congruence has 3 solutions.

One of the 3 solutions can be found as follows:

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

$\Rightarrow 15 \mid (9x - 12)$

$\Rightarrow 9x - 12 = 15y$ for $y \in Z$

$\Rightarrow 9x - 15y = 12 \longrightarrow (1)$

Now we express $(9, 15) = 3$ as a linear combination of 9, 15.

$3 = 9 - 6 \times 1$

$= 9 - (15 - 9)$

$= 9 - 15 + 9$

$= 2(9) - 15(1)$

i.e., $3 = 2 \times 9 - 1 \times 15 \longrightarrow (2)$

$(2) \times 4 \Rightarrow 12 = 8 \times 9 - 4 \times 15$

comparing with (1),

$x = x_0 = 8$

$y = y_0 = 4$

$15 = 9 \times 1 + 6$

$9 = 6 \times 1 + 3$ ✓

$6 = 3 \times 2 + 0$

$9x - 15y = 12$

$= 3$

$b = 9(1) - 15(1)$

$b = 9(2) - 15(1)$

$x \equiv x_0 \pmod{m}$

i.e., $x \equiv 8 \pmod{15}$

Other solutions,

$x = x_0 + \frac{m}{d} \cdot t$ where $t = 0, 1, \ldots d-1$

$8 = x_0 + \frac{15}{3} t$ where $t = 0, 1, 2$

$\Rightarrow 8 = x_0 + 5t$

(i) $x_0 = 8$ (ii) $x_0 = 13$ (iii) $x_0 = 18$

∴ Solutions are, $x \equiv 8 \pmod{15}$

$x \equiv 13 \pmod{15}$

$x \equiv 18 \pmod{15}$ or $x \equiv 3 \pmod{15}$

($\because 3 = 18 - 15$)

Working rule to find solutions of linear congruence

Step1: Consider the given linear congruence $ax \equiv b \pmod{m}$

Step2: Find $d = (a, m)$

If $d \mid b$ then there are 'd' no.of solutions

else no solutions.

step3: Using From the given linear congruence, write

$b = ax - my$ for $y \in z$ ($\because m \mid ax - b$)

$\rightarrow$ (i)

step4: Using Euclidian algorithm express 'd' as a linear combination of a, m and then comparing with (1), obtain x & y. $b = ax_0 - my_0$

step5: ∴ The first solution is $x \equiv x_0 \pmod{m}$

step6: Remaining solutions are, $x = x_0 + \frac{m}{d} t$ for $t = 0, 1, \ldots (d$

1) Solve the linear congruence $31x \equiv 12 \pmod{24}$

$31x \equiv 12 \pmod{24}$;

Here, $a = 31$, $b = 12$, $m = 24$

$(a,m) = (31,24) = 1$ and $1 \mid 12$

∴ The linear congruence $31x \equiv 12 \pmod{24}$ has 1 solution.

Now, $(31,24) = 1$, $31x \equiv 12 \pmod{24}$

$\Rightarrow 24 \mid (31x - 12)$

$\Rightarrow 31x - 12 = 24y$

$\Rightarrow 31x - 24y = 12 \rightarrow (1)$

By EA,

$31 = 24(1) + 7$

$24 = 7(3) + 3$

$7 = 3(2) + 1$

$3 = 1(3) + 0$

Now, $1 = 7 - 3(2)$

$= 7 - (24 - 7 \times 3)$

$= 7 \times 4 - 24$

$= (31 - 24) \times 4 - 24$

$= 31(4) - 24(5) \Rightarrow 12 = 31(48) - 24(60)$

From (1), $x = x_0 = 48$

$y = y_0 = 60$

∴ solution is, $x \equiv 48 \pmod{24}$

11/A1 20/12/22

1) Find all solutions of each of the following linear congruences

(a) $2x \equiv 5 \pmod 7$

$a = 2, b = 5, m = 7$

$(a,m) = (2,7) = 1$ and $1 \mid 5$

∴ It has 1 solution.

