

19/12/22

Linear congruence :

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

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

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

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

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

$$x=2, x=4, x=6, \text{etc}$$

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

2.

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

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

sol'n's are,  $\{-10, -4, 2, 8, 14, 20, \dots\}$  i.e;  $x \equiv 2 \pmod{6}$

$$\{ -7, -1, 5, 11, 17, \dots \} \text{ i.e; } x \equiv 5 \pmod{6}$$

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

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

sol'n's are,  $\{-16, -7, 2, 11, 20, \dots\}$  i.e;  $x \equiv 2 \pmod{9}$

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

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

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

$x \in$  This congruence has no solution.

Statement I: If  $a, b \in \mathbb{Z}$  &  $m \in \mathbb{Z}^+$  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  $\frac{d}{\text{exactly}}$   $\rightarrow$  (distinct) incongruent sol'n's

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

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

$$\underline{\text{Ex:}} \quad 4x \equiv 8 \pmod{6}$$

$$a=4, b=8, m=6 \quad (\text{L.H.S.}) \neq (\text{R.H.S.})$$

$$(a, m) = (4, 6) = 2 = d, \text{ as } 2 \mid 8 \text{ i.e., } d \mid b$$

$\therefore$  system has 2 solutions.

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

$$\text{i.e., } x \equiv 2 \pmod{6}$$

$$\text{Now, } x_0 = 2$$

the other sol'n is,

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

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

$$\in \text{L.H.S.} \quad \in \text{R.H.S.} \quad \in \text{L.H.S.}$$

$$= 5$$

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

$$2. \quad 6x \equiv 18 \pmod{9}$$

$$x=0, \text{ is a sol'n}$$

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

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

$$\text{i.e., } x \equiv 0 \pmod{9}$$

$$\text{and } 8t+0 \text{ as } 3 \mid 18$$

system has 3 solns.

Other solns are,

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

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

$$x=3, x=6$$

$$\therefore x \equiv 3 \pmod{9}, \Rightarrow x \equiv 6 \pmod{9}$$

H/W  
19/12/22

1) Show that each of the following congruences holds.

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

$$a=13, b=1, m=2 \quad (\text{L.H.S.}) \neq (\text{R.H.S.})$$

$$a-b=12$$

$$2 \mid 12$$

$$\therefore 13 \equiv 1 \pmod{2}$$

$$(b) 69 \equiv 62 \pmod{7}$$

$$a=69, b=62, m=7 \quad (\text{L.H.S.}) \neq (\text{R.H.S.})$$

$$a-b=7$$

$$7 \mid 7$$

$$\therefore 69 \equiv 62 \pmod{7}$$

$$(c) 22 \equiv 7 \pmod{5}$$

$$a=22, b=7, m=5 \quad (\text{L.H.S.}) \neq (\text{R.H.S.})$$

$$a-b=15$$

$$5 \mid 15$$

$$\therefore 22 \equiv 7 \pmod{5}$$

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

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

$$a-b=91$$

$$13|91$$

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

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

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

$$a-b=120$$

$$40|120$$

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

$$(e) -2 \equiv 11$$

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

$$a-b=-3$$

$$3|-3$$

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

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

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

$$m|a-b=666$$

$$37|666$$

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

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

$$(a) 1, 15$$

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

$$a-b=-14$$

$$7|-14$$

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

$$(k) 2, 99$$

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

$$a-b=-97$$

$$7|-97$$

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

$$(e) -9, 5$$

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

$$a-b=-14$$

$$7|-14$$

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

$$(b) 0, 42$$

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

$$a-b=-42$$

$$7|-42$$

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

$$(d) -1, 8$$

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

$$a-b=-9$$

$$7|-9$$

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

$$(f) -1, 699$$

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

$$a-b=-700$$

$$7|-700$$

$$\therefore -1 \equiv 699 \pmod{7}$$

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

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

$$(a) 22 \quad (b) 100 \quad (c) 1001 \quad (d) -1$$

$$22 = 13(1) + 9$$

$$100 = 13(7) + 9$$

$$1001 = 13(77) + 0$$

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

$$\therefore r=9$$

$$\therefore r=9$$

$$\therefore r=0$$

$$\therefore r=12$$

$$(e) -100$$

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

$$\therefore r=4$$

$$(f) -1000$$

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

$$\therefore r=1$$

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

Given,  $m=28 \Rightarrow \tau = \{0, 1, \dots, 27\}$

(a) 99

$$99 = 28(3) + 15$$

$$\therefore \tau = \underline{\underline{15}}$$

(b) 1100

$$1100 = 28(39) + 8$$

$$\therefore \tau = \underline{\underline{8}}$$

(c) 12,345

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

$$\therefore \tau = \underline{\underline{25}}$$

(d) -1

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

$$\therefore \tau = \underline{\underline{27}}$$

(e) -1000

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

$$\therefore \tau = \underline{\underline{8}}$$

(f) -54,321

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

$$\therefore \tau = \underline{\underline{27}}$$

20/2/22

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

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

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

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

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

One of the 3 solutions can be found as follows:

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

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

$$\Rightarrow 9x-12 = 15y \text{ for } y \in \mathbb{Z}$$

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

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

of 9, 15.

$$3 = 9-6 \times 1$$

$$= 9-(15-9)$$

$$= 9-15+9$$

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

$$(1) \times 4 \Rightarrow 12 = 8 \times 9 - 4 \times 15$$

$$\text{Comparing with (1),}$$

$$x = x_0 = 8$$

$$y = y_0 = 4$$

$$b = a^{-1} - m \tau$$

$$b = 9^{-1} - 15[1]$$

$$x \equiv x_0 \pmod{m}$$

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

Other solutions,

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

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

$$\Rightarrow 8 = x_0 + 5t$$

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

Solutions are,  $x \equiv 8 \pmod{15}$  or  $x \equiv 13 \pmod{15}$  or  $x \equiv 18 \pmod{15}$

$$x \equiv 13 \pmod{15}$$

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

Working rule to find solutions of linear congruence

Step 1: Consider the given linear congruence  $ax \equiv b \pmod{m}$

Step 2: Find  $d = (a, m)$

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

Step 3: Using From the given linear congruence, write

$$b = ax - my \text{ for } y \in \mathbb{Z} \quad (\because m \mid ax - b)$$

Step 4: Using Euclidian algorithm express 'd' as a linear combination of  $a, m$  and then comparing with ①, obtains  $x \& y$ .  $b = ax_0 - my_0$

Step 5:  $\therefore$  The first solution is  $x \equiv x_0 \pmod{m}$

Step 6: Remaining solutions are,  $x = x_0 + \frac{m}{d}t$  for  $t = 0, 1, \dots, (d-1)$

$(d, m) = d$

$$P = R = P'$$

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

$31x \equiv 12 \pmod{24}$  (modular arithmetic to reduce the congruence)

