UNIT 5: THEORY OF CONGRUENCE -II

UNIT STRUCTURE

5.1 Learning Objective
5.2 Introduction
5.3 Linear Diphantine Equation : Definition and Examples
5.4 Necessary and Sufficient condition for a Diophantine equation to has a integer solution
5.5 The Chinese Remainder Theorem
5.6 Let Us Sum Up
5.7 Answers to check your progress
5.8 Further Reading
5.9 Model Questions

5.1 LEARNING OBJECTIVE

After studying the current unit reader able to

- Understanding the diefinition of linear diphantine equation.
- Solving equations of the form $ax + by = c$ in integers
- Determining the existence of integer solutions using Greatest Common Divisor (GCD)
- Explore real-world application in member theory.
- Analyze constraints, such as modular arithematic.
- Understanding fundamental principles of Chinese Remainder Theorem
- Solve systems of simultaneous congruences.

5.2 INTRODUCTION

A Diophantine equation is an equation where only integer solutions are sought. It is named after the ancient Greek Mathematician Diphantus of Alexandra, who studied such equations in his works. Among these, linear Diphantine equations are a special category where the equation is linear, meaning all variables appear only to the first power.

A linear Diphantine equation in two variables has the general form

$$ax + by = c$$

where a, b, and c are given integers, x and y are unknown integers that need to be found. The goal is to determine where integer solutions exist and, if so, to find them.

Linear Diphantine equations have application in

(i) Cryptography (e.g. RSA encryption,
(ii) Computer Sciece (e.g. algorithm desing)
(iii) Economics (e.g., resource allocation)
(iv) Number Theory (e.g., modular arithmetic)

The Chinese Remainder Theorem (CRT) is a foundamental theorem in number theory that deals with solving systems of simultaneous congruences with pairwise coprime moduli. It states that if we have a set of congruences with moduli that are relatively prime, then there exists a unique solution moduli the product of those moduli.

The CRT has several practical applications including :

1. **Crypto graphy :** It is used in RSA encryption to speed up modualar exponentiation.
2. **Computer Science :** It helps in parallel computing and distributed systems.
3. **Error Detection :** Used in check sums and error detection method.
4. **Calendrical Calculations :** Helps in determining cycles, such as finding a common year for different repeating events.

The Chinese Remainder Theorem provides a way to solve systems of modular congruences efficiently. It guarantees a unique solution madulo the product of the moduli when they are comprime.

5.3. LINEAR DIOPHANTINE EQUATION : DEFINITION AND EXAMPLES

Definiton 5.3.1 (Linear Diophantine Equation). An equation of the form $ax + by = c$ where a, b, c are given integers and a, b are not both zero, that is to be solved in the integers is called linear Diophantine equation in two unknowns x and y. A solution of this equation is a pair of integers x, y that, when substituted into the equation, satisfy it.

A given linear Diophantine equation can have a number of solutions, as is the case with $3x + 6y=18$, where

$$3.4+6.1=18$$
$$3.(-6)+6.6=18$$
$$3.10+6.(-2)=18$$

By contrast, there is no solution to the equation $2x + 10y =17$. Indeed, the left-hand side is an even integer whatever the choice of x and y, whereas the right-hand side is not.

Similarly, $2x + 3y = 12$ has integer solution $x = 3$ and $y = 12$. But $8x + 17y = 7$ has no integer solution.

5.4. NECESSARY AND SUFFICIENT CONDITION FOR A DIOPHANTINE EQUATION TO HAS A INTEGER SOLUTION :

Theorem 5.4.1. The linear Diophantine equation $ax + by = c$ admits a solution if and only if d/c, where $d = (a, b)$. If x_0, y_0 any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t$$

Where $t \in \mathbb{Z}$

Proof : Let d = (a, b), Then $\exists$ integers r and s with (r, s) = 1 such that a = dr, b = ds.
Suppose is x_0, y_0 is a solution of ax + by = c. Then $c = ax_0 + by_0 = dr\,x_0 + ds\,y_0$

$$= d\,(rx_0 + sy_0)$$

$\Rightarrow d / c$

Therefore, if the equation $ax + by = c$ has a solution, then d/c where $d = (a, b)$.

Conversely, we assume that d/c, where d = (a, b)

$$\Rightarrow c = dt \text{ for some } t \in Z$$

Since d = (a, b) so $\exists\ x_0, y_0 \in Z$ such that $d = ax_0 + by_0$.