$2x \equiv 5 \pmod 7$

$\Rightarrow 7 \mid (2x-5)$

$\Rightarrow 2x - 5 = 7y \quad \forall\, y \in Z$

$\Rightarrow 2x - 7y = 5 \rightarrow (1)$

Now, $(2,7) = 1$ in linear combination is

$1 = 7 - 2(3)$ $\qquad 7 = 2(3) + 1$

$\times 5 \Rightarrow 5 = 7 \times 5 - 2 \times 15$ $\qquad 2 = 1(2) + 0$

∴ From (1), $x = -15, y = -5$

∴ sol'n is, $x \equiv -15 \pmod 7$

(b) $19x \equiv 30 \pmod{40}$

$a = 19, b = 30, m = 40$

$(a,m) = (19,40) = 1$ and $1 \mid 30$

∴ It has 1 solution.

$19x \equiv 30 \pmod{40}$

$\Rightarrow 40 \mid (19x - 30)$

$\Rightarrow 19x - 30 = 40y$

$\Rightarrow 19x - 40y = 30 \rightarrow (1)$

Now, $(19,40) = 1$ in linear combination is,

$1 = 19 - 2 \times 9$

$= 19 - (40 - 19 \times 2) \times 9$

$= 19 \times 1 - 40 \times 9 + 19 \times 18$

$= 19 \times 19 - 40 \times 9$

$\times 30 \Rightarrow 30 = 19(570) - 40(270)$

$40 = 19(2) + 2$

$19 = 2(9) + 1$

$2 = 1(2) + 0$

$\therefore$ From ①, $x = x_0 = 570$, $y = y_0 = 270$

$\therefore$ $x \equiv 570 \pmod{40}$ is a solution.

(b) $3x \equiv 6 \pmod 9$

$a = 3, b = 6, m = 9$

$(a, m) = (3, 9) = 3$ and $3 \mid 6$

$\therefore$ It has 3 solutions.

$3x \equiv 6 \pmod 9$

$\Rightarrow 9 \mid (3x - 6)$

$\Rightarrow 3x - 6 = 9y$

$\Rightarrow 3x - 9y = 6 \longrightarrow (1)$

Now, $(3, 9) = 3$ in linear combination is,

$3 = 9 - 3(2) = 9 \times 1 - 3 \times 2$

$\times 2 \Rightarrow 6 = 9 \times 2 - 3 \times 4$

From ①, $x_0 = -4$, $y_0 = -2$

$\therefore$ $x \equiv -4 \pmod 9$ is a sol'n.

Other solutions are,

$x = x_0 + \frac{m}{d} \cdot t$ where $t = 0, 1, 2$ $\quad d = 3$

$\Rightarrow -4 = x_0 + \frac{9}{3} t$

$\Rightarrow -4 = x_0 + 3t$ where $t = 0, 1, 2$

(i) $t = 0$ $\Rightarrow x_0 = -4$

(ii) $t = 1$ $\Rightarrow x_0 = -4 - 3 = -7$

(iii) $t = 2$ $\Rightarrow x_0 = -10$

$\therefore$ sol'ns are,

$x \equiv -4 \pmod 9$

$x \equiv -7 \pmod 9$

$x \equiv -10 \pmod 9$

(d) $9x \equiv 5 \pmod{25}$

$a=9,\ b=5,\ m=25$

$(a,m) = (9,25) = 1$ and $1 \mid 5$

$\therefore$ It has 1 solution.

$9x \equiv 5 \pmod{25}$

$\Rightarrow 25 \mid (9x-5)$

$\Rightarrow 9x-5 = 25y \Rightarrow 9x-25y = 5 \longrightarrow (1)$

Now, $(9,25)=1$ in l.c is,

$1 = 25\times 4 - 9\times 11$

$\times 5 \Rightarrow 5 = 25(20) - 9(55)$

$25 = 9(2) + 7$

$9 = 7(1) + 2$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

From (1), $x_0 = -55,\ y_0 = -20$

$\therefore x \equiv -55 \pmod{25}$ is a sol'n.

