Unit-4

DIOPHANTINE EQUATIONS AND CONGRUENCES

Defn [Linear diophantine equation]

A linear diophantine equation in two variables x and y is an equation of the form $ax + by = c$

Here a, b, c are integers with a & b are not both zero.

Example $2x + 3y = 4$.

Theorem ①: The linear diophantine equation $ax + by = c$ has a solution iff d/c where $d = gcd(a, b)$

If x_0, y_0 is any particular solution of this eqn, then all other solutions are given by $x = x_0 + \left(\frac{b}{d}\right)t$ and

$y = y_0 - \left(\frac{a}{d}\right)t$ for varying integers t

Proof:-

Let $ax + by = c$ be the linear diophantine eqn with $d = gcd(a, b)$

Assume that $ax + by = c$ has a soln.

i) $\exists$ integers x_0, y_0 such that $ax_0 + by_0 = c$ ⟶ ①

Claim: d/c.

Since $d = gcd(a, b)$, d/a and d/b.

$\Rightarrow a = q_1 d$ and $b = q_2 d$, $q_1, q_2 \in \mathbb{Z}$

Sub $a = q_1 d$ and $b = q_2 d$ in ①

$$q_1 d x_0 + q_2 d y_0 = c$$

$$d[q_1 x_0 + q_2 y_0] = c.$$

(or) c is a multiple of d.

$\Rightarrow d/c$.

Conversely assume that d/c.

Claim: $ax+by=c$ has a soln.

Since d/c, $c = td$ → (2) where $t \in Z$.

We know that, "gcd of a & b can be written as a linear combination of themselves."

$\therefore d = ax_0 + by_0$ for some integers x_0 & y_0.

Multiply both sides by t

$$td = t(ax_0 + by_0)$$

$$c = t(ax_0 + by_0). \quad \text{(using (2))}$$

$$c = a(tx_0) + b(ty_0).$$

∴ The linear diophantine eqn $ax+by=c$ has a soln $x = tx_0$, $y = ty_0$.

To prove: General soln of $ax+by=c$ has the form

$$\boxed{\begin{aligned} x &= x_0 + \left(\frac{b}{d}\right)t \\ y &= y_0 - \left(\frac{a}{d}\right)t \end{aligned}}$$

where x_0 & y_0 is any particular soln.

Let x_0, y_0 be particular soln of $ax+by=c$

$\Rightarrow ax_0 + by_0 = c$ → (3)

Let x' & y' be any other soln of $ax+by=c$.

$\Rightarrow ax'+by'=c$. → (4)

It is enough to prove $x' = x_0 + \left(\frac{b}{d}\right)t$

$y' = y_0 - \left(\frac{a}{d}\right)t$.

From ② & ④,

$$ax_0 + by_0 = ax' + by'$$

$$\Rightarrow by_0 - by' = ax' - ax_0$$

$$\Rightarrow b(y_0 - y') = a(x' - x_0).$$

$$\Rightarrow \frac{b}{d}(y_0 - y') = \frac{a}{d}(x' - x_0). \longrightarrow ⑤.$$

Since $\gcd(a,b) = d$, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

From ⑤ $\left(\frac{b}{d}\right)$ devides $\left(\frac{a}{d}\right)(x' - x_0)$.

Euclid: If A, B are relatively prime with A/BC then A/C.

Applying Euclid theorem with $A = b/d$, $B = a/d$, $C = (x' - x_0)$.

Then $\left(\frac{b}{d}\right)$ devides $(x' - x_0)$.

$\Rightarrow x' - x_0$ is a multiple of b/d.

$\Rightarrow x' - x_0 = \left(\frac{b}{d}\right)t$ where $t \in Z$. $\longrightarrow$ ⑥.

$\Rightarrow \boxed{x' = x_0 + \left(\frac{b}{d}\right)t}$, $t \in Z$ $\longrightarrow$ ⑥.

Sub ⑥ in ⑤

$$\left(\frac{b}{d}\right)(y_0 - y') = \left(\frac{a}{d}\right) \times \left(\frac{b}{d}\right)t.$$

$$\Rightarrow y_0 - y' = \left(\frac{a}{d}\right)t.$$

$$\Rightarrow \boxed{y' = y_0 - \left(\frac{a}{d}\right)t}$$

Hence the proof.

Procedure For Finding Solution of Linear Diophantine Eqn

Suppose we want to find the general soln of

LDE $ax + by = c$ ⟶ ①

Step ① Find the $\gcd(a,b) = d$ (say)

If d/c, given LDE has a soln

If $d \not| c$, given LDE does not have a soln.

Step ② Write $\gcd(a,b)$ as a linear combination of a and b.

Say $\alpha a + \beta b = d$ where $d = \gcd(a,b)$

⟶ ②

Step ③

Multiply eqn ② by an integer $\frac{c}{d}$.

Then the resulting eqn is of the form

$$\alpha \frac{c}{d}(a) + \beta \frac{c}{d}(b) = c.$$

Particular soln is

$$x_0 = \alpha \frac{c}{d}$$

$$y_0 = \beta \frac{c}{d}.$$

Step (4)

General soln is

$$x = x_0 + \left(\frac{b}{d}\right)t$$

$$y = y_0 - \left(\frac{a}{d}\right)t$$

where t is any integer.

If we put different values of t we get infinite number of solutions for given LDE.

Problems

① Find all the possible solution of the linear diophantine equation $172x + 20y = 1000$.

Soln.

Step① To find gcd (172, 20).

Divide 172 by 20, $172 = 8(20) + 12$; $0 < 12 < 20$.

Divide 20 by 12, $20 = 1(12) + 8$, $0 < 8 < 12$

Divide 12 by 8, $12 = 1(8) + 4$, $0 < 4 < 8$.

Divide 8 by 4, $8 = 2(4) + 0$.

Stop the process

The last non-zero remainder is gcd (172, 20).

$\therefore$ gcd (172, 20) = 4.

$4 / 1000$ $\therefore$ Given LDE has a soln.

