Linear Diophantine Equation : An equation in one or more unknowns which is to be solved in integers is said to be a Diophantine equation (named after the Greek Mathematician Diophantus).

The equation $ax+by=c$, where a, b, c are integers, a and b both not zero, is said to be a linear Diophantine equation in two unknowns x and y.

This type of equation may have many solutions in integers or may not have even a single solution.

For example, $2x+4y=6$ has many solutions in integers, since, $2.1+4.1=6$, $2.5+4(-1)=6$, $2.9+4(-3)=6, \cdots$, whereas, the equation $2x+4y=3$ can not have a solution in integers as the left hand side is always even and the right hand side is odd.

[A solution of the Diophantine equation $ax+by=c$ is a pair (x_0, y_0) of integers such that $ax_0+by_0=c$, we call (x_0, y_0) an integral solution of the equation $ax+by=c$]

Theorem 14 : Let a, b, c be integers with a and b both not zero. Then the equation $ax+by=c$ has an integral solution if and only if d divides c where $\gcd(a,b)=d$. Furthermore, if (x_0, y_0) is a particular integral solution of this equation, then all integral solutions of this equation are given by

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n$$ where n is any integer.

Proof: Suppose $ax+by=c$ has an integral solution (x_0, y_0). Then $ax_0+by_0=c$. Let $d=\gcd(a,b)$. Then d divides a and b. Hence d divides ax_0+by_0. This implies d divides c.

Conversely, let d divides c. Then $c=dk$ for some integer k.

Since $d = \gcd(a,b)$, there exist integers r and t such that $ar + bt = d$. Hence $ark + btk = dk$

or, $a(rk) + b(tk) = c$

Let $x_0 = rk$ and $y_0 = rk$. Hence (x_0, y_0) is an integral solution of $ax + by = c$. Suppose (x', y') is an integral solution of $ax + by = c$. Then $ax' + by' = ax_0 + by_0$ and so

$$\frac{a}{d}x' + \frac{b}{d}y' = \frac{a}{d}x_0 + \frac{b}{d}y_0$$

So, $$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y') \quad \cdots (1)$$

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

Then from (1) it follows that a/d divides $y_0 - y'$ and $\frac{b}{d}$ divides $x' - x_0$. Hence $$\frac{x' - x_0}{b/d} = \frac{y_0 - y'}{a/d} = n \text{ (say)}$$

So, ~~for each integral solution~~ $\left(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n\right)$ is an integral solution of the given equation for any integer n as $a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) = ax_0 + by_0 = c$

Hence if (x_0, y_0) is an integral solution of the given equation, Then all integral solution are given by

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n$$ where n is any integer.

Worked out problems: 1. Find all the solutions of the linear Diophantine equation $3x + 2y = 6$

Solution: Here $\gcd(3,2) = 1$ and 1 divides 6. Hence $3x + 2y = 6$ has integral solution. Now $1 = 3.1 + 2(-1)$

Hence $3.6 + 2(-6) = 6$

So, $(x_0, y_0) = (6, -6)$ is an integral solution of the given equation. Hence all integral solutions of the given

equation are given by

$x = 6 + \frac{2}{1}n$ and $y = -6 - \frac{3}{1}n$, for any integer n. i.e., $x = 6 + 2n$ and $y = -6 - 3n$ for any integer n.

2. For each of the following linear Diophantine equation, either find all integral solutions or show there are no integral solution.

(a) $18x + 12y = 2$ (b) $8x - 10y = 42$

Solution: (a) $\gcd(18, 12) = 6$. Since 6 does not divide 2, it follows that the given equation has no integral solution.

(b) $\gcd(8, -10) = 2$ and 2 divides 42. Hence the given equation has integral solutions.

Now $-10 = (-2)8 + 6$

$8 = 1.6 + 2$

$6 = 2.3$

Then $2 = 8 - 1.6 = 8 - [-10 - (-2)8]$

$= 8 - 2.8 + (-1)(-10)$

$= (-1)8 + (-1)(-10)$

So, $8(-21) + (-10)(-21) = 42$

Hence $(-21, -21)$ is an integral solution $8x - 10y = 42$

So, all integral solutions of the given equation are given by

$x = -21 + \frac{-10}{2}n$ and $y = -21 - \frac{8}{2}n$

i.e., $x = -21 - 5n$ and $y = -21 - 4n$ for all integers n.

3. Find all positive ~~integers~~ integral solutions of $5x + 7y = 100$

Solution: $\gcd(5, 7) = 1$ and 1 divides 100. Hence $5x + 7y = 100$ has integral solution. Now $7 = 5.1 + 2$

$5 = 2.2 + 1$

Then $1 = 5 - 2.2 = 5 - 2(7 - 5.1) = 5.3 + 7(-2)$

Hence $5 \cdot 300 + 7(-200) = 100$

Then, one integral solution of the given equation is

$$x_0 = 300 \ , \ y_0 = -200$$

Hence all integral solutions of the given equation are given by

$$x = 300 + 7n \quad \text{and} \quad y = -200 - 5n \quad \text{for all integer } n.$$

If the solutions are positive, then

$$300 + 7n > 0 \quad \text{and} \quad -200 - 5n > 0$$

So the integer n must satisfy

$$-\frac{300}{7} < n < -40$$

So, $n = -42, \ n = -41$

Hence the equation $5x + 7y = 100$ has exactly two positive integral solutions and these are

$$x = 300 + 7(-42) = 6, \ y = -200 - 5(-42) = 10$$

and $x = 300 + 7(-41) = 13, \ y = -200 - 5(-41) = 5$

4. A man pays Rs 145 for some cups and glasses. If If a cup costs Rs. 17 and a glass costs Rs. 15, how many of each did he buy?