(e) $103x \equiv 444 \pmod{999}$

$a=103,\ b=444,\ m=999$

$(a,m) = (103,999) = 1$ and $1 \mid 444$

$\therefore$ It has 1 sol'n.

$103x \equiv 444 \pmod{999}$

$\Rightarrow 999 \mid (103x-444)$

$\Rightarrow 103x - 444 = 999y \Rightarrow 103x - 999y = 444 \longrightarrow (1)$

Now, $(103,999)=1$ in l.c is

$1 = 103(97) - 999(10)$

$\times 444 \Rightarrow 444 = 103(43,068) - 999(4440)$

$\therefore$ From (1), $x_0 = 43,068,\ y_0 = 4440$

$\therefore x \equiv 43,068 \pmod{999}$ is a sol'n

(f) $980x \equiv 610 \pmod{1597}$

$a = 980, b = 610, m = 1597$

$(a, m) = (980, 1597) = 1$ and $1 \mid 610$

$\therefore$ It has 1 sol'n.

$980x \equiv 610 \pmod{1597}$

$\Rightarrow 1597 \mid (980x - 610)$

$\Rightarrow 980x - 610 = 1597y \Rightarrow 980x - 1597y = 610 \rightarrow (1)$

Now, $(980, 1597) = 1$ in l.c is,

$1 = 980(44) - 1597(27)$

$\times 610 \Rightarrow 610 = 980(26,840) - 1597(16470)$

From (1), $x_0 = 26840$, $y_0 = 16470$

$\therefore x \equiv 26840 \pmod{1597}$ is a sol'n

2) Find all solutions of each of the following linear congruences.

(a) $3x \equiv 2 \pmod{7}$

$a = 3, b = 2, m = 7$

$(a, m) = (3, 7) = 1$ and $1 \mid 2$

$\therefore$ It has 1 sol'n

$3x \equiv 2 \pmod{7}$

$\Rightarrow 7 \mid (3x - 2)$

$\Rightarrow 3x - 2 = 7y \Rightarrow 3x - 7y = 2 \rightarrow (1)$

Now, $(3, 7) = 1$ in l.c is,

$1 = 3(5) - 7(2)$

$\times 2 \Rightarrow 2 = 3(10) - 7(4)$

From (1), $x_0 = 10$, $y_0 = 4$

$\therefore x \equiv 10 \pmod{7}$ is a sol'n

(or) $x \equiv 3 \pmod{7}$

(b) $6x \equiv 3 \pmod 9$

$a=6, b=3, m=9$

$(a,m) = (6,9) = 3$ and $3|3$

$\therefore$ It has 3 sol'ns.

$6x \equiv 3 \pmod 9$

$\Rightarrow 9 | (6x-3)$

$\Rightarrow 6x-3 = 9y \Rightarrow 6x-9y = 3 \rightarrow (1)$

Now, $(6,9)=3$ in l.c is,

$3 = 6(5) - 9(3)$

From (1), $x_0 = 5$, $y_0 = 3$

$\therefore x \equiv 5 \pmod 9$ is a sol'n

Other sol'ns are,

$x = x_0 + \frac{m}{d}t \qquad d=3, \; t=0,1,2$

$\Rightarrow 5 = x_0 + \frac{9}{3}t$

$\Rightarrow 5 \equiv x_0 + 3t \quad (t=0,1,2)$

(i) $x_0 = 5$ (ii) $x_0 = 2$ (iii) $x_0 = -1$

$\therefore$ sol'ns are,

$x \equiv 5 \pmod 9$

$x \equiv 2 \pmod 9$

$x \equiv -1 \pmod 9$

(c) $17x \equiv 14 \pmod{21}$

$a=17, b=14, m=21$

$(a,m) = (17,21) = 1$ and $1|14$

$\therefore$ It has 1 sol'n

$17x \equiv 14 \pmod{21}$

$\Rightarrow 21 | (17x-14)$

$\Rightarrow 21y = 17x - 14$

$\Rightarrow 17x - 21y = 4 \rightarrow (1)$

Now, $(17,21)=1$ in l.c is,

$$1 = 17 - 4\times 4$$
$$= 17 - (21\times 1 - 17\times 1)\times 4$$
$$= 17\times 5 - 21\times 4$$