Step② Write gcd (172, 20) as a linear combination of 172, 20

Using above eqns in step①

$4 = 12 - 8$

$= 12 - [20 - 12]$

$= 2(12) - 20.$

$= 2(172 - 8(20)) - 20$

$4 = 2(172) - 17(20).$

Step③

~~2(172) + 20(-17) = 4.~~ $172(2) + 20(-17) = 4.$

Multiply by 250.

~~500(172) + 20(-17)250 = 1000.~~ $172(2 \times 250) + 20(-17 \times 250) = 1000$

$\Rightarrow 172(500) + 20(-4250) = 1000.$

∴ Particular soln $\boxed{x_0 = 500 \quad y_0 = -4250}$

Step (4)

General soln $x = x_0 + \left(\frac{b}{d}\right)t$

$y = y_0 - \left(\frac{a}{d}\right)t.$

$a = 172, \quad b = 20. \quad , \quad d = \gcd(172, 20) = 4.$

∴ $x = 500 + \left(\frac{20}{4}\right)t.$

$x = 500 + 5t$

$y = y_0 - \left(\frac{a}{d}\right)t$

$y = -4250 - \left(\frac{172}{4}\right)t$

$y = -4250 - 43t$

$=$ ~~0 4 9 9 3 0~~.

$=$

∴ General soln is $\boxed{x = 500 + 5t \quad y = -4250 - 43t}$; $t \in Z$.

(2) Find the general soln of a linear diophantine eqn

$76x + 176y = 276$.

Soln

Step(1) To find $\gcd(76, 176)$.

Divide 176 by 76, $176 = 2(76) + 24$; $0 < 24 < 76$.

Divide 76 by 24, $76 = 3(24) + 4$; $0 < 4 < 24$.

Divide 24 by 4, $24 = 6(4) + 0$.

Stop the process.

$\gcd(76, 176)$ = last non zero remainder

$\gcd(76, 176) = 4$.

$4 \mid 276$ ∴ Given LDE has a soln.

Step(2) To write $\gcd(76, 176)$ as a linear combination of 76, 176.

$$4 = 76 - 3(24)$$
$$= 76 - 3[176 - 2(76)]$$
$$= 76 - 3(176) + 6(76)$$
$$4 = 7(76) - 3(176).$$

Step(3)

$76(7) + 176(-3) = 4$.

Multiply by 69.

$76(7 \times 69) + 176(-3 \times 69) = 276$.

$76(483) + 176(-207) = 276$.

∴ $x_0 = 483$, $y_0 = -207$ is particular soln.

276
4
= 69

Step(4)

General soln $x = x_0 + \left(\frac{b}{d}\right)t$

$y = y_0 - \left(\frac{a}{d}\right)t$.

$a = 76,\ b = 176,\ d = 4,\ x_0 = 483,\ y_0 = -207.$

$x = 483 + \left(\frac{176}{4}\right)t$; $y = y_0 - \left(\frac{a}{d}\right)t$

$x = 483 + 44t$; $y = -207 - \left(\frac{76}{4}\right)t$

$y = -207 - 19t$

$\therefore$ $\boxed{\begin{aligned} x &= 483 + 44t \\ y &= -207 - 19t \end{aligned}}$; $t \in Z$ is general soln of given LDE.

Homework

(1) Determine whether each LDE is solvable

(i) $24x + 52y = 102$

(ii) $43x + 8y = 1$

(iii) $2x + 6y = 3$.

(2) Find the general soln of $12x + 20y = 28$.

③ If a cock is worth five coins, a hen three coins and three chicks together one coin, how many cocks, hens and chicks, totalling 100, can be bought for 100 coins.

Soln.

Let x be the number of cocks

y be the number of hens

z be the number of chicks.

Then $x+y+z = 100 \longrightarrow ①$

$5x + 3y + \frac{z}{3} = 100. \longrightarrow ②$

From ①, $z = 100 - x - y. \longrightarrow ③$

Sub ③ in ②

$$5x + 3y + \frac{(100 - x - y)}{3} = 100.$$

Multiply by 3

$$15x + 9y + (100 - x - y) = 300.$$

$$\Rightarrow 14x + 8y = 200.$$

$\div$ by 2, $7x + 4y = 100.$

We will solve the LDE $7x + 4y = 100.$

Step (0) To find gcd (7, 4).

Divide 7 by 4, $7 = 1(4) + 3$, $0 < 3 < 4.$

Divide 4 by 3, $4 = 1(3) + 1$, $0 < 1 < 3.$

Divide 3 by 1, $3 = 1(3) + 0.$

Stop the process.

$\therefore$ gcd (7, 4) = 1. $\mid 100$ $\therefore 7x + 4y = 100$ has a soln.

Step(2) TO write gcd(7,4) as a linear combination of 7 and 4.

$$1 = 4 - 3$$
$$= 4 - (7-4)$$
$$1 = 2(4) - 1(7)$$

Step(3)

$\therefore 7(-1) + 4(2) = 1.$

Multiply by 100

$7(-100) + 4(200) = 100.$

$\therefore$ Particular soln is $\boxed{\begin{aligned} x_0 &= -100 \\ y_0 &= 200 \end{aligned}}$

Step(4). TO find General soln $x = x_0 + \left(\frac{b}{d}\right)t$

$$y = y_0 - \left(\frac{a}{d}\right)t.$$

Here $a=7,\ b=4,\ d=1.$

$$x = -100 + 4t$$
$$y = 200 - 7t. \quad ; t \in Z.$$

Since x and y are number of cocks and hens respectively, they cannot be negative

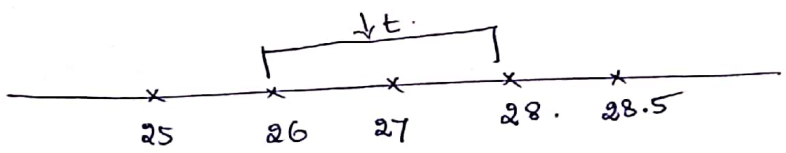
$\therefore$ We must choose 't' so that $x \geq 0$ & $y \geq 0$.

i) $x = -100 + 4t \geq 0.$ and $y = 200 - 7t \geq 0.$

$\Rightarrow 4t \geq 100$ and $7t \leq 200$

$\Rightarrow t \geq 25$ and $t \leq \frac{200}{7} = 28.5.$

$\therefore t \geq 25$ and $t \leq 28.5.$



$\therefore$ t can take values 26, 27 or 28.

t	$x = -100+4t$	$y = 200-7t$	$z = 100-x-y$
26	$x = -100+104$ $x = 4$	$y = 200-7(26)$ $y = 18$	$z = 100-4-18$ $z = 78$
27	$x = 8$	$y = 11$	$z = 81$
28	$x = 12$	$y = 4$	$z = 84$.