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

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

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

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

$$\Rightarrow 24 \mid (31x - 12) \quad (\text{cancel } 12)$$

$$\Rightarrow 31x - 12 = 24y \quad (24 \mid x)$$

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

By EA,

$$31 = 24(1) + 7$$

$$24 = 7(3) + 3$$

$$7(3) = 7 = 3(2) + 1$$

$$3(2) = 6 = 2(3) + 0$$

$$\text{Now, } 1 = 7 - 3(2) = 7 - 2(3) - 2(2) = 7 - 2(24 - 7) = 7 - 2(24) + 2(7) = 7 - 2(24) + 2(3(2)) = 7 - 2(24) + 6(2) = 7 - 2(24) + 6(3(2)) = 7 - 2(24) + 18(2) = 7 - 2(24) + 18(3(2)) = 7 - 2(24) + 54(2) = 7 - 2(24) + 54(3(2)) = 7 - 2(24) + 162(2) = 7 - 2(24) + 162(3(2)) = 7 - 2(24) + 486(2) = 7 - 2(24) + 486(3(2)) = 7 - 2(24) + 1458(2) = 7 - 2(24) + 1458(3(2)) = 7 - 2(24) + 4374(2) = 7 - 2(24) + 4374(3(2)) = 7 - 2(24) + 13122(2) = 7 - 2(24) + 13122(3(2)) = 7 - 2(24) + 39366(2) = 7 - 2(24) + 39366(3(2)) = 7 - 2(24) + 118098(2) = 7 - 2(24) + 118098(3(2)) = 7 - 2(24) + 354294(2) = 7 - 2(24) + 354294(3(2)) = 7 - 2(24) + 1062882(2) = 7 - 2(24) + 1062882(3(2)) = 7 - 2(24) + 3188646(2) = 7 - 2(24) + 3188646(3(2)) = 7 - 2(24) + 9565938(2) = 7 - 2(24) + 9565938(3(2)) = 7 - 2(24) + 28697814(2) = 7 - 2(24) + 28697814(3(2)) = 7 - 2(24) + 86093442(2) = 7 - 2(24) + 86093442(3(2)) = 7 - 2(24) + 258280326(2) = 7 - 2(24) + 258280326(3(2)) = 7 - 2(24) + 774840978(2) = 7 - 2(24) + 774840978(3(2)) = 7 - 2(24) + 2324522934(2) = 7 - 2(24) + 2324522934(3(2)) = 7 - 2(24) + 6973568802(2) = 7 - 2(24) + 6973568802(3(2)) = 7 - 2(24) + 20920706406(2) = 7 - 2(24) + 20920706406(3(2)) = 7 - 2(24) + 62762119218(2) = 7 - 2(24) + 62762119218(3(2)) = 7 - 2(24) + 188286357654(2) = 7 - 2(24) + 188286357654(3(2)) = 7 - 2(24) + 564859072962(2) = 7 - 2(24) + 564859072962(3(2)) = 7 - 2(24) + 1694577218886(2) = 7 - 2(24) + 1694577218886(3(2)) = 7 - 2(24) + 5083731656658(2) = 7 - 2(24) + 5083731656658(3(2)) = 7 - 2(24) + 15251194970074(2) = 7 - 2(24) + 15251194970074(3(2)) = 7 - 2(24) + 45753584910222(2) = 7 - 2(24) + 45753584910222(3(2)) = 7 - 2(24) + 137260754730666(2) = 7 - 2(24) + 137260754730666(3(2)) = 7 - 2(24) + 411782264191998(2) = 7 - 2(24) + 411782264191998(3(2)) = 7 - 2(24) + 1235346792575994(2) = 7 - 2(24) + 1235346792575994(3(2)) = 7 - 2(24) + 3706039377731982(2) = 7 - 2(24) + 3706039377731982(3(2)) = 7 - 2(24) + 11118118133205946(2) = 7 - 2(24) + 11118118133205946(3(2)) = 7 - 2(24) + 33354354399617838(2) = 7 - 2(24) + 33354354399617838(3(2)) = 7 - 2(24) + 100063063198853514(2) = 7 - 2(24) + 100063063198853514(3(2)) = 7 - 2(24) + 300189190596560542(2) = 7 - 2(24) + 300189190596560542(3(2)) = 7 - 2(24) + 900567571789181626(2) = 7 - 2(24) + 900567571789181626(3(2)) = 7 - 2(24) + 2701702715367545878(2) = 7 - 2(24) + 2701702715367545878(3(2)) = 7 - 2(24) + 8105108146102637634(2) = 7 - 2(24) + 8105108146102637634(3(2)) = 7 - 2(24) + 24315324438307912902(2) = 7 - 2(24) + 24315324438307912902(3(2)) = 7 - 2(24) + 72946073314923738706(2) = 7 - 2(24) + 72946073314923738706(3(2)) = 7 - 2(24) + 218838220944771216118(2) = 7 - 2(24) + 218838220944771216118(3(2)) = 7 - 2(24) + 656514662834313648354(2) = 7 - 2(24) + 656514662834313648354(3(2)) = 7 - 2(24) + 1969543988502940945062(2) = 7 - 2(24) + 1969543988502940945062(3(2)) = 7 - 2(24) + 5908631965508822835186(2) = 7 - 2(24) + 5908631965508822835186(3(2)) = 7 - 2(24) + 17725895916526468505558(2) = 7 - 2(24) + 17725895916526468505558(3(2)) = 7 - 2(24) + 53177687749579385516674(2) = 7 - 2(24) + 53177687749579385516674(3(2)) = 7 - 2(24) + 169533063248738156549992(2) = 7 - 2(24) + 169533063248738156549992(3(2)) = 7 - 2(24) + 508599190746214469649976(2) = 7 - 2(24) + 508599190746214469649976(3(2)) = 7 - 2(24) + 1525797572238643388949928(2) = 7 - 2(24) + 1525797572238643388949928(3(2)) = 7 - 2(24) + 4577392716715930166849884(2) = 7 - 2(24) + 4577392716715930166849884(3(2)) = 7 - 2(24) + 13722378150147790500549652(2) = 7 - 2(24) + 13722378150147790500549652(3(2)) = 7 - 2(24) + 41167134450443371501648956(2) = 