$$21 = 17(1) + 4$$
$$17 = 4(4) + 1$$
$$4 = 1(4) + 0$$

$\times 4 \Rightarrow 4 = 17(20) - 21(16)$

From ①, $x_0 = 20$, $y_0 = 16$

$\therefore x \equiv 20 \pmod{21}$ is a soln

(d) $15x \equiv 9 \pmod{25}$

$a = 15$, $b = 9$, $m = 25$

$(a,m) = (15,25) = 5$ but $5 \nmid 9$

∴ It has no solution.

(e) $128x \equiv 833 \pmod{1001}$

$a = 128$, $b = 833$, $m = 1001$

$(a,m) = (128,1001) = 1$ and $1 \mid 833$

∴ It has 1 soln.

$128x \equiv 833 \pmod{1001}$

$\Rightarrow 1001 \mid (128x - 833)$

$\Rightarrow 128x - 833 = 1001y \Rightarrow 128x - 1001y = 833 \rightarrow (1)$

Now, $(128,1001) = 1$ in l.c is,

$$1 = 128(305) - 1001(39)$$

$$1001 = 128(7) + 105$$
$$128 = 105(1) + 23$$
$$105 = 23(4) + 13$$
$$23 = 13(1) + 10$$
$$13 = 10(1) + 3$$
$$10 = 3(3) + 1$$
$$3 = 1(3) + 0$$

$\times 833 \Rightarrow 833 = 128(2,54,065) - 1001(32,487)$

From ①, $x_0 = 2,54,065$, $y_0 = 32,487$

$\therefore x \equiv 2,54,065 \pmod{1001}$ is soln

(4) $987x \equiv 610 \pmod{1597}$

$a=987,\ b=610,\ m=1597$

$(a,m) = (987,1597) = 1$ and $1 \mid 610$

$\therefore$ It has 1 sol'n.

$987x \equiv 610 \pmod{1597}$

$\Rightarrow 1597 \mid (987x - 610)$

$\Rightarrow 987x - 610 = 1597y \Rightarrow 987x - 1597y = 610 \longrightarrow (1)$

Now, $(987,1597)=1$ in l.c is,

$1 = 987(610) - (1597)(377)$

From (1), $x_0 = 372100$

$\therefore x \equiv 372100 \pmod{1597}$

$\rightarrow x \equiv 1596 \pmod{1597}$ is sol'n

$1597 = 987(1) + 610$

$987 = 610(1) + 377$

$610 = 377(1) + 233$

$377 = 233(1) + 144$

$233 = 144(1) + 89$

$144 = 89(1) + 55$

$89 = 55(1) + 34$

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

22/12/22

Inverse of 'a' modulo 'm' :-

If $a \in z$, $m \in z^+$ and $(a,m) = 1$ then an integer solution 'x' of the linear congruence, $ax \equiv 1 \pmod{m}$ is called an inverse of 'a' modulo 'm'.

Ex:- $a=3$ & $m=4$

'Inverse' of '3' modulo '4' (here $(3,4)=1$) is the sol'n of $3x \equiv 1 \pmod{4}$

here, $x=3$ is a sol'n

i.e., $x \equiv 3 \pmod{4}$ $\{\ldots -5, -1, 3, 7, 11, \ldots\}$

$\therefore$ '3' is inverse of '3' modulo '4' or

$x \equiv 3 \pmod{4}$ is the inverse of '3' modulo '4'.

Ex: What is the inverse of '7' modulo '31'

$a=7, m=31, (7,31)=1$

$\therefore 7x \equiv 1 \pmod{31}$

here, $x=9$ is a sol'n.

$x \equiv 9 \pmod{31}$ is $\{\ldots -22, 9, 40, 71, \ldots\}$

the inverse of '7' modulo '31'.