Now $c = dt = (ax_0 + by_0)t$

$$= a(x_0 t) + b(y_0 t)$$

Therefore the equation $ax + by = c$ has a particular solution

Second Part : Suppose that a solution x_0, y_0 is known. If x', y' is any other solution,

then

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

$$\Rightarrow a(x' - x_0) = b(y_0 - y') \qquad \text{---------- (1)}$$

We have *d = (a, b)*. So $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ and there exist integers *r* and *s* such that

$\left(\frac{a}{d}, \frac{b}{f}\right) = (r, s) = 1$. Then a = dr and b = ds. Substituting *a = dr* and *b = ds* in (1), we get

$$dr(x' - x_0) = dx(y_0 - y')$$

$$\Rightarrow r(x' - x_0) = s(y_0 - y')$$

$$\Rightarrow r / s(y_0 - y')$$

$$\Rightarrow r / y_0 - y' \qquad [\because (r, s) = 1]$$

$\Rightarrow y_0 - y' = rt$ for some $t \in \mathbb{Z}$

$\Rightarrow y' = y_0 - rt$

(2) $\Rightarrow r(x' - x_0) = srt$

$\Rightarrow x' - x_0 + = st$

$\Rightarrow x' = x_0 + st$

Thus, we get

$x' = x_0 + st$ and $y' = y_0 - rt$ for some $t \in \mathbb{Z}$

$\Rightarrow x' - x_0 + \frac{b}{d}t$ and $y' = y_0 - \frac{a}{d}t$ for some $t \in \mathbb{Z}$

Whatever the values of t (integer) these values of *x'* and *y'* satisfy the Diophantine equation *ax+by=c* because

$$ax' + by' = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$
$$= ax_0 + by_0$$
$$= c$$

Corollary 5.4.2. If (x_0, y_0) is one solution of *ax + by = c, (a, b) = d* and *d/c*, then give the general solution.

Proof : If (x_0, y_0) is one solution of *ax + by =c, (a, b) =d* and *d/c*, then whatever the values of $t \in \mathbb{Z}$, $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$ is the general solution. Therefore, replacing t by –t, we get

$x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$ is the general solution of

Corollary 5.4.3. If (x_0, y_0) is one solution of *ax + by = c, (a, b) =1* then $x = x_0 + bt,\ y = y_0 - at$ give the general solution of the equation *ax + by = c*.

Example 1. Find the general solution of *10x – 8y = 42*.

Solution: The given linear Diophantine equation is

10x – 8y = 42

Here *a = 10, b = -8* and *c = 42*. Therefore

(a, b) = (10, -8) = 2 and *2|42*.

Thus, the given equation has integer solution.

$x_0 = 1,\ y_0 = -4$ is a particular solution of it. Hence general solution is given by

$$x = x_0 + \frac{(-8)}{2}t \text{ and } y = y_0 - \frac{10}{2}t,\ \ t \in Z$$

Or $x = 1 - 4t$ and $y = -4 - 5t,\ \ t \in Z$

Example 2. Find the general solution of $170x - 455y = 625$.

Solution: The given linear Diophantine equation is

$$170x - 455y = 625$$

First, we have to finde ged *(170, 455)*

∴ Ged *(170, 455) = 5* and *5 | 625*.

Thus $170x - 455y = 625$ has integer solutions.

We observe that $x_0 = 1$ and $y_0 = -1$ is a particular solution of the given equation.

Therefore, its general solution is given by

$x = x_0 + \left(\frac{-455}{5}\right)t$ and $y = y_0 - \frac{170}{5}t$ where $t \in \mathbb{Z}$

or $x = 1 - 91t$ and $y = -1 - 34t$ where $t \in \mathbb{Z}$

Example 3. Find the positive integer solutions of the linear Diophantine equation *172x + 20y=1000*.

Solution: First we find the ged (172, 20) by applying the Euclidean's Algorithm,

172 = 8 × 20 + 12

20 = 1 × 12 + 8

12 = 1 × 8 + 4 or

∴ ged (172, 20) = 4 and 4|1000. Thus the given equation has integer solutions. Now we expressed 4 as a linear combination of 172 and 20 as follows :

4 = 12 – 8

= 12 – (20 – 12)

= 2.12 – 20

= 2.(172 – 8.20) – 20

= 2.172 + (–17).20

∴ 1000 = 250 × 4

= 250 × [2.172 + (–17).20]

= 500.172 + (– 4250).20

⇒ 172.500 + 20. (– 4250) = 1000

Thus x = 500 and y = – 4250 is a particular solution. The general solution is given by

$$x = 500 + \frac{20}{4}t \text{ and } y = -4250 - \left(\frac{172}{4}\right)t,\ t \in Z$$