7 - 2(24) + 41167134450443371501648956(3(2)) = 7 - 2(24) + 12350140335132991450594668(2) = 7 - 2(24) + 12350140335132991450594668(3(2)) = 7 - 2(24) + 37017000000000000000000000(2) = 7 - 2(24) + 37017000000000000000000000(3(2)) = 7 - 2(24) + 111181000000000000000000000(2) = 7 - 2(24) + 111181000000000000000000000(3(2)) = 7 - 2(24) + 333543000000000000000000000(2) = 7 - 2(24) + 333543000000000000000000000(3(2)) = 7 - 2(24) + 1000630000000000000000000000(2) = 7 - 2(24) + 1000630000000000000000000000(3(2)) = 7 - 2(24) + 3001890000000000000000000000(2) = 7 - 2(24) + 3001890000000000000000000000(3(2)) = 7 - 2(24) + 9005670000000000000000000000(2) = 7 - 2(24) + 9005670000000000000000000000(3(2)) = 7 - 2(24) + 27017020000000000000000000000(2) = 7 - 2(24) + 27017020000000000000000000000(3(2)) = 7 - 2(24) + 81051080000000000000000000000(2) = 7 - 2(24) + 81051080000000000000000000000(3(2)) = 7 - 2(24) + 243153240000000000000000000000(2) = 7 - 2(24) + 243153240000000000000000000000(3(2)) = 7 - 2(24) + 729460730000000000000000000000(2) = 7 - 2(24) + 729460730000000000000000000000(3(2)) = 7 - 2(24) + 2188382200000000000000000000000(2) = 7 - 2(24) + 2188382200000000000000000000000(3(2)) = 7 - 2(24) + 6565146620000000000000000000000(2) = 7 - 2(24) + 6565146620000000000000000000000(3(2)) = 7 - 2(24) + 19695439885029409450620000000000(2) = 7 - 2(24) + 19695439885029409450620000000000(3(2)) = 7 - 2(24) + 59086319655088228351860000000000(2) = 7 - 2(24) + 59086319655088228351860000000000(3(2)) = 7 - 2(24) + 177258959165264685055580000000000(2) = 7 - 2(24) + 177258959165264685055580000000000(3(2)) = 7 - 2(24) + 531776877495793855166740000000000(2) = 7 - 2(24) + 531776877495793855166740000000000(3(2)) = 7 - 2(24) + 1525797572238643388949928000000000(2) = 7 - 2(24) + 1525797572238643388949928000000000(3(2)) = 7 - 2(24) + 4577392716715930166849884000000000(2) = 7 - 2(24) + 4577392716715930166849884000000000(3(2)) = 7 - 2(24) + 13722378150147790500549652000000000(2) = 7 - 2(24) + 13722378150147790500549652000000000(3(2)) = 7 - 2(24) + 41167134450443371501648956000000000(2) = 7 - 2(24) + 41167134450443371501648956000000000(3(2)) = 7 - 2(24) + 123501403351329914505946680000000000(2) = 7 - 2(24) + 123501403351329914505946680000000000(3(2)) = 7 - 2(24) + 3701700000000000000000000000000000(2) = 7 - 2(24) + 3701700000000000000000000000000000(3(2)) = 7 - 2(24) + 11118100000000000000000000000000000(2) = 7 - 2(24) + 11118100000000000000000000000000000(3(2)) = 7 - 2(24) + 33354300000000000000000000000000000(2) = 7 - 2(24) + 33354300000000000000000000000000000(3(2)) = 7 - 2(24) + 100063000000000000000000000000000000(2) = 7 - 2(24) + 100063000000000000000000000000000000(3(2)) = 7 - 2(24) + 300189000000000000000000000000000000(2) = 7 - 2(24) + 300189000000000000000000000000000000(3(2)) = 7 - 2(24) + 900567000000000000000000000000000000(2) = 7 - 2(24) + 900567000000000000000000000000000000(3(2)) = 7 - 2(24) + 2701702000000000000000000000000000000(2) = 7 - 2(24) + 2701702000000000000000000000000000000(3(2)) = 7 - 2(24) + 81051080000000000000000000000000000000(2) = 7 - 2(24) + 81051080000000000000000000000000000000(3(2)) = 7 - 2(24) + 243153240000000000000000000000000000000(2) = 7 - 2(24) + 243153240000000000000000000000000000000(3(2)) = 7 - 2(24) + 729460730000000000000000000000000000000(2) = 7 - 2(24) + 729460730000000000000000000000000000000(3(2)) = 7 - 2(24) + 2188382200000000000000000000000000000000(2) = 7 - 2(24) + 2188382200000000000000000000000000000000(3(2)) = 7 - 2(24) + 6565146620000000000000000000000000000000(2) = 7 - 2(24) + 6565146620000000000000000000000000000000(3(2)) = 7 - 2(24) + 19695439885029409450620000000000000000000(2) = 7 - 2(24) + 19695439885029409450620000000000000000000(3(2)) = 7 - 2(24) + 59086319655088228351860000000000000000000(2) = 7 - 2(24) + 59086319655088228351860000000000000000000(3(2)) = 7 - 2(24) + 177258959165264685055580000000000000000000(2) = 7 - 2(24) + 177258959165264685055580000000000000000000(3(2)) = 7 - 2(24) + 531776877495793855166740000000000000000000($$