Statement: Let p be a prime, then a positive integer 'a' is its own inverse modulo 'p' iff

$a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Ex:- $a=4$, $p=3$ and $(a,p) = (4,3) = 1$

inverse of '4' = sol'n of $4x \equiv 1 \pmod{3}$

4 is the sol'n of $4x \equiv 1 \pmod{3} \Rightarrow 4 \equiv 1 \pmod{3}$ ✓

or

i.e; '4' is the inverse of '4' mod '3' $4 \equiv -1 \pmod{3}$

Chinese Remainder Theorem:

Let $m_1, m_2, \ldots m_r$ be pairwise relatively prime positive integers. Then the congruences

$x_1 \equiv a_1 \pmod{m_1}$, $x_2 \equiv a_2 \pmod{m_2}, \ldots x_r \equiv a_r \pmod{m_r}$

has unique solution, modulo $M = (m_1 \cdot m_2 \ldots m_r)$.

Working rule

Solve three LC; $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$,

$x \equiv a_3 \pmod{m_3}$

step1: check $(m_1, m_2) = 1$, $(m_2, m_3) = 1$, $(m_3, m_1) = 1$

(pairwise relatively prime else CRT can't apply)

step2: Find $M = m_1 \cdot m_2 \cdot m_3$

step3: Find $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

Step4: Find inverse y_1 of M_1 modulo m_1

(i.e; sol'n of $M_1x \equiv 1 \pmod{m_1}$)

i.e; $M_1y_1 \equiv 1 \pmod{m_1}$

Find inverse y_2 of 'M_2' modulo 'm_2'

i.e; sol'n of $M_2x \equiv 1 \pmod{m_2}$

Find inverse y_3 of 'M_3' modulo 'm_3'

i.e; sol'n of $M_3x \equiv 1 \pmod{m_3}$

Step5: Find the value $\sum_{i=1}^{3} a_iM_iy_i$

Now, $\boxed{x \equiv \left(\sum_{i=1}^{3} a_iM_iy_i\right) \pmod{M}}$ is the unique sol'n of three linear congruences.

23/11/17

1) Solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

Given, $a_1 = 1, a_2 = 2, a_3 = 3$

$m_1 = 3, m_2 = 5, m_3 = 7$

clearly, $(3,5) = 1, (5,7) = 1, (7,3) = 1$

$\therefore$ They are pair-wise relatively prime.

Now, we can apply CRT

Now, $M = m_1 \cdot m_2 \cdot m_3$

$= (3)(5)(7)$

$= 105$

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

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

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

Let, 'y_1' be the inverse of 'M_1' modulo 'm_1'

$M_1y_1 \equiv 1 \pmod{m_1}$

$\Rightarrow 35y_1 \equiv 1 \pmod 3 \Rightarrow y_1 = 2$ is sol'n (inverse is)

Similarly, $21y_2 \equiv 1 \pmod 5 \Rightarrow y_2 = 1$ is sol'n

$15y_3 \equiv 1 \pmod 7 \Rightarrow y_3 = 1$ is sol'n

Now, $\sum_{i=1}^{3} a_i M_i y_i = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$= (1)(35)(2) + (2)(21)(1) + (3)(15)(1)$

$= 70 + 42 + 45$

$= 157$

$\therefore x \equiv 157 \pmod{105}$ is the sol'n of three linear congruences.

i.e., $x \equiv 52 \pmod{105}$

2) Solve $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 7$

Given, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$

$m_1 = 4$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$

Clearly, $(4,3) = 1$, $(3,5) = 1$, $(5,7) = 1$, $(7,4) = 1$

$\therefore m_1, m_2, m_3$ & m_4 are pair-wise relatively prime.