Or $x = 500 + 5t$ and $y = -4250 - 43t,\ t \in Z$

Now, we find positive integer solutions. Consider

$500 + 5t > 0$ and $-4250 - 43t > 0$

$\Rightarrow 5t > -500$ and $-4250 > 43t$

$\Rightarrow t > -100$ and $\frac{-4250}{43} > t$

$\Rightarrow -100 < t < -98\frac{36}{43}$

Since t is an integer, so t = – 99. Thus the given linear Diophantine equation has a unique positive solution x = 500 + 5 × (– 99), y = – 4250 – 43 × (– 99)

Or x = 5, y = 7 corresponding to the value t = – 99.

Theorem 5.4.4. If *ax + by = c, (a, b) = 1* ---------- (1)

and b is numerically smaller of the two coefficients a and b and a_1 and c_1 are the minimal remainders of a and c respecting with to |b|, then (1) can be written in the form

$$a_1x + |b|y_1 = c_1$$

Where $|a_1| \le \frac{|b|}{2}$ and $|c_1| \le \frac{|b|}{2}$

Proof : Since a_1 and c_1 are the minimal remainders of a and c respecting with to |b|, therefore

$a = |b|Q_1 + a_1$ Where $0 < |a_1| \le \frac{|b|}{2}$

$c = |b|Q_2 + c_1$ Where $0 < |c_1| \le \frac{|b|}{2}$

Then (1) becomes

$$(|b|Q_1 + a_1)x + by = |b|Q_2 + c_1$$

$$\Rightarrow a_1x + |b|\left(Q_1x + \frac{b}{|b|}y - Q_2\right) = c_1$$

Putting $Q_1x + \frac{b}{|b|}y - Q_1 = y_1$, we obtain

$$a_1x + |b|y_1 = c_1$$

Example. 4 Find the general solution of

$$21x + 13y = 1791$$

Solution : We have

$$21x + 13y = 1791$$

And coefficient 13 is smaller numerically, so

$21 = 2 \times 13 - 5$

$1791 = 138 \times 13 - 3$

Then (1) becomes,

$(2 \times 13 - 5)\, x + 13y = 138 \times 13 - 3$

$\Rightarrow -5x + 13\,(2x + y - 138) = -3$

$\Rightarrow -5x + 13y_1 = -3$ ..... (2)

Where $y_1 = 2x + y - 138$

Since (2) satisfied by $x = 11$, $y_1 = 4$, so we have

$-5x + 13y_1 = -3$, $x = 11$, $y_1 = 4$

$13 = 3 \times 5 - 2$

$3 = 1 \times 5 - 2$

Then (2) becomes

$-5x + (3 \times 5 - 2)\, y_1 = -(1 \times 5 - 2)$

$\Rightarrow 5\,(x - 3y_1 - 1) - 2y_1 = 2$

$\Rightarrow -5x_1 + 2y_1 = -2$ ..... (4)

Where $x_1 = x\ 3y_1 - 1$ ..... (5)

Now equation (4) is satisfied by $x_1 = 0$, $y_1 = -1$.

Here 2 is numerically smaller coefficient and $2 \mid -2$, so putting $x_1 = 0$, $y_1 = -1$ in (5) we get

$0 = x - 3.(-1) - 1$

$\Rightarrow x = -2$

From (3), $-1 = 2.(2) + y - 138$

$\Rightarrow y = |4|$

Hence general solution of the given equation is given by

$x = -2 + 13t$

$y = |4| - 21t$, where $t \in \mathbb{Z}$

Example 5. Find the general solution of

$311\,x - 112y = 73$ ..... (1)

Here $(112, 311) = 1$ and $1/73$. Therefore the equation (1) has integer solutions. Here 112 is numerically small coefficient.

So we write $311 = 112 \times 3 - 25$

$73 = 112 \times 1 - 39$

Therefore (1) becomes

$(112 \times 3 - 25)\, x - 112y = 112y \mid -39$

$\Rightarrow -25x + 112\,(3x - y - 1) = -39$

$\Rightarrow -25x + 112y_1 = -39$ ..... (2)

Where $y_1 = 3x - y - 1$ ..... (3)

Now (2) satisfied by $x = 14$, $y_1 = 3$

In equation (2), neither of the two coefficients is unity. Therefore equation (2) can be treated in the same way as

(1). Here 25 is memerically small coefficient. Therefore, we write

$112 = 25 \times 4 + 12$

$39 = 25 \times 2 - 11$

Herefore equation (20 becomes

$-25x + (25 \times 4 + 12)\, y_1 = -(25 \times 2 - 11)$

$\Rightarrow +25(-x + 4y_1 + 2) + 12y_1 = +11$

$\Rightarrow +25x_1 + 12y_1 = +11$ .....(4)

Where $x_1 = -x + 4y_1 + 2$ .....(5)

Now (4) is satisfied by $x_1 = -1$, $y_1 = 3$.