Solution : Suppose he bought x cups and y glasses

Then $17x + 15y = 145 \quad \ldots (1)$

Now $\gcd(17, 15) = 1$

$$17 = 1 \cdot 15 + 2$$

$$15 = 7 \cdot 2 + 1$$

Hence $1 = 15 - 7 \cdot 2 = 15 - 7(17 - 15) = 8 \cdot 15 + (-7)17$

Then $17(-1015) + 15(1160)$

This implies $x_0 = -1015$, $y_0 = 1160$ is an integral solution of (1).

Hence all integral solutions of (1) are

$$x = -1015 + 15n$$
$$y = 1160 - 17n \quad \text{for any integer } n.$$

Since $x > 0$, $y > 0$ we find that

$$-1015 + 15n > 0 \quad \text{and} \quad 1160 - 17n > 0$$

Hence $$\frac{203}{3} < n < \frac{1160}{17} \quad \text{i.e.,} \quad 67\frac{2}{3} < n < 68\frac{14}{17}$$

So, $n = 68$. Hence

$$x = -1015 + 15 \cdot 68 = -1015 + 1020 = 5$$

and $$y = 1160 - 17 \cdot 68 = 1160 - 1156 = 4$$

Hence the number of cups is 5 and the number of glasses is 4.

Exercises: 1. Which of the following Linear Diophantine equations can not be solved? (a) $6x + 4y = 91$ (b) $621x + 736y = 46$
(c) $158x - 57y = 7$

2. Solve the following linear Diophantine equations:

(a) $5x + 18y = 48$ (b) $3x + 4y = 9$

(c) $7x - 5y = 100$ (d) $25x + 65y = 50$

3. Find all positive integral solutions, if there be any,

(a) $61x + 56y = 7643$ (b) $2x + 3y = 50$

(c) $120x + 41y = 11$ (d) $5x + 7y = 100$

4. A retailer wants to order pens and pencils for Rs. 302. If a pen costs Rs. 18 and a pencil Rs. 7, find in how many ways he can place his order.

Congruences

Definition: If a and b are integers and m is a positive integer, we say that a is congruent to b modulo m when m divides $a-b$. If a is congruent to b modulo m, we write $a \equiv b \pmod m$. If a is not congruent to b modulo m i.e., if $a-b$ is not divisible by m then we write $a \not\equiv b \pmod m$

Example: 5 divides $17-2$. Hence $17 \equiv 2 \pmod 5$. But $11-3$ is not divisible by 5. Hence $11 \not\equiv 3 \pmod 5$

Theorem 15. Let a, b, c, d be integers and m a positive integer. Then
(i) $a \equiv a \pmod m$
(ii) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$
(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$

Proof: (i) m divides $a-a=0$. Hence $a \equiv a \pmod m$

(ii) Suppose $a \equiv b \pmod m$. Then m divides $a-b$. So, $a-b = km$, k is an integer. So, $b-a = (-k)m$. So, m divides $b-a$. So, $b \equiv a \pmod m$

(iii) Suppose $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Then m divides $a-b$ and m divides $b-c$. So, $a-b = km$ and $b-c = sm$, where k and s are some integers.

Now $a-c = a-b+b-c = km+sm = (k+s)m = tm$

where $t = k+s$ is an integer.

Hence m divides $a-c$. So, $a \equiv c \pmod m$

Theorem 16. Let a, b, c, d be integers and m a positive integer. Then
(i) $a \equiv b \pmod m$ implies $(a+c) \equiv (b+d) \pmod m$
(ii) $a \equiv b \pmod m$ implies $ac \equiv bd \pmod m$

Proof: (i) Let $a \equiv b \pmod m$ Then $a-b = km$, k is an integer.

Then $(a+c)-(b+c) = a-b = km$. So, $(a+c) \equiv (b+c) \pmod m$

(ii) Let $a \equiv b \pmod m$. Then $a-b = km$, k is an integer.

Then $ac - bc = (a-b)c = (kc)m = k'm$ where $k' = kc$ is an integer. So, $ac \equiv bc \pmod m$

Theorem 17 Let a, b, c, d be integers and m a positive integer. Then

(i) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $(a+c) \equiv (b+d) \pmod m$

(ii) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$

(iii) If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$ for any positive integer n.

Proof: (i) Since $a \equiv b \pmod m$ and $c \equiv d \pmod m$, $a - b = k_1 m$ and $c - d = k_2 m$, k_1 and k_2 are integers

Now, $(a+c) - (b+d) = (a-b) + (c-d) = k_1 m + k_2 m = (k_1 + k_2)m = k'm$

where $k' = k_1 + k_2$ is an integer.

So, $(a+c) \equiv (b+d) \pmod m$

(ii) As $a \equiv b \pmod m$ and $c \equiv d \pmod m$, $a - b = k_1 m$ and $c - d = k_2 m$ where k_1, k_2 are integers. So $ac - bc = (k_1 