Now we can apply CRT

Now, $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4$

$= 4 \times 3 \times 5 \times 7$

$= 420$

$M_1 = \frac{M}{m_1} = \frac{420}{4} = 105$

$M_2 = \frac{M}{m_2} = \frac{420}{3} = 140$

$M_3 = \frac{M}{m_3} = \frac{420}{5} = 84$

$M_4 = \frac{M}{m_4} = \frac{420}{7} = 60$

Let, 'y_1' be the inverse of 'M_1' modulo 'm_1'

(i) $105x \equiv 1 \pmod 4$

$\Rightarrow x = 1$ is a sol'n

$\therefore$ inverse, $y_1 = 1$

Now, (ii) $140x \equiv 1 \pmod 3$

$\Rightarrow x = 2$ is a sol'n

$\therefore$ inverse, $y_2 = 2$

(iii) $84x \equiv 1 \pmod 5$

$\Rightarrow x = 4$ is a sol'n

$\therefore$ inverse, $y_3 = 4$

(iv) $60x \equiv 1 \pmod 7$

$\Rightarrow x = 2$ is a sol'n

$\therefore$ inverse, $y_4 = 2$

Now, $\sum_{i=1}^{4} a_i M_i y_i = (1)(105)(1) + (2)(140)(2) + (3)(84)(4) + (5)(6$

$= 105 + 560 + 1008 + 600$

$= 2273$

sol'n is, $x \equiv 2273 \pmod{420}$

$\therefore x \equiv 173 \pmod{420}$

Method - 2 when any of $m_1, m_2, m_3 \cdots$ are not pairwise relatively prime

step - 1

Consider the system of linear congruences,

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$

This system has a solution iff $(m_1, m_2) \mid a_1 - a_2$

If there is a solution, it is unique modulo, mod $[m_1, m_2]$ (lcm)

Statement - 2 :-

Consider the system of l.c,

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $x_3 \equiv a_3 \pmod{m_3}$

This system has a sol'n iff $(m_i, m_j) \mid a_i - a_j \ \forall (i, j)$

If there is a sol'n, it is unique mod $[m_1, m_2, m_3]$

$x \equiv a \pmod m \Rightarrow x = mk + a$,

$ax \equiv b \pmod m \Rightarrow$ 1 sol'n is, $x \equiv x_0 \pmod m$

other sol'ns are,

$x = x_0 + \frac{m}{d} t$

where, $d = (a, m)$

$t = 0, 1, \ldots, d-1$

1) solve $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$

(i) Here, $a_1 = 5$, $a_2 = 3$

$m_1 = 6$, $m_2 = 10$

$(m_1, m_2) = (6, 10) = 2$

$a_1 - a_2 = 5 - 3 = 2$

$(m_1, m_2) \mid a_1 - a_2$ ∴ the system has sol'n

(ii) consider, $x \equiv 5 \pmod 6$

$\Rightarrow x = 6t + 5$ for $t \in Z$

$\rightarrow$ (1)

sub 'x' in 2nd eq'n.

$6t + 5 \equiv 3 \pmod{10}$

$\rightarrow 6t \equiv -2 \pmod{10}$

$t \equiv 3 \pmod{10}$ is the sol'n.

other sol'ns are, $t = x_0 + \frac{m}{d} \cdot u$, $u = 0, 1, \ldots d-1$

$\rightarrow t = 3 + \frac{10}{2} \cdot u$, $u = 0, 1$

∴ $t = 3$, $t = 8$ $\rightarrow t = 3 + 5u$

sub in (1),

$x = 6(3 + 5u) + 5$

$\rightarrow x = 23 + 30u$

$\Rightarrow x \equiv 23 \pmod{30}$ is the sol'n

24/12/22 11/W

4) Find all the solutions of each of the following systems of linear congruences.

(a) $x \equiv 4 \pmod{11}$

$x \equiv 3 \pmod{17}$

Given, $a_1 = 4$, $a_2 = 3$

$m_1 = 11$, $m_2 = 17$

$(m_1, m_2) = (11, 17) = 1$ ∴ m_1, m_2 are relatively prime

$M = m_1 \cdot m_2 = 11 \times 17 = 187$

$M_1 = \frac{M}{m_1} = 17$

$M_2 = \frac{M}{m_2} = 11$

Let 'y1' be the inverse of 'M1' modulo 'm1'

$$17x \equiv 1 \pmod{11}$$

$x = 2$ is a sol'n

$\therefore y_1 = 2$

Let 'y2' be the inverse of 'M2' modulo 'm2'