In equation (4), neither of two coefficient is unity.

Therefore, we again treat equation (4) in the same manner as 1. Here 12 is numerically small coefficient. Therefore

$25 = 12 \times 2 + 1$

$11 = 12 \times 1 - 1$

Equation (4) becomes,

$(12 \times 2 + 1)x1 + 12y_1 = (12 \times 1 - 1)$

$\Rightarrow 12(2x_1 + y_1 - 1) + x_1 = -1$

$\Rightarrow 12y_2 + 12y_2 = -1$

$\Rightarrow X_1 + 12y_2 = -1$ ..... (6)

Where $y_2 = 2x_1 + y_1 - 1$

In equation (6), one coefficient is unity. Now putting y2 = 0, we get x1 = –1

From (5), $-1 = -x + 4.3 + 2 \Rightarrow x = 15$

From (3), $3 = 3.15 - y - 1 \Rightarrow y = 41$

Thus x = 15, y = 41 is a particular solution. Hence general solution is given by

$$x = 15 + \left(\frac{-112}{1}\right)t,\ y - 4 \mid -\frac{311}{1}t,\ t \in Z$$

Or $x = 15 - 11t,\ y = 4 \mid -31 \mid t,\ t \in Z$

Example 6. A customer bought a dozen pieces of fruit, apples and oranges, for Rs 132. If an apple costs Rs 3 more than a orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Solution : Let x be the number of apples and y be the number of oranges purchased, in addition, let z represent the cost (in rupees) of an orange. Then

$(z + 3)x + zy = 132$

$\Rightarrow 3x + (x + y)z = 132$ ..... (1)

We have x + y = 12. So equation (1) becomes

$3x + 12z = 132$

$\Rightarrow x + 4z = 44$ ..... (2)

Here ged(1, 4) = 1 and 1/44. Therefore equation (2) has integer solutions. Upon multiplying the relation $1 = 1 \times (-3) + 4 \times 1$ by 44 to get

$1 \times (-132) + 4 \times 44 = 44$

It follows that $x_0 = -132$, $z_0 = 4^4$ is a particular solution.

All other solutions of equation (2) are given by

$X = -132 + 4t$, $z = 44 - t$, where $t \in \mathbb{Z}$

Since the customer bought more apple than oranges, so

$6 < x \leq 12$

$\Rightarrow 6 < -132 + 4t \leq 12$

$\Rightarrow 132 + 6 < 132 - 132 + 4t \leq 132 + 12$

$\Rightarrow 138 < 4t \leq 144$

$$\Rightarrow \frac{138}{4} < t \le \frac{144}{4}$$

$$\Rightarrow 34\frac{1}{2} < t \le 36$$

$\therefore t = 35$ and 36

For t = 35, x = – 132 + 4 × 35 = 140 – 132 = 8, z = 9

For t = 36, x = – 132 + 4 × 36 = 144 – 132 = 12, z = 8

Thus, there are two possibilities of purchases :

(i) 8 apples at Rs 12 each and 4 oranges at Rs 9 each (the case where t = 35)

Or (ii) a dozen apples costing Rs 11 a piece (the case where t = 36)

W CHECK YOUR PROGRESS

Q.1. Determine all solution in the integers of the following Diophantine equations :

(a) 56x + 72y = 40

(b) 24x + 138y = 18

Q.2. Find the positive integer solutions of the linear Diophantine equation : 18x + 5y = 48

Q.3. Find the general solution of the linear Diophantine eqution : 11x + 5y = 79.

5.5 THE CHINESE REMAINDER THEOREM

Statement : Let $n_1, n_2, n_3, ...n_r$ be positive integers such that $(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$x \equiv a_3 \pmod{n_3}$

.....

.....

$x \equiv a_r \pmod{n_r}$

has a simultaneous solution which is unique medulo to the integer $n_1.n_2.n_3....n_r$.