The above table gives possible soln of given problem.

④ Find the general solution of the LDE $15x + 21y = 39$.

U.Q

8m

Soln. Given : $15x + 21y = 39$.

Step(1) To find $\gcd(15, 21)$.

Divide 21 by 15, $21 = 1(15) + 6$. , $0 < 6 < 15$

Divide 15 by 6, $15 = 2(6) + 3$, $0 < 3 < 6$.

Divide 6 by 3 , $6 = 2(3) + 0$.

Stop the process.

$\therefore \gcd(15, 21) =$ last non zero remainder

$d = \gcd(15, 21) = 3$.

$3/39$ $\therefore$ given LDE has a soln.

Step(2) To write $\gcd(15, 21)$ as a linear combination of 15 and 21.

$$3 = 15 - 2(6)$$
$$= 15 - 2[21 - 15]$$
$$= 15 - 2(21) + 2(15)$$
$$3 = 3(15) - 2(21)$$

Step(3)

$$15(3) + 21(-2) = 3.$$

Multiply by 13.

$$15(3 \times 13) + 21(-2 \times 13) = 39.$$

$$15(39) + 21(-26) = 39.$$

$\therefore$ Particular soln is $\boxed{\begin{array}{l} a_0 = 39 \\ y_0 = -26 \end{array}}$

Step(4)

General soln is $x = x_0 + \left(\frac{b}{d}\right)t$

$y = y_0 - \left(\frac{a}{d}\right)t.$

$x_0 = 39,\ y_0 = -26,\ a = 15,\ b = 21,\ d = 3.$

$\therefore\ x = 39 + \left(\frac{21}{3}\right)t \Rightarrow x = 39 + 7t$

$y = -26 - \left(\frac{15}{3}\right)t \Rightarrow y = -26 - 5t$; t

$\therefore$ General soln of given LDE is of the form

$x = 39 + 7t$

$y = -26 - 5t$ where $t \in \mathbb{Z}$.

Defn [Congruence modulo m].

Let m be a +ve integer.

An integer 'a' is congruent to an integer b modulo m if $m \mid a-b$.

In symbol $a \equiv b \pmod{m}$.

[may be read as a is congruent to b mod m]

Examples

① $23 \equiv 3 \pmod{5}$

$\because 5 \mid (23-3) = 20$.

② $20 \not\equiv 3 \pmod{4}$

$\because 4 \nmid (20-3) = 17$.

Theorem ② $a \equiv b \pmod m$ if and only if a and b leave the same remainder when divided by m.

Proof: Assume that $a \equiv b \pmod m$

$\Rightarrow m \mid a-b.$

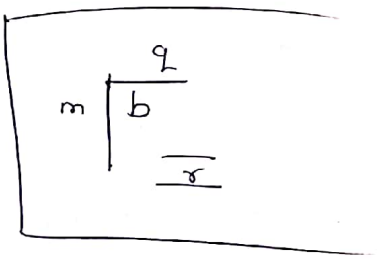
$\Rightarrow a-b$ is a multiple of m

$\Rightarrow a-b = km$ where $k \in Z$.

$\Rightarrow a = b+km.$ $\longrightarrow$ ①

Claim: a and b leave the same remainder when divided by m.

Using division algorithm, $b = mq + r$ $\longrightarrow$ ②



Sub ② in ①

$a = mq + r + km$

$a = m(q+k) + r$

$\therefore$ a leaves the remainder 'r' when it divided by m.

Also b leaves the remainder 'r' when it divided by m.

Conversely assume that a and b leave the same remainder when it divided by m.

$\Rightarrow a = q_1 m + r$

and

$b = q_2 m + r.$

$\therefore a-b = (q_1 - q_2)m$ is a multiple of m.

$\Rightarrow m \mid (a-b)$

$\therefore a \equiv b \pmod m$

H/p.

Important Results

① $a \equiv a \pmod m$ [Reflexive property]

② If $a \equiv b \pmod m$ then $b \equiv a \pmod m$ [Symmetric property]

③ If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ then $a \equiv c \pmod m$

[Transitive property]

④ If $a \equiv b \pmod m$ and $c \equiv d \pmod m$

then $a + c \equiv b + d \pmod m$

also $ac \equiv bd \pmod m$

⑤ Suppose a, b are ~~+ve integers~~ non -ve integers, $0 \le b < m$

$a \equiv b \pmod m$ means that "a leaves the remainder b" when it divided by m".

For example $23 \equiv 3 \pmod 4$.

$$4 \overline{)23} \quad (5)$$
$$20$$
$$3.$$

$3 \rightarrow$ remainder.

⑥ If $a \equiv b \pmod m$

then $a^n \equiv b^n \pmod m$, n is any +ve integer.

⑦ If $a \equiv b \pmod m$

then $ac \equiv bc \pmod m$, $c \in Z$.

Problems

① U.Q 2m

What is the remainder when 3^{31} is divided by 7.

Soln.

$3^2 \equiv 2 \pmod 7$.

$3^3 \equiv 6 \pmod 7$.

$3^4 \equiv 4 \pmod 7$

$3^5 \equiv 5 \pmod 7$

$3^6 \equiv 1 \pmod 7$

$3^6 = 729$

$$7 \overline{)729} \quad 104 \quad (728 \quad 1$$

$\Rightarrow (3^6)^5 \equiv 1^5 \pmod 7$

$\Rightarrow 3^{30} \equiv 1 \pmod 7$

$\Rightarrow 3^{30} \times 3 \equiv 1 \times 3 \pmod 7$

$\Rightarrow 3^{31} \equiv 3 \pmod 7$.