$$11x \equiv 1 \pmod{17}$$

$x = 14$ is a sol'n

$\therefore y_2 = 14$

Now, $\sum_{i=1}^{2} a_i M_i y_i = a_1 M_1 y_1 + a_2 M_2 y_2$

$= (4)(17)(2) + (3)(11)(14)$

$= 136 + 462$

$= 598$

$\therefore$ sol'n is, $x \equiv 598 \pmod{187}$

$\Rightarrow x \equiv 37 \pmod{187}$

(b) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$

Given, $a_1 = 1, a_2 = 2, a_3 = 3$

$m_1 = 2, m_2 = 3, m_3 = 5$

$(2,3) = (3,5) = (2,5) = 1$ $\therefore m_1, m_2, m_3$ relatively prime

$M = m_1 \cdot m_2 \cdot m_3 = 30$

$M_1 = \frac{M}{m_1} = 15$

$M_2 = \frac{M}{m_2} = 10$

$M_3 = \frac{M}{m_3} = 6$

Let 'y1' be the inverse of 'M1' modulo 'm1'

$$15x \equiv 1 \pmod 2$$

$x = 1$ is a sol'n

$\therefore y_1 = 1$

Now, $10x \equiv 1 \pmod 3$

$x = 1$ is sol'n

$\therefore y_2 = 1$

$6x \equiv 1 \pmod 5$

$x = 1$ is a sol'n

$\therefore y_3 = 1$

Now,

$$\sum_{i=1}^{3} a_i M_i y_i = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$

$$= (1)(15)(1) + (2)(10)(1) + (3)(6 \times 1)$$

$$= 15 + 20 + 18$$

$$= 53$$

$\therefore x \equiv 53 \pmod{30}$

$\rightarrow x \equiv 23 \pmod{30}$ is the sol'n

(a) $x \equiv 4 \pmod 6$

$x \equiv 13 \pmod{15}$

Given, $a_1 = 4$, $a_2 = 13$

$m_1 = 6$, $m_2 = 15$

$(6, 15) = 3$ i.e., m_1, m_2 are not relatively prime

$(m_1, m_2) \mid a_1 - a_2$

$\therefore$ The system has sol'n

consider, $x \equiv 4 \pmod 6$

$\Rightarrow x = 6t + 4 \quad \forall\, t \in Z$ $\rightarrow (1)$

sub 'x' in 2nd eq'n

$\Rightarrow 6t + 4 \equiv 13 \pmod{15}$

$\Rightarrow 6t \equiv 11 \pmod{15}$

$\therefore t \equiv 1 \pmod{15}$ is the sol'n.

Other sol'ns are,

$t = x_0 + \frac{m}{d} \cdot u$

$\Rightarrow t = 1 + \frac{15}{3} \cdot u$ where $u = 0, 1, 2$

$\Rightarrow t = 1 + 5u$

sub in (1)

$\Rightarrow x = 6(1 + 5u) + 4$

$\Rightarrow x = 5u + 10$

$\therefore x \equiv 10 \pmod 5$ is the sol'n

2-1-12-22.

1) Solve $x \equiv 4 \pmod 6$, $x \equiv 2 \pmod 8$, $x \equiv 1 \pmod 9$

Given, $a_1 = 4$, $a_2 = 2$, $a_3 = 1$

$m_1 = 6$, $m_2 = 8$, $m_3 = 9$

$(6,8) = 2$ & $2 \mid 4-2$

$(8,9) = 1$ & $1 \mid 2-1$

$(9,6) = 3$ & $3 \mid 4-1$

∴ The system has sol'n.