Proof : Let $n = n_1.n_2.n_3.....n_r$

For each k = 1, 2, 3,..... r, let

$$N_k = \frac{n}{n_k} = n_1.n_2.....n_{k-1}.n_{k+1}.....n_r$$

By hypothesis, the n_i's are relative prime in pairs, so

$(N_k, n_k) = 1$

We consider the congruences

$n_k.x \equiv 1 \pmod{n_k}$ for k = 1, 2, 3, ..., r

Since $(N_k, n_k) = 1$, so each congruence has using solution. Let x_k be the unique solution of the congruence $N_k.x \equiv 1 \pmod{n_k}$ for k = 1, 2, ..., r.

Clain that the integer

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + ... + a_rN_r\,x_r$ is a simultaneous solution of the given system of congruences.

Firstly, we observe that $N_i \equiv 0 (\text{mod } n_k)$ for $i \neq k$

$\Rightarrow n_k \mid N_i$ for $i \neq k$

Thus $\overline{x} \equiv a_1N_1x_1 + a_2N_2x_2 + ... + a_kN_kx_k + ... + a_rN_rx_r$

$\equiv a_kN_kx_k \pmod{n_k}$

But the integer x_k satisfies the congruence $N_k.x \equiv | (\text{mod } n_k)$ so $N_k.x_k \equiv 1 (\text{mod } n_k)$ and hence

$$\overline{x} \equiv a_k \pmod{n_k}$$

This shows that a solution to the given system of congruences exists.

Uniqueness : Suppose x' is any other integer that satisfies these congruences. Then

$\overline{x} \equiv a_k \equiv x' (\text{mod } n_k)$

$\Rightarrow n_k \mid \overline{x} - x'$ for all k = 1, 2, ..., r

$\Rightarrow n_1.n_2.n_3.....n_r \mid \overline{x} - x'$

$\Rightarrow n \mid \overline{x} - x'$

$\Rightarrow \overline{x} \equiv x'$ (modn)

So the solution is unique.

Example 1. Solve the following system of linear congruences using Chinee Remainder Theorem :

$x \equiv 1 \ (mod\ 2)$

$x \equiv 2 \ (mod\ 3)$

$x \equiv 3 \ (mod\ 5)$

$x \equiv 5 \ (mod\ 7)$

Solution : Here $a_1 = 1,\ a_2 = 2,\ a_3 = 3,\ a_4 = 5$

$n_1 = 2,\ n_2 = 3,\ n_3 = 5,\ n_4 = 7$

Clearly $(n_i, n_j) = 1$ for $i \neq k$

Let $n = n_1.\ n_2.\ n_3.\ n_4 = 2.\ 3.\ 5.\ 7 = 210$ and

$$N_1 = \frac{n}{n_1} = \frac{210}{2} = 105$$

$$N_2 = \frac{n}{n_2} = \frac{210}{3} = 70$$

$$N_3 = \frac{n}{n_3} = \frac{210}{5} = 42$$

$$N_4 = \frac{n}{n_4} = \frac{210}{7} = 30$$

Now the linear congruences

Are satisfied by $x_1 = 1,\ x_2 = 1,\ x_3 = 3,\ x_4 = 4$.

Thus a solution of the system is given by

$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4$

$= 1.105.1 + 2.70.1 + 3.42.3 + 5.30.4$

$\equiv 1223 \pmod{210}$

We get the unique solution

$x \equiv 173 \pmod{210}$

Example 2. Find the least natural number which when divided by 7, 10, 11 leaves remainder 1, 6, 2 respectively.

Solution : Let x be the required least natural number. Then

$x \equiv 1 \pmod 7$

$x \equiv 6 \pmod{10}$

$x \equiv 2 \pmod{11}$

Here $a_1 = 1,\ a_2 = 6, a_3 = 2$

$n_1 = 7,\ n_2 = 10,\ n_3 = 11$

Therefore $n = n_1. n_2. n_3 = 7.10.11 \equiv 770$

And $N_1 = \frac{n}{n_1} = \frac{770}{7} = 110$

$N_2 = \frac{n}{n_2} = \frac{770}{10} = 77$

$N_3 = \frac{n}{n_3} = \frac{770}{11} = 70$

How the linear congruences

$110x_1 \equiv 1 \pmod 7$

$77x_2 \equiv 1 \pmod{10}$

$70x_3 \equiv 1 \pmod{11}$

are satisfied by $x_1 = 3,\ x_2 = 3,\ x_3 = 3$.

The required unique solution of the system is given by

$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$= 1.110.3 + 6.77.3 + 2.70.3$

$\equiv 2136 \pmod{770}$

$\equiv 596 \pmod{770}$

Hence the required least natural number is 596.

Example 3. Solve the following system of linear congruences, if exists,

$x \equiv 6 \pmod{17}$

$x \equiv 17 \pmod{24}$

$x \equiv 13 \pmod{33}$

Solution : Here 24 and 33 are not relatively prime.