$\therefore 3^{31}$ leaves the remainder 3 when it divided by 7.

② Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 15.

Soln.

$1! \equiv 1 \pmod{15}$

$2! \equiv 2 \pmod{15}$

$3! \equiv 6 \pmod{15}$

$4! \equiv 9 \pmod{15}$

$5! \equiv 0 \pmod{15}$

$6! \equiv 0 \pmod{15}$

$\vdots$

$100! \equiv 0 \pmod{15}$

$\Rightarrow 1! + 2! + \cdots + 100! \equiv 1 + 2 + 6 + 9 + 0 + \cdots + 0 \pmod{15}$

$\equiv 3 \pmod{15}$.

$\therefore$ Required remainder is '3'

(3) Show that $41 \mid 2^{20}-1$.

Soln:

It is enough to prove $2^{20} \equiv 1 \pmod{41}$.

We know that $2 \equiv 2 \pmod{41}$ $\left(\because 41 \mid 2-2\right)$

$2^2 \equiv 2^2 \pmod{41}$

$2^5 \equiv 2^5 \pmod{41}$

$\because$ $2^5 \equiv 32 \pmod{41}$. $\longrightarrow$ (1)

Also $32 \equiv -9 \pmod{41}$ $\longrightarrow$ (2).

Using Transitive property, $2^5 \equiv -9 \pmod{41}$

$\Rightarrow (2^5)^4 \equiv (-9)^4 \pmod{41}$

$\Rightarrow 2^{20} \equiv 6561 \pmod{41}$. $\longrightarrow$ (3)

$6561 \equiv 1 \pmod{41}$ $\longrightarrow$ (4)

$\left(\because 41 \mid (6561-1)\right)$

Using Transitive property $2^{20} \equiv 1 \pmod{41}$.

$\therefore 41 \mid 2^{20}-1$.

Homeworks

(1) Show that $89 \mid 2^{44}-1$.

(2) Show that $97 \mid 2^{48}-1$.

Linear Congruence

Defn [Linear congruence]

The congruence $ax \equiv b \pmod{m}$ is called linear congruence.

Notes * The solution of a linear congruence is an integer 'x_0' such that $ax_0 \equiv b \pmod{m}$.

Example

$2x \equiv 3 \pmod{5}$ is a linear congruence.

and $x_0 = 4$ is a soln of this linear congruence.

$(\because\ 2(4) \equiv 3 \pmod{5})$

$5/_{8-3}$

Solution of Linear congruence $ax \equiv b \pmod{m}$

Step ① Find $\gcd(a, m) = d$.

If $\gcd(a, m)$ divides b, then linear congruence has a soln

Otherwise not.

Step ② Guess any particular soln x_0.

Step ③ General solution is $x = x_0 + \left(\frac{m}{d}\right)t$ where $0 \le t < d$.

If we put $t = 0, 1, 2, \ldots (d-1)$ then we get 'd' Incongruent solutions.

Problems

① Solve the congruence $12x \equiv 48 \pmod{18}$.

Soln:

Step①

We know that $ax \equiv b \pmod{m}$ has a soln if $\gcd(a,m)$ devides b.

$a=12,\ b=48,\ m=18.$

$\gcd(a,m) = \gcd(12,18) = 6.$

$6 \mid 48.$

∴ Given linear congruence has a soln.

Step②

Put $x=1$ in given eqn : $12x \equiv 48 \pmod{18}$

$12 \equiv 48 \pmod{18}$

$18 \mid 12-48$ (or) $18 \mid -36$. is True.

∴ $x_0 = 1$ is a particular soln.

Step(3)

General soln is $x = x_0 + \left(\frac{m}{d}\right)t$

where $d = \gcd(a,m)$, $t = 0,1,2,\ldots (d-1)$.

$x = 1 + \left(\frac{18}{6}\right)t$; $t = 0,1,2\ldots (d-1)$

$x = 1+3t$; $t = 0,1,2,\ldots (6-1)$

$x = 1+3t$, $t = 0,1,2,\ldots 5$.

∴ $\boxed{x = 1,4,7,10,13,16}$ are solutions.

(2) Solve $49x \equiv 94 \pmod{36}$ for incongruent solutions.

Soln

Step (1) $ax \equiv b \pmod{m}$ has a soln if $\gcd(a,m) \mid b$.

$49x \equiv 94 \pmod{36}$.

$a = 49,\ b = 94,\ m = 36$.

$49 = 7 \times 7$

$36 = 2 \times 2 \times 3 \times 3$.

$\therefore$ Using canonical decomposition $\gcd(49,36) = 1$.

$1 \mid 94$.

$\therefore$ given linear congruence has a soln.

Step (2) By guessing $x_0 = 46$ is a soln.

($\because 49 \times 46 = 2254 \equiv 94 \pmod{36}$)

Since the given linear congruence has only one soln, general soln is $\boxed{x = 46.}$

$\therefore$ There is only one incongruent solution $x = 46$.

③ Solve $91x \equiv 119 \pmod{28}$ for incongruent solutions.

Soln

$ax \equiv b \pmod{m}$ has a soln if $\gcd(a,m) \mid b$.

Step ①

$91x \equiv 119 \pmod{28}$

$a = 91,\ b = 119,\ m = 28$

$91 = 7 \times 13$

$28 = 2^2 \times 7$

$\therefore \gcd(91, 28) = 7$

Also $7 \mid 119$.

$\therefore$ Given linear congruence has soln.

Step ②

Put $x = 1$ in $91x \equiv 119 \pmod{28}$

$91 \times 1 \equiv 119 \pmod{28}$

$28 \mid (91 - 119) = -28$.

$\therefore x_0 = 1$ is a particular soln.

Step ③

General soln is $x = x_0 + \left(\frac{m}{d}\right)t,\ t = 0, 1, 2, \ldots, (d-1)$

$d = \gcd(a, m)$

$d = \gcd(91, 28) = 7$.