H/W 20/12/22 (Section 3) - Linear Congruences

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

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

$a = 2, b = 5, m = 7$   $\text{GCD}(2, 7) = 1 = (\mu, 18)$

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

$\therefore$  It has 1 solution,  $\text{GCD}(2, 7) = 1 = (\mu, 18)$

$$2x \equiv 5 \pmod{7}$$

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

$$\Rightarrow 2x - 5 = 7y \quad \forall y \in \mathbb{Z}$$

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

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

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

$$x5 \Rightarrow 5 = 7 \times 5 - 2 \times 15$$

$\therefore$  From ①,  $x = -15, y = -5$

$\therefore$  sol'n is,  $\cancel{x=5} \quad x \equiv -15 \pmod{7}$

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

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

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

$\therefore$  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,

$$1 = 19 - 2 \times 9$$

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

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

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

$$40 = 19(2) + 2$$

$$19 = 2(9) + 1$$

$$2 = 1(2) + 0$$

$$x30 \Rightarrow 30 = 19(570) - 40(270)$$

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

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

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

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

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

$\therefore$  It has 3 solutions.

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

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

$$\Rightarrow 3x - 6 = 9y$$

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

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

$$3 = 9 - 3(2) = 9x_1 - 3x_2$$

$$x_2 \Rightarrow 6 = 9x_2 - 3x_4$$

From ①,  $x_0 = -4, y_0 = -2$

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

Other solutions are,

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

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

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

$$(i) t = 0$$

$$(ii) t = 1$$

$$\Rightarrow x_0 = -4$$

$$\Rightarrow x_0 = -4 - 3 = -7 \Rightarrow x_0 = -10$$

$\therefore$  sol'n's are,

$$x \equiv -4 \pmod{9}, x \equiv -7 \pmod{9}, x \equiv -10 \pmod{9}$$

$$x \equiv -7 \pmod{9}$$

$$x \equiv -10 \pmod{9}$$

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

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

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

∴ It has 1 solution.

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

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

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

Now,  $(9, 25) = 1$  in L.C is,

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

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

From ①,  $x_0 = -55, y_0 = -20$

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

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

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

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

∴ It has 1 sol'n.

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

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

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

Now,  $(103, 999) = 1$  in L.C is

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

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

∴ From ①,  $x_0 = 43,068, y_0 = 4440$

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

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

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

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

∴ It has 1 sol'n.

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

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

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

$$\text{Now, } (980, 1597) = 1 \text{ in L.C.S,}$$

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

$$x610 \Rightarrow 610 = 980(26840) - 1597(16470)$$

$$\text{From } (1), x_0 = 26840, y_0 = 16470$$

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

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

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

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

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

∴ It has 1 sol'n

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

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

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

$$\text{Now, } (3, 7) = 1 \text{ in L.C.S,}$$

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

$$x_2 \Rightarrow 2 = 3(10) - 7(4)$$

$$\text{From } (1), x_0 = 10, y_0 = 4$$

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

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

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

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

$$(a,m) = (6,9) = 3 \text{ and } 3 \nmid 3$$

$\therefore$  It has 3 sol'n's.

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

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

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

Now,  $(6,9)=3$  in L.C is,

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

$$\text{From (1), } x_0=5, y_0=3$$

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

Other sol'n's are,

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

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

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

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

$\therefore$  sol'n's are,

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

$$x \equiv 2 \pmod{9}$$

$$x \equiv -1 \pmod{9}$$

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

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

$$(a,m) = (17,21) = 1 \text{ and } 1 \mid 14$$

$\therefore$  It has 1 sol'n

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

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

$$\Rightarrow 21y = 17x-14$$

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

Now,  $(17, 21) = 1$  in l.c is,  $\therefore (17, 21) \text{ gcd} \in \text{FCF}(1)$

$$\begin{aligned} 1 &= 17 - 4 \times 4 \\ &= 17 - (21 \times 1 - 17 \times 1) \times 4 \\ &= 17 \times 5 - 21 \times 4 \end{aligned}$$

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

From ①,  $x_0 = 20, y_0 = 16$

$\therefore x \equiv 20 \pmod{21}$  is a sol'n

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

$$a = 15, b = 9, m = 25 \quad (15, 25) = 5 \quad (15)(25) + (0)(5) = 1$$

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

$\therefore$  It has no solution.

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

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

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

$\therefore$  It has 1 sol'n.