We have $x \equiv 17 \pmod{24}$

$\Rightarrow 24 \mid x - 17$

$\Rightarrow 3 \mid x - 17,\ 8 \mid x - 17$

$\Rightarrow 3 \mid x - 17,\ 2 \mid x - 17$

$\Rightarrow x \equiv 17 \pmod 3,\ x \equiv 17 \pmod 2$

$\Rightarrow x \equiv 2 \pmod 3, x \equiv 1 \pmod 2$

And $x \equiv 13 \pmod{33}$

$\Rightarrow 33 \mid x - 13$

$\Rightarrow 3 \mid x - 13,\ 11 \mid x - 13$

$\Rightarrow x \equiv 13 \pmod 3$, $x \equiv 13 \pmod{11}$

$\Rightarrow x \equiv 1 \pmod 3$, $x \equiv 2 \pmod{11}$

Now the linear congruences

$$110x_1 \equiv 1 \pmod 7$$
$$77x_2 \equiv 1 \pmod{10}$$
$$70x_3 \equiv 1 \pmod{11}$$

are satisfied by $x_1 = 3$, $x_2 = 3$, $x_3 = 3$.

The required unique solution of the system is given by

$x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

$= 1.110.3 + 6.77.3 + 2.70.3$

$= 2136 \pmod{770}$

$= 596 \pmod{770}$

Hence the required least natural number is 596.

Example 3. Solve the following system of linear congruences, if exists

$$x \equiv 6 \pmod{17}$$
$$x \equiv 17 \pmod{24}$$
$$x \equiv 13 \pmod{33}$$

Solution : Here 24 and 33 are not relatively prime.

We have $x \equiv 17 \pmod{24}$

$24 \mid x - 17$

$3 \mid x - 17$, $8 \mid x - 17$

$3 \mid x - 17$, $2 \mid x - 17$

$x \equiv 17 \pmod 3$, $x \equiv 17 \pmod 2$

$x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 2$

and $x \equiv 13 \pmod{33}$

$\Rightarrow 33 \mid x - 13$

$\Rightarrow 3 \mid x - 13$, $11 \mid x - 13$

$\Rightarrow x \equiv 13 \pmod 3$, $x \equiv 13 \pmod 1$

$\Rightarrow x \equiv 1 \pmod 3$, $x \equiv 2 \pmod{11}$

We are left with

$$x \equiv 6 \pmod{17}$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 2$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod{11}$$

Since $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod 3$ are not possible at a same time.

Therefore the given system of congruences has no solution.

W CHECK YOUR PROGRESS

Q.4. Solve each of the following sets of simultaneous congruences using Chinese Remainder Theorem.

(a) $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

(b) $x \equiv 5 \pmod{18}$
$x \equiv -1 \pmod{24}$
$x \equiv 17 \pmod{33}$

(c) $x \equiv 3 \pmod{11}$
$x \equiv 5 \pmod{19}$
$x \equiv 10 \pmod{29}$

25.6. LET US SUM UP

- Linear Diophantine Equation : An equation of the form ax + by = c, where a, b, c are given integer and a, b are not both zero, that is to be solved in the integers is called linear Diophantine equation in two unknowns x and y.
- The linear Diophantine equation ax + by = c admits a solution if and only if d|c, where d = (a, b). If x_0, y_0 any particular solution of this equation, then all the solutions are given by
$$x = x_0 + \left(\frac{b}{d}\right)t,\ y = y_0 - \left(\frac{a}{d}\right)t \text{ where } t \in Z$$
- If (x_0, y_0) is one solution of ax + by = c, (a, b) = 1, then $x = x_0 + bt$, $y = y_0 - at$, $t \in Z$ give the general solution of the equation ax + by = c.
- If ax + by = c, (a, b) = 1 and b is numerically smaller of the two coefficients a and b and a_1 and c_1 are the minimal remainders of a and c respectively with respect to |b|, then the equation can be written in the form $a_1x + |b|\ y_1 = c_1$
Where $|a_1| \le \frac{|b|}{2}$ and $|c_1| \le \frac{|b|}{2}$
- The Chinese Remainder Theorem : Let n_1, n_2, ..., n_r be positive integers such that (n_i, n_j) = 1 for $i \neq k$
Then the system of linear congruences
$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
.....
.....
$x \equiv a_r \pmod{n_r}$
has a simultaneous unique solution
$$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + ... + a_rN_rx_r \pmod n$$
Where $n = n_1.n_2.n_3.....n_r;\ N_k = \frac{n}{n_k}$ for k = 1, 2, ...r and x_k are solutions of $N_kx \equiv 1 \pmod{n_k}$ for all k = 1, 2, 3,...., r

K 5.7. ANSWERS TO CHECK YOUR PROGRESS

Ans to Q.1.