$\therefore x = 1 + \left(\frac{28}{7}\right)t,\ t = 0, 1, 2, \ldots (7-1)$

$x = 1 + 4t,\ t = 0, 1, 2, \ldots 6$.

$x = 1, 5, 9, 13, 17, 21, 25$ are incongruent solutions.

(4) Solve $48x \equiv 144 \pmod{84}$ for incongruent solutions.

Soln

Step(1) $ax \equiv b \pmod{m}$ has a soln if $\gcd(a,m) \mid b$.

$48x \equiv 144 \pmod{84}$

$a=48,\ b=144,\ m=84.$

$48 = 2\times2\times2\times2\times3 = 2^4\times3$

$84 = 2\times2\times3\times7 = 2^2\times3\times7.$

$\therefore \gcd(48,84) = 2^2\times3 = 12.$

Also $12 \mid 144$.

$\therefore$ Given congruence has soln.

Step(2) Put $x=3$ in $48x \equiv 144 \pmod{84}$

$48\times3 \equiv 144 \pmod{84}$

$144 \equiv 144 \pmod{84}$

$\because 84 \mid 144-144.$

$\therefore x_0 = 3$ is a particular soln.

Step(3) General soln is $x = x_0 + \left(\frac{m}{d}\right)t,\ t=0,1,2\ldots(d-1)$

$d = \gcd(a,m) = \gcd(48,84) = 12.$

$\therefore x = 3 + \left(\frac{84}{12}\right)t,\ t=0,1,2\ldots(d-1)$

$x = 3+7t,\ t=0,1,2\ldots,(12-1)$

$x = 3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73, 80.$ are required incongruent solns.

2 x 2 Linear System

A 2x2 linear system is a system of linear congruence of the form

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

A solution of the linear system is a pair $x = x_0 \pmod{m}$, $y = y_0 \pmod{m}$ that satisfies both congruences.

Example

$$\left.\begin{aligned} 2x + 3y &\equiv 4 \pmod{13} \\ 3x + 4y &\equiv 5 \pmod{13} \end{aligned}\right\} \longrightarrow ①$$

is a 2x2 linear system.

Also $x \equiv 12 \pmod{13}$, $y = 2 \pmod{13}$ is a solution of the system.

i) $x - 12$ = multipe of 13

$\Rightarrow x - 12 = 13t$

$\Rightarrow \boxed{x = 12 + 13t}$, $t \in Z$

$y - 2$ = multipe of 13

$\boxed{y = 2 + 13t}$, $t \in Z$

For example, $x = 12$, $y = 2$ is a soln of 2x2 linear system

(Put $x = 12$, $y = 2$ in ①

$24 + 6 = 30 \equiv 4 \pmod{13}$

$36 + 8 = 44 \equiv 5 \pmod{13}$)

① Solve the linear system $2x + 3y \equiv 4 \pmod{13}$

$3x + 4y \equiv 5 \pmod{13}$

Soln

Given $2x + 3y \equiv 4 \pmod{13}$ ⟶ ①

$3x + 4y \equiv 5 \pmod{13}$ ⟶ ②

① × 4 $\Rightarrow$ $8x + 12y \equiv 16 \pmod{13}$

② × 3 $\Rightarrow$ $9x + 12y \equiv 15 \pmod{13}$

(−) $-x \equiv 1 \pmod{13}$

$\Rightarrow x \equiv -1 \pmod{13}$

$\Rightarrow x \equiv (13-1) \pmod{13}$

$\Rightarrow \boxed{x \equiv 12 \pmod{13}}$

Sub $x \equiv 12 \pmod{13}$ in ①

$2(12) + 3y \equiv 4 \pmod{13}$

$\Rightarrow 24 + 3y \equiv 4 \pmod{13}$

$\Rightarrow 3y \equiv 4 - 24 \pmod{13}$

$\Rightarrow 3y \equiv -20 \pmod{13}$

Also $-20 \equiv 6 \pmod{13}$

$\Rightarrow 3y \equiv 6 \pmod{13}$

$\Rightarrow \frac{3y}{3} \equiv \frac{6}{3} \pmod{13}$

$\Rightarrow \boxed{y \equiv 2 \pmod{13}}$

∵ Using Transitive property

$3y \equiv -20 \pmod{13}, -20 \equiv 6 \pmod{13}$

$\Rightarrow 3y \equiv 6 \pmod{13}$

∴ Soln is $\boxed{\begin{array}{l} x \equiv 12 \pmod{13} \\ y = 2 \pmod{13} \end{array}}$

(2) Solve the linear system

U.Q

8m

$$5x + 6y \equiv 10 \pmod{13}$$
$$6x - 7y \equiv 2 \pmod{13}$$

Soln

Given $5x + 6y \equiv 10 \pmod{13}$ ⟶ ①

$6x - 7y \equiv 2 \pmod{13}$ ⟶ ②

① × 7 $\Rightarrow 35x + 42y \equiv 70 \pmod{13}$

② × 6 $\Rightarrow 36x - 42y \equiv 12 \pmod{13}$

(+) $71x \equiv 82 \pmod{13}$

$82 \equiv 5 \times 71 \pmod{13}$

Using Transitive property $71.x \equiv 5 \times 71 \pmod{13}$

$\Rightarrow \frac{71x}{71} \equiv \frac{5 \times 71}{71} \pmod{13}$

$\Rightarrow \boxed{x \equiv 5 \pmod{13}}$

Sub $x \equiv 5 \pmod{13}$ in ①

$5(5) + 6y \equiv 10 \pmod{13}$

$25 + 6y \equiv 10 \pmod{13}$

$6y \equiv -15 \pmod{13}$

$-15 \equiv 11 \pmod{13}$

Transitive property $\Rightarrow 6y \equiv 11 \pmod{13}$

$11 \equiv 24 \pmod{13}$

Trans. prop. $\Rightarrow 6y \equiv 24 \pmod{13}$

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

~~$\Rightarrow y \equiv 4 \pmod{13}$~~

$\Rightarrow \boxed{y \equiv 4 \pmod{13}}$

∴ Soln is

$\boxed{\begin{aligned} x &= 5 \pmod{13} \\ y &= 4 \pmod{13} \end{aligned}}$

(3) Solve the 2x2 linear system

$3x + 4y = 5 \pmod 7$

$4x + 5y \equiv 6 \pmod 7$

Soln:

Given $3x + 4y \equiv 5 \pmod 7 \longrightarrow ①$

$4x + 5y \equiv 6 \pmod 7 \longrightarrow ②$

$① \times 5 \Rightarrow 15x + 20y \equiv 25 \pmod 7$

$② \times 4 \Rightarrow 16x + 20y \equiv 24 \pmod 7$

$(-)$

$-x \equiv 1 \pmod 7$

$\Rightarrow x \equiv -1 \pmod 7$

$\Rightarrow x \equiv (7-1) \pmod 7$

$\Rightarrow \boxed{x \equiv 6 \pmod 7}$

Sub $x \equiv 6 \pmod 7$ in ①

$3(6) + 4y \equiv 5 \pmod 7$

$18 + 4y \equiv 5 \pmod 7$

$4y \equiv 5 - 18 \pmod 7$

$4y \equiv -13 \pmod 7$

$-13 \equiv 1 \pmod 7$

Transitive property $\Rightarrow 4y \equiv 1 \pmod 7$

$1 \equiv -20 \pmod 7$

Transitive property $\Rightarrow 4y \equiv -20 \pmod 7$

$\Rightarrow y \equiv -5 \pmod 7$

$\Rightarrow y \equiv (7-5) \pmod 7$

$\boxed{y \equiv 2 \pmod 7}$

$\therefore$ Soln is $\boxed{\begin{array}{l} x \equiv 6 \pmod 7 \\ y \equiv 2 \pmod 7 \end{array}}$

④ Solve the 2×2 linear system

$$x + 3y \equiv 3 \pmod{11}$$
$$5x + y \equiv 5 \pmod{11}$$

Soln Given $x + 3y \equiv 3 \pmod{11}$ ⟶ ①

$5x + y \equiv 5 \pmod{11}$ ⟶ ②

① $\Rightarrow$ $x + 3y \equiv 3 \pmod{11}$

②×3 $\Rightarrow$ $15x + 3y \equiv 15 \pmod{11}$

(−) $-14x \equiv -12 \pmod{11}$

$\Rightarrow 14x \equiv 12 \pmod{11}$

$12 \equiv 56 \pmod{11}$

Trans. prop $\Rightarrow 14x \equiv 56 \pmod{11}$

$\Rightarrow \boxed{x \equiv 4 \pmod{11}}$

Sub $x \equiv 4 \pmod{11}$ in eqn ①

$4 + 3y \equiv 3 \pmod{11}$

$\Rightarrow 3y \equiv 3 - 4 \pmod{11}$

$\Rightarrow 3y \equiv -1 \pmod{11}$

$\Rightarrow 3y \equiv (11 - 1) \pmod{11}$

$\Rightarrow 3y \equiv 10 \pmod{11}$

~~$10 \equiv -1 \pmod{11}$~~

$10 \equiv 21 \pmod{11}$

Trans. prop $\Rightarrow 3y \equiv 21 \pmod{11}$

$\Rightarrow \boxed{y \equiv 7 \pmod{11}}$

$\therefore$ Soln is $\boxed{\begin{array}{l} x \equiv 4 \pmod{11} \\ y \equiv 7 \pmod{11} \end{array}}$

(5) Solve $4x + 5y \equiv 5 \pmod 8$

$3x - 6y \equiv 3 \pmod 8$

Soln

Given $4x + 5y \equiv 5 \pmod 8 \longrightarrow (1)$

$3x - 6y \equiv 3 \pmod 8 \longrightarrow (2)$

$(1) \times 6 \Rightarrow 24x + 30y \equiv 30 \pmod 8$

$(2) \times 5 \Rightarrow 15x - 30y \equiv 15 \pmod 8$

(+) $39x \equiv 45 \pmod 8$

$45 \equiv 3 \times 39 \pmod 8$

Trans. prop $\Rightarrow 39x \equiv 3 \times 39 \pmod 8$

$\Rightarrow \frac{39x}{39} \equiv \frac{3 \times 39}{39} \pmod 8$

$\Rightarrow \boxed{x \equiv 3 \pmod 8}$

Sub $x \equiv 3 \pmod 8$ in eqn (1)

$4(3) + 5y \equiv 5 \pmod 8$

$\Rightarrow 5y \equiv 5 - 12 \pmod 8$

$\Rightarrow 5y \equiv -7 \pmod 8$

$\Rightarrow 5y \equiv (8 - 7) \pmod 8$

$\Rightarrow 5y \equiv 1 \pmod 8$

$1 \equiv 25 \pmod 8$

Transitive prop- $\Rightarrow 5y \equiv 25 \pmod 8$

$\Rightarrow \boxed{y \equiv 5 \pmod 8}$

$\therefore$ Soln is $\boxed{\begin{array}{l} x \equiv 3 \pmod 8 \\ y \equiv 5 \pmod 8 \end{array}}$

Chinese Remainder Theorem

Introduction:

"Find a number that leaves the remainder of 1 when divided by 3, a remainder of 2 when divided by 5, a remainder of 3 when divided by 7."

The above question leads to solve the linear system of congruences

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

We must try to find an integer 'x'.

Chinese Mathematician Sun-Tsu proved chinese Remainder theorem which gives solution for the above problem.

$x = 52$ is the soln for above question

$$52 \equiv 1 \pmod 3$$
$$52 \equiv 2 \pmod 5$$
$$52 \equiv 3 \pmod 7$$

We will prove chinese remainder theorem in general.

Chinese Remainder Theorem

Q.2 The linear system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

where $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$, $1 \leq i, j \leq k$.

has a unique solution modulo $(m_1 \times m_2 \times \cdots \times m_k)$

Proof Let $M = m_1 \times m_2 \times \cdots \times m_k$ and

$$M_i = \frac{M}{m_i} \quad \text{where} \quad 1 \leq i \leq k.$$

Since $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$, $\gcd(M_i, m_i) = 1 \quad \forall i$.