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

$$\Rightarrow 1001 \mid (128x - 833) \quad \text{and to 'k' solutions repeat no soln}$$

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

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

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

$$x 833 \Rightarrow 833 = 128(2,54,065) - 1001(32,487) \quad 105 = 23(4) + 13$$

$$1001 = 128(7) + 105$$

$$128 = 105(1) + 23$$

$$23 = 13(1) + 10$$

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

$$13 = 10(1) + 3$$

$$10 = 3(3) + 1$$

$\therefore x \equiv 2,54,065 \pmod{1001}$  is sol'n

$$3 = 1(3) + 0$$

$\therefore$  solution is to move left in (l.c) & right in (r.c)

$$(1) 987x \equiv 610 \pmod{1597}$$

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

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

$\therefore$  It has 1 sol'n.

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

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

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

Now,  $(987, 1597) = 1$  in L.C. is,

$$1 = 987(610) - (1597)(377) \quad 1597 = 987(1) + 610$$

$$\text{From (1), } x_0 = 372100$$

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

$$\Rightarrow x \equiv 1596 \pmod{1597} \text{ is soln}$$

22/12/22

Inverse of 'a' modulo 'm' :-

If  $a \in \mathbb{Z}$ ,  $m \in \mathbb{Z}^+$  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'.

$$\underline{\text{Ex}}: a=3 \text{ & } m=4$$

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.,  $x \equiv 3 \pmod{4}$

$\therefore (3)^{-1}$  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.

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

the inverse of '7' modulo '31'.

Statement: Let  $P$  be a prime, then a positive

integer 'a' is its own inverse modulo 'P' iff

$$a \equiv 1 \pmod{P} \text{ or } a \equiv -1 \pmod{P}.$$

$$\text{Ex} : a=4, P=3 \text{ and } (a, P) = (4, 3) = 1$$

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

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

i.e., '4' is the inverse (of '4') mod '3'  $\therefore 4 \equiv -1 \pmod{3}$

Chinese Remainder Theorem:

Let  $m_1, m_2, \dots, m_r$  be pairwise relatively prime

positive integers. Then the congruences

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

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

Working rule

$$x_1 = \frac{a_1}{m_2} \cdot \frac{M}{m_1} = p_1$$

$$x_2 = \frac{a_2}{m_3} \cdot \frac{M}{m_2} = p_2$$

$$x_3 = a_3 \pmod{m_3}$$

$$x_4 = \frac{a_4}{m_5} \cdot \frac{M}{m_4} = p_4$$

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

$$x \equiv a_3 \pmod{m_3}$$

Step 1: Check  $(m_1, m_2) = 1, (m_2, m_3) = 1, (m_3, m_1) = 1$   
(pairwise relatively prime else CRT can't apply)

Step 2: Find  $M = m_1 \cdot m_2 \cdot m_3$

$$\text{also } a_1, a_2, a_3 \in \mathbb{Z} \iff (a_1 m_2 m_3), (a_2 m_1 m_3), (a_3 m_1 m_2) \in \mathbb{Z}$$

$$\text{Step 3: Find } M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, M_3 = \frac{M}{m_3}$$

$$(a_1 m_2 m_3) \in \mathbb{Z}$$

$$(a_2 m_1 m_3) \in \mathbb{Z}$$

$$(a_3 m_1 m_2) \in \mathbb{Z}$$

$$(a_1 m_2 m_3) \in \mathbb{Z}$$

Step 4: Find inverse  $y_1$  of  $M_1$  modulo  $m_1$

(i.e., sol'n of  $M_1 y_1 \equiv 1 \pmod{m_1}$ )

i.e.,  $M_1 y_1 \equiv 1 \pmod{m_1}$

Find inverse  $y_2$  of ' $M_2$ ' modulo ' $m_2$ '

i.e., sol'n of  $M_2 y_2 \equiv 1 \pmod{m_2}$

Find inverse  $y_3$  of ' $M_3$ ' modulo ' $m_3$ '

i.e., sol'n of  $M_3 y_3 \equiv 1 \pmod{m_3}$

Step 5: Find the value  $\sum_{i=1}^3 a_i M_i y_i$

Now,  $\boxed{x \equiv (\sum_{i=1}^3 a_i M_i y_i) \pmod{M}}$  is the unique

sol'n of three linear congruences.

~~$x \equiv 1 \pmod{3}$ ,  $x \equiv 2 \pmod{5}$ ,  $x \equiv 3 \pmod{7}$~~

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

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

$$= 105$$

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

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

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

Let,  $y_i$  be the inverse of ' $M_i$ ' modulo ' $m_i$ '

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$\Rightarrow 35 y_1 \equiv 1 \pmod{3} \Rightarrow y_1 = 2 \text{ is sol'n}$$

$$\text{Hence, } 21 y_2 \equiv 1 \pmod{5} \Rightarrow y_2 = 1 \text{ is sol'n}$$

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

$$\begin{aligned}
 \text{Now, } \sum_{i=1}^3 a_i M_i y_i &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \quad (\text{L.H.S}) \\
 &= (1)(35)(2) + (2)(21)(1) + (3)(15)(1) \\
 &= 70 + 42 + 45 \\
 &= 157
 \end{aligned}$$

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

linear congruences.