(a) The given linear Diophantine equation is

$$56x + 72y = 40$$

First we find ged (56, 72) by Euchlildean division algorithm,

$$56\overline{)72}\ 1$$
$$56$$
$$16\overline{)56}\ 3$$
$$48$$
$$8\overline{)16}\ 2$$
$$16$$

Or

$72 = 56 \times 1 + 16$

$56 = 16 \times 3 + 8$

$16 = 8 \times 2 + 0$

Therefore ged (56, 72) = 8. Since 8|40, therefore given equation has integer solutions. We have

$$\begin{aligned} 8 &= 56 - 16 \times 3 \\ &= 56 - (72 - 56 \times 1) \times 3 \\ &= 56 - 72 \times 3 + 56 \times 3 \\ &= 56 \times 4 - 72 \times 3 \end{aligned}$$

$\therefore 40 = 56 \times 20 + 72 \times (-15)$ [multiplying both sides by 5]

Thus (20, – 15) is a particular solution and other solutions are given by

$$x = 20 + \frac{72}{8}t,\ y = -15 - 7t,\ \text{Where } t \in Z$$

Or $x = 20 + 9t$, $y = -15 - 7t$, where $t \in Z$

(b) Left as an exercise

Ans. to Q.2. The given linear Diophantine equation is

$$18x + 5y = 48$$

Clearly ged (18, 5) = 1. Since 1|48, so the given equation has integer solutions. Since $x_0 = 1$, $y_0 = 6$ is a particular solution, therefore other solutions are given by $x = 1 + 5t$, $y = 6 - 18t$, where $t \in Z$

If $x, y > 0$, then $1 + 5t > 0$, $6 - 18t > 0$

$$\Rightarrow 5t > -1,\ 6 - 18t$$

$\Rightarrow t > -\frac{1}{5}, \quad \frac{6}{18} > t$

$\Rightarrow -\frac{1}{5} < t < \frac{1}{3}$

Since $t \in \mathbb{Z}$ therefore t = 0. Hence the required positive solution is x = 0, y = 6.

Ans to Q 3. The given linear Diphoantine equation is

$$11x + 5y = 79$$

Here (11, 5) = 1. Since 1|79, therefore give equation has integer solution.

Since $x_0 = -1$ and $y_0 = 18$ is a particular solution, therefore general equation is given by

$X = -1 + 5t, \; y = 18 - 11t, \;$ where $t \in Z$.

Ans to Q 4.

(a) The given system of linear congruences

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Here $a_1 = 2, \; a_2 = 3, \; a_3 = 2$

$n_1 = 3, \; n_2 = 5, \; n_3 = 7$

Clearly n_i's are pair wise coprime. We have $n = n_1 . n_2 . n_3 = 3.5.7 = 105$ and

$$N_1 = \frac{n}{n_1} = \frac{105}{3} = 35, \; N_2 = \frac{n}{n_2} = \frac{105}{5} = 21, \; N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$$

Now the linear congruences

$35x_1 \equiv 1 \pmod 3, \; 21x_2 \equiv 1 \pmod 5, \; 15x_3 \equiv 1 \pmod 7$

Are satisfied by $x_1 = 2, \; x_2 = 1, \; x_3 = 1$ respectively.

Thus a solution of the system is given by

$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$

$= 2.35.2 + 3.21.1 + 2.15.1$

$= 233$

$\equiv 23 \pmod{105}$

(b) The given system of linear congruences

$x \equiv 5 \pmod{18}$

$x \equiv -1 \pmod{24}$

$x \equiv 17 \pmod{33}$

Here n_i's are not relatively prime in pairwise.