$\Rightarrow$ The congruence $M_i y_i \equiv 1 \pmod{m_i}$ has a unique soln → ①

> W.K.T $ax \equiv b \pmod{m}$ has 'd' number of solutions where $d = \gcd(a, m)$

Also $M_i \equiv 0 \pmod{m_j}$ ($\because M_i$ is a multiple of m_j) whenever $i \neq j$ → ②

Let $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k$

Claim ① x is a solution for given system of congruences.

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k$$
$$= \sum_{\substack{i=1 \\ i \neq j}}^{k} a_i M_i y_i + a_j M_j y_j$$
$$\equiv 0 + a_j (1) \pmod{m_j} \quad (\text{using } ①, ②)$$

$\Rightarrow x \equiv a_j \pmod{m_j}$; $1 \le j \le k$.

$\therefore$ x is a soln.

Claim ②: x is unique soln modulo 'm'

Suppose x and x_1 are two solutions of the system

We will prove $x \equiv x_1 \pmod{m}$

$1 \le j \le k$.

Sine $x \equiv a_j \pmod{m_j}$ and $x_1 \equiv a_j \pmod{m_j}$

$\Rightarrow x_1 - x \equiv (a_j - a_j) \pmod{m_j}$

$\Rightarrow x_1 - x \equiv 0 \pmod{m_j}$

$\Rightarrow m_j \mid x_1 - x$ ($\because$ $x_1 - x$ is a multiple of m_j)

$m_j \mid x_1 - x$ for $1 \le j \le k$

$\Rightarrow \text{lcm}(m_1, m_2, \ldots, m_k) \mid x_1 - x$.

But $\text{lcm}(m_1, m_2, \ldots, m_k) = m$. ($\because (m_i, m_j) = 1$)

$\Rightarrow m \mid x_1 - x$.

$\Rightarrow x_1 - x$ is a multiple of m

$\Rightarrow x_1 - x \equiv 0 \pmod{m}$

$\Rightarrow x_1 \equiv x \pmod{m}$

$\Rightarrow x \equiv x_1 \pmod{m}$.

Hence the uniqueness.

Hence the proof.

Procedure for solving Linear system of congruences using Chinese remainder theorem.

Suppose we want to solve $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

Step ①

Let $M = m_1 \times m_2 \times \cdots \times m_k$.

Define $M_i = \frac{M}{m_i}$; $1 \le i \le k$.

Step ②

Solve the congruences

$M_i y_i \equiv 1 \pmod{m_i}$ by guessing.

Solutions are $y_1, y_2, \ldots y_k$.

Step ③

Define $x = \sum_{i=1}^{k} a_i M_i y_i$

Divide x by M

$$M \overline{)\, x \,} \quad (\quad) \qquad \underline{\quad r \quad}$$

Then $x \equiv r \pmod{M}$

r is ~~particular~~ unique soln.

General soln is $x = r + Mt$, $t \in \mathbb{Z}$.

Problems

① Solve $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$ using chinese remainder theorem.

$x \equiv 3 \pmod 7$.

Soln

Step ① $M = m_1 \times m_2 \times m_3$ where $m_1 = 3, m_2 = 5, m_3 = 7$.

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

Define $M_i = \frac{M}{m_i}$ $= \frac{3 \times 5 \times 7}{3}$

$M_1 = \frac{M}{m_1} = \frac{3 \times 5 \times 7}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{3 \times 5 \times 7}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{3 \times 5 \times 7}{7} = 15$

Step ③ Solve the congruences $M_i y_i \equiv 1 \pmod{m_i}$

When $i=1$, $M_1 y_1 \equiv 1 \pmod{m_1}$

$35 y_1 \equiv 1 \pmod 3$

We must choose y_1 so that $3 \mid 35y_1 - 1$.

$\therefore$ By guessing $\boxed{y_1 = 2}$ $(\because 3 \mid 35(2) - 1)$.

When $i=2$, $M_2 y_2 \equiv 1 \pmod{m_2}$

$21 y_2 \equiv 1 \pmod 5$

$\therefore \boxed{y_2 = 1}$ $(\because 5 \mid (21 - 1))$

When $i=3$, $M_3 y_3 \equiv 1 \pmod{m_3}$

$15 y_3 \equiv 1 \pmod 7$

$\therefore \boxed{y_3 = 1}$ $(\because 7 \mid 15 - 1)$

Step ③

$$x = \sum_{i=1}^{3} a_i m_i y_i$$

$a_1 = 1, \quad a_2 = 2, \quad a_3 = 3.$

$m_1 = 35, \quad m_2 = 21, \quad m_3 = 15$

$y_1 = 2, \quad y_2 = 1, \quad y_3 = 1.$

$\therefore x = (1 \times 35 \times 2) + (2 \times 21 \times 1) + (3 \times 15 \times 1)$

$= 70 + 42 + 45$

$= 157$

$x \equiv 52 \pmod{105}$

$$\begin{array}{r|l} & 1 \\ \hline 105 & 157 \\ & 105 \\ \hline \end{array}$$

remainder = 52

$\therefore$ Unique solution is 52 modulo 105.

General solution is $x = 52 + 105t, \quad t \in Z.$

Checking

$x = 52$ in the case $t = 0$.

$52 \equiv 1 \pmod 3$ $\quad (\because 3 \mid (52-1))$

$52 \equiv 2 \pmod 5$ $\quad (\because 5 \mid (52-2))$

$52 \equiv 3 \pmod 7$ $\quad (\because 7 \mid (52-3))$

(2) Using Chinese remainder theorem find the least positive integer such that it leaves the remainder 1 when divided by 3, 2 when divided 4, and 3 when divided by 5.