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

(\*) Solve  $x \equiv 1 \pmod{4}$ ,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$ ,

$$x \equiv 5 \pmod{7}$$

$$\begin{aligned}
 &\text{Given, } a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 5 \\
 &m_1 = 4, m_2 = 3, m_3 = 5, m_4 = 7
 \end{aligned}$$

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

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

Now we can apply CRT

$$\text{Now, } M = m_1 \cdot m_2 \cdot m_3 \cdot m_4$$

$\leftarrow 4 \times 3 \times 5 \times 7$  (to make it easier)

$$= 420$$

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

$$[m, m] M_2 = 0 \pmod{m_2} = \frac{420}{3} = 140$$

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

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

Let,  $y_i$  be the inverse of  $M_i$  modulo  $m_i$ .

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

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

$$\text{equation, } 105x + 4k = 1 \iff (m \text{ b.o.m}) D \in \mathbb{Z}$$

$$\therefore \text{inverse, } y_1 = 1$$

$$\text{iiy, (ii) } 140x \equiv 1 \pmod{3}$$

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

$$\frac{M}{m_2} + k = 10$$

$$\therefore \text{inverse, } y_2 = 2$$

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

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

$\therefore$  inverse,  $y_3 = 4$

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

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

$\therefore$  inverse,  $y_4 = 2$

$$\text{Now, } \sum_{i=1}^4 a_i M_i y_i = (1)(105)(1) + (2)(140)(2) + (3)(84)(4) + (5)(60) \\ = 105 + 560 + 1008 + 600 \\ = 2273$$

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

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

Method - 2 when any of  $m_1, m_2, m_3, \dots$  are not relatively prime see slide

Statement - 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  $\text{mod } [m_1, m_2]$

Statement - 2:

Consider the system of L.C.,

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

This system has a sol'n iff  $(m_1, m_2, m_3) \mid a_1 - a_2 \pmod{(i,j)}$

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

$$x \equiv a \pmod{m} \Rightarrow x = mk + a$$

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

other solns are,

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

where,  $d = (a, m)$

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

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

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

$m_1 = 6$ ,  $m_2 = 10$

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

$a_1 - a_2 = 5 - 3 = 2$

$(m_1, m_2) \mid a_1 - a_2 \therefore \text{the system has sol'n}$

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

$\Rightarrow x = 6t + 5 \text{ for } t \in \mathbb{Z}$

$\rightarrow \textcircled{1}$

sub 'x' in and eqn.

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

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

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

other sol'n's are,

$t = x_0 + \frac{m_2}{d} \cdot u, u = 0, 1, \dots, d-1$

$\rightarrow t = 3 + \frac{10}{2} \cdot u, u = 0, 1, \dots, 9 \text{ (i)}$

$\therefore t = 3, t = 8 \rightarrow t = 3 + 5u$   
 $\text{sub in } \textcircled{1},$

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

$\rightarrow x = 23 + 30u$

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

Ans. 11/11

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

$m_1 = 11$ ,  $m_2 = 17$

$(m_1, m_2) = (11, 17) = 1 \therefore m_1, m_2 \text{ are relatively prime}$

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

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

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

Let ' $y_1$ ' be the inverse of 'M' modulo 'm'

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

$x=2$  is a sol'n

$$\therefore y_1 = 2$$

if  $y_1, y_2$  be the inverse of 'M' modulo ' $m_1, m_2$ '

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

$x=14$  is a sol'n

$$\therefore y_2 = 14$$

$$\begin{aligned} \text{Now, } \sum_{i=1}^3 a_i M_i y_i &= a_1 M_1 y_1 + a_2 M_2 y_2 \\ &= (4)(17)(2) + (3)(11)(14) \\ &= 136 + 462 \\ &= 598 \end{aligned}$$

$\therefore$  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,  $a_1 = 1, a_2 = 2, a_3 = 3$

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

$(2, 3) = (3, 5) = (2, 5) = 1$  i.e.  $m_1, m_2, m_3$  relatively prime

$$M_1 = m_1 m_2 m_3 = 30$$

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

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

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

Let ' $y_1$ ' be the inverse of 'M' modulo 'm'