(i) Consider, $x \equiv 4 \pmod 6$

$\Rightarrow x = 6t + 4 \quad \forall\, t \in Z \longrightarrow (1)$

(ii) sub (1) in 2nd eq'n $x \equiv 2 \pmod 8$

$\Rightarrow 6t + 4 \equiv 2 \pmod 8$

$\Rightarrow 6t \equiv -2 \pmod 8$

$t = 1$ is a sol'n

* $\Rightarrow 3t \equiv -1 \pmod 4$ (÷ by 2)

$t = 1$ is a sol'n

i.e; $t \equiv 1 \pmod 4$

$\Rightarrow t = 4u + 1$

sub 't' in (1)

$\Rightarrow x = 6(4u+1) + 4$

$\Rightarrow x = 24u + 10 \longrightarrow (2)$

(iii) sub (2) in 3rd eq'n $x \equiv 1 \pmod 9$

$\Rightarrow 24u + 10 \equiv 1 \pmod 9$

$\Rightarrow 24u \equiv -9 \pmod 9$

* $\Rightarrow 8u \equiv -3 \pmod 3$ (∵ ÷ by 3)

$u = 0$ is a sol'n

i.e; $u \equiv 0 \pmod 3$ is the sol'n.

$\Rightarrow u = 3v + 0 \longrightarrow (3)$

sub (3) in (2)

$\Rightarrow x = 24(3v) + 10$

$\Rightarrow x = 72v + 10$

$\therefore x \equiv 10 \pmod{72}$ is the soln.

2) $x \equiv 0 \pmod 4$, $x \equiv 5 \pmod 9$, $x \equiv 8 \pmod{12}$

Given, $a_1 = 0$, $a_2 = 5$, $a_3 = 8$

$m_1 = 4$, $m_2 = 9$, $m_3 = 12$

$(4,9) = 1$ & $1 \mid 0-5$

$(9,12) = 3$ & $3 \mid 5-8$

$(12,4) = 4$ & $4 \mid 0-8$

$\therefore$ The system has soln.

consider, $x \equiv 0 \pmod 4$

$\Rightarrow x = 4t \quad \forall\ t \in Z$

$\longrightarrow (1)$

sub (1) in 2nd eqn

$4t \equiv 5 \pmod 9$

$t = 8$ is a soln

i.e., $t \equiv 8 \pmod 9$

$\Rightarrow t = 9u + 8$

sub 't' in (1)

$x = 4(9u+8)$

$\Rightarrow x = 36u + 32 \longrightarrow (2)$

sub (2) in 3rd eqn

$\rightarrow 36u + 32 \equiv 8 \pmod{12}$

$\rightarrow 36u \equiv -24 \pmod{12}$

$\Rightarrow 3u \equiv -2 \pmod 1$

$u = 0$ is a soln

$\Rightarrow u \equiv 0 \pmod 1$ is the soln.

$\Rightarrow u = v \longrightarrow (3)$

sub (3) in (2)

$x = 36v + 32$

$\Rightarrow x \equiv 32 \pmod{36}$ is the sol'n

System of linear congruences in 2 variables

Consider the 2 linear congruences in the variables x, y

$ax + by \equiv e \pmod{m}$

$cx + dy \equiv f \pmod{m}$

1) Solve $3x + 4y \equiv 5 \pmod{13}$ $\longrightarrow (1)$, $2x + 5y \equiv 7 \pmod{13}$ $\longrightarrow (2)$

(1)$\times 5$ - (2)$\times 4$

$15x + 20y \equiv 25 \pmod{13}$

$-\ 8x + 20y \equiv 28 \pmod{13}$

$7x \equiv -3 \pmod{13}$

[$\because a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$]

whose sol'n is, $\boxed{x \equiv 7 \pmod{13}}$ (by trial & error)

sub $x = 7$ in (1),

$3(7) + 4y \equiv 5 \pmod{13}$

$\Rightarrow 4y \equiv -16 \pmod{13}$

whose sol'n is, $\boxed{y \equiv 9 \pmod{13}}$

Method - 2

$ax + by \equiv e \pmod{m}$

$cx + dy \equiv f \pmod{m}$

sol'n is,

$x \equiv \bar{\Delta}(de - bf) \pmod{m}$

$y \equiv \bar{\Delta}(af - ce) \pmod{m}$

if $\bar{\Delta}$ is inverse of $\Delta \bmod m$ where, $\Delta = ad - bc$