Soln

It is enough to solve the following system

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 5$$

Step ①

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

$m_1 = 3, \quad m_2 = 4, \quad m_3 = 5$

$$m = m_1 \times m_2 \times m_3$$
$$= 3 \times 4 \times 5$$
$$= 60$$

$$M_1 = \frac{m}{m_1} = \frac{3 \times 4 \times 5}{3} = 20$$

$$m_2 = \frac{m}{m_2} = \frac{3 \times 4 \times 5}{4} = 15$$

$$m_3 = \frac{m}{m_3} = \frac{3 \times 4 \times 5}{5} = 12.$$

Step ②

Solve the congruence

$$M_i y_i = 1 \pmod{m_i},$$

$i = 1, \quad M_1 y_1 \equiv 1 \pmod{m_1}$

$$20 y_1 \equiv 1 \pmod 3$$

$$\boxed{y_1 = 2}$$

$\left(\because \frac{3}{(20 \times 2 - 1)} \text{ or } \frac{3}{39}\right)$

$i=2$, $\quad m_2 y_2 \equiv 1 \pmod{m_2}$

$15 y_2 \equiv 1 \pmod 4$

$\boxed{y_2 = 3}$ $\quad \left(\because \; 4/_{15(3)-1} \text{ or } 4/_{44}\right)$

$i=3$, $\quad m_3 y_3 \equiv 1 \pmod{m_3}$

$12 y_3 \equiv 1 \pmod 5$

$\boxed{y_3 = 3}$ $\quad \left(\because \; 5/_{12(3)-1} \text{ or } 5/_{35}\right)$

Step ③

$$x = a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3$$

$$= 1(20)(2) + 2(15)(3) + 3(12)(3)$$

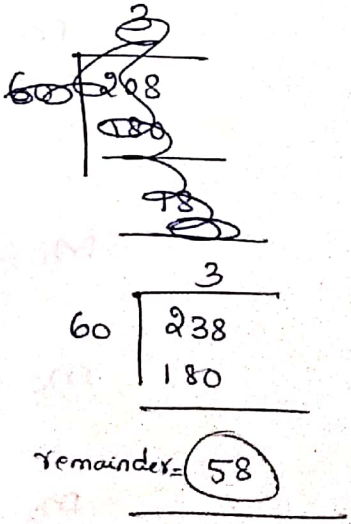
~~$= 40 + 60 + 108 =$~~

~~$= 208$~~

$$= 40 + 90 + 108$$

$$= 238$$

$$x \equiv 58 \pmod{60}$$



$\therefore$ 58 is unique soln modulo 60.

General soln is $x = 58 + 60t$.

Checking

When $t=0$, $\quad x = 58$.

$58 \equiv 1 \pmod 3$ $\quad \left(\because \; 3/_{58-1}\right)$

$58 \equiv 2 \pmod 4$ $\quad \left(\because \; 4/_{58-2}\right)$

$58 \equiv 3 \pmod 5$ $\quad \left(\because \; 5/_{58-3}\right)$

③ Solve the following linear system using chinese remainder theorem.

$$x \equiv 1 \pmod 3$$
$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 7$$
$$x \equiv 7 \pmod{11}$$

Soln

Step ① Given $a_1 = 1,\ a_2 = 3,\ a_3 = 4,\ a_4 = 7.$

$m_1 = 3,\ m_2 = 4,\ m_3 = 7,\ m_4 = 11.$

$$M = m_1 \times m_2 \times m_3 \times m_4$$
$$= 3 \times 4 \times 7 \times 11$$
$$= 924$$

$$M_1 = \frac{M}{m_1} = \frac{924}{3} = 308$$

$$M_2 = \frac{M}{m_2} = \frac{924}{4} = 231$$

$$M_3 = \frac{M}{m_3} = \frac{924}{7} = 132$$

$$M_4 = \frac{M}{m_4} = \frac{924}{11} = 84.$$

Step ② Solve the congruences

$$M_i y_i \equiv 1 \pmod{m_i}$$

$i = 1,\quad M_1 y_1 \equiv 1 \pmod{m_1}$

$$308 y_1 \equiv 1 \pmod 3$$

$$\boxed{y_1 = 2}$$ $\left(\because 3 \mid 308 \times 2 - 1\right.$

$i=2$, $\quad m_2 y_2 \equiv 1 \pmod{m_2}$

$231 y_2 \equiv 1 \pmod{1}$

$\boxed{y_2 = 3}$ $\quad \left(\because \frac{1}{231 \times 3 - 1}\right)$

$i=3$, $\quad m_3 y_3 \equiv 1 \pmod{m_3}$

$132 y_3 \equiv 1 \pmod{7}$

$\boxed{y_3 = 6}$ $\quad \left(\because \frac{7}{(132 \times 6) - 1}\right)$

$i=4$, $\quad m_4 y_4 \equiv 1 \pmod{m_4}$

$84 y_4 \equiv 1 \pmod{11}$

$\boxed{y_4 = 8}$ $\quad \left(\because \frac{11}{(84 \times 8) - 1}\right)$

Step ③

$a_1 = 1$, $a_2 = 3$, $a_3 = 4$, $a_4 = 7$.

$m_1 = 308$, $m_2 = 231$, $m_3 = 132$, $m_4 = 84$

$y_1 = 2$, $y_2 = 3$, $y_3 = 6$, $y_4 = 8$

$$x = a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3 + a_4 m_4 y_4$$

$$= (1 \times 308 \times 2) + (3 \times 231 \times 3) + (4 \times 132 \times 6) + (7 \times 84 \times 8)$$

$$= 616 + 2079 + 3168 + 4704$$

$$= 10567$$

$x \equiv 403 \pmod{924}$.

$$\begin{array}{r|l} & 11 \\ 924 & 10567 \\ & 10164 \\ \hline \text{remainder} = & \boxed{403} \end{array}$$

∴ Unique soln $= 403$ modulo 924.

General soln is $x = 403 + 924t$.

Checking

When $t=0$,

$$x = 403$$

$403 \equiv 1 \pmod 3$ $\quad (\because 3/(403-1) = 402$

$403 \equiv 3 \pmod 4$ $\quad (\because 4/(403-3) = 400$

$403 \equiv 4 \pmod 7$ $\quad (\because 7/(403-4) = 399$

$403 \equiv 7 \pmod{11}$ $\quad (\because 11/(403-7) = 396$