We have $x \equiv 5 \pmod{18}$

$\Rightarrow x \equiv 5 \pmod 2$ and $x \equiv 5 \pmod 9$

$\Rightarrow x \equiv 1 \pmod 2$ and $x \equiv 5 \pmod 9$

Similarly, $x \equiv -1 \pmod{24}$ is equivalent to

$x \equiv -1 \pmod 3$ and $x \equiv -1 \pmod 8$

and $x \equiv 17 \pmod{33}$ is equivalent to

$x \equiv -17 \pmod 3$ and $x \equiv 17 \pmod{11}$

$\Rightarrow x \equiv 2 \pmod 3$ and $x \equiv 6 \pmod{11}$

Therefore the given system equivalent to

$x \equiv 1 \pmod 2$ ..... (1)

$x \equiv 5 \pmod 9$ ..... (2)

$x \equiv -1 \pmod 3$ ..... (3)
$x \equiv -1 \pmod 8$ ..... (4)
$x \equiv 2 \pmod 3$ ..... (5)
$x \equiv 6 \pmod{11}$ ..... (6)

Now $x \equiv 5 \pmod 9 \Rightarrow 9 \mid x - 5$
$\Rightarrow x - 5 = 9k$ for some $k \in \mathbb{Z}$
$\Rightarrow x = 5 + 9k$
$\Rightarrow x = 2 + 3 + 9k$
$\Rightarrow x \equiv 2 \pmod 3$

which is same as (5).

Again $x \equiv -1 \pmod 8$
$\Rightarrow 8 \mid x + 1$
$\Rightarrow x + 1 = 8l$ for some integer l.
$\Rightarrow x = 8l - 2 + 1$
$\Rightarrow x \equiv 1 \pmod 2$

Which is same as (L). Therefore, we are now left with

$x \equiv 5 \pmod 9$
$x \equiv -1 \pmod 8$
$x \equiv 6 \pmod{11}$

Clearly n_i's are pairwise coprime.

Here $a_1 = 5$, $a_2 = -1$, $a_3 = 6$
$n_1 = 9$, $n_2 = 8$, $n_3 = 11$

We have $n = n_1 . n_2 . n_3 = 9.8.11 = 792$

and $N_1 = \frac{792}{9} = 88,\ N_2 = \frac{792}{8} = 99,\ N_3 = \frac{792}{11} = 72$

Now the linear congruences

$88x_1 \equiv 1 \pmod 9$, $99x_2 \equiv 1 \pmod 8$, $72x_3 \equiv 1 \pmod{11}$ are satisfied by

$x_1 = 4,\ x_2 = 3,\ x_3 = 2$

Thus a solution of the system is given by

$X = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$
$= 5.88.4 + (-1).99.3 + 6.72.2$
$= 2327$
$\equiv 743 \pmod{792}$

(c) Left as an exercise.

O 5.8. FURTHER READING

1. David M. Buston, Elementary Number Theory (7th Edn.). Nc Graw Hill Education (India) Private Limited Chennai – 600116, 2018

2. S.B. Malik, Basic Number Theory (2nd Edn.), Vikash Publishing House Private Limited, Noida – 201301, 2017.
3. H. Kishan, Number Theory, Krishna Prakashan Media (P) Limited, Meerut – 250001 (UP), India, 2017.
4. G.H. Hardy and E.M. Wright, Theory of Numbers, Oxford Science Publication, 2003.

M 5.9 MODEL QUESTIONS

1. Determine all solutions in the integers of the following Diophanetine equations :

(a) $39x - 56y = 11$
(b) $221x + 35y = 11$
(c) $6x + 51y = 22$
(d) $33x + 14y = 115$

2. Determine all solutions in the positive integers of the following Diophantine equations :

(a) $5x + 14y = 620$
(b) $54x + 21y = 906$
(c) $123x + 360y = 99$

3. If a and b are relatively prime positive integers, prove that the Diophantine equation $ax - by = 0$ has infinitely many solutions in the positive integers.

4. If a cock is worth Rs 500, a her Rs 300 and three chicks together Rs 100, how many cocks, hens and chicks, totalling 100, can be bought for Rs 1000?

5. The neighbourhood theatre charges Rs 180 for adult admissions and Rs 75 for child. On a particular evening the total receipts were Rs 9000. Assuming that more adults than children were present, how many people attended.

6. Solve the systems of Linear congruences by using Chinese Remainder Theorem :

(a) $x \equiv 5 \pmod 6$
$x \equiv 4 \pmod{11}$
$x \equiv 3 \pmod{17}$

(b) $x \equiv 3 \pmod{11}$
$x \equiv 5 \pmod{19}$
$x \equiv 10 \pmod{29}$

(c) $x \equiv 5 \pmod{11}$

$x \equiv 14 \pmod{19}$
$x \equiv 15 \pmod{31}$

(d) $2x \equiv 1 \pmod{5}$
$3x \equiv 9 \pmod{6}$
$4x \equiv 1 \pmod{7}$
$5x \equiv 9 \pmod{11}$

7. Find an integer having the remainder 3, 11, 15 when divided by 10, 13, 17 respectively.

*** *** ***