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

$x=1$  is a sol'n

$$\therefore y_1 = 1$$

$$10x \equiv 1 \pmod{3}$$

$x=1$  is sol'n

$$\therefore y_2 = 1$$

$$6x \equiv 1 \pmod{5}$$

$x=1$  is a sol'n

$$\therefore y_0 = 1$$

Now,

$$\begin{aligned} \sum_{i=1}^3 a_i M_i y_i &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= (1)(15)(1) + (2)(10)(1) + (3)(6)(1) \\ &= 15 + 20 + 18 \\ &= 53 \end{aligned}$$

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

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

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

$$x \equiv 13 \pmod{15}$$

Given,  $a_1 = 4, a_2 = 13$

$$m_1 = 6, m_2 = 15$$

$$(6, 15) = 3 \quad \text{i.e., } m_1, m_2 \text{ are not relatively prime}$$

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

$\therefore$  The system has sol'n

consider,  $x \equiv 4 \pmod{6}$

$$\Rightarrow x = 6t + 4 \quad \forall t \in \mathbb{Z} \quad (1)$$

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'n's are,

$$t = x_0 + \frac{m}{d} \cdot u \quad \text{due to } \text{LCM}$$

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

$$\Rightarrow t = 1 + 5u$$

$$\text{sub in } (1) \quad \text{due to LCM}$$

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

$$\Rightarrow x = 5u + 10$$

$\therefore x \equiv 10 \pmod{15}$  is the sol'n

27/12/22

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

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

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

$$(6, 8) = 2 \quad \text{e.g. } 2 \mid 4-2$$

$$(8, 9) = 1 \quad \text{e.g. } 1 \mid 8-1$$

$$(9, 6) = 3 \quad \text{e.g. } 3 \mid 4-1$$

$\therefore$  The system has sol'n.

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

$$\Rightarrow x = 6t + 4 \quad \forall t \in \mathbb{Z}$$

$\rightarrow (1)$

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

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

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

$t=1$  is a sol'n

\* ~~too~~

$$\Rightarrow 3t \equiv -1 \pmod{4}$$

$t=1$  is a sol'n

i.e.,  $t \equiv 1 \pmod{4}$

$$\Rightarrow t = 4u + 1$$

sub 't' in (1)

$$\Rightarrow x = 6(4u+1) + 4 \quad \text{or } x \equiv 4 + 24u \pmod{24}$$

$$\Rightarrow x = 24u + 10$$

$\rightarrow (2)$

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

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

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

$$\Rightarrow 8u \equiv -3 \pmod{9}$$

( $\because \div \text{ by } 3$ )

$u = 0$  is a sol'n

$\therefore u \equiv 0 \pmod{3}$  is the sol'n.

$$\Rightarrow u = 3v + 0 \rightarrow (3) \text{ is a sol'n}$$

sub ③ in ②

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

$$\Rightarrow x = 72v + 10$$

$\therefore x \equiv 10 \pmod{72}$  is the sol'n.

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

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

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

$$(4,9) = 1 \quad \text{e.g. } 10 \equiv 5 \pmod{4}$$

$$(9,12) = 3 \quad \text{e.g. } 3 \mid 5 - 8$$

$$(12,4) = 4 \quad \text{e.g. } 4 \mid 10 - 8$$

$\therefore$  The system has sol'n.

consider,  $x \equiv 0 \pmod{4}$

$$\Rightarrow x = 4t \quad t \in \mathbb{Z}$$

→ ①

$$x \equiv 4t \equiv 0 \pmod{4}$$

sub ① in 2nd eqn

$$4t \equiv 5 \pmod{9}$$

$t = 8$  is a sol'n

$$\therefore t \equiv 8 \pmod{9}$$

$$\Rightarrow t = 9u + 8$$

$$\begin{aligned} &\text{sub 't' in ①} \\ &x = 4(9u + 8) \end{aligned}$$

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

sub ② in 3rd eqn

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

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

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

$3u + 1 \equiv 0 \pmod{1}$  is a sol'n if  $u = 0$

$$\Rightarrow u \equiv 0 \pmod{1} \text{ is the sol'n.}$$

$$\rightarrow u = v \rightarrow (3)$$

sub (3) in (2)

or  
a'

$$x = 36v + 32$$

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

### System of linear congruences in 2 variables

\*  
so

Consider the 2 linear congruences in the variables

$$x, y \quad ax + by \equiv e \pmod{m}$$

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

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

$$\textcircled{1} \times 5 - \textcircled{2} \times 4$$

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

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

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

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

$$\text{sub } x = 7 \text{ in } (1),$$

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

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

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

### Method - 2

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

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

sol'n is,

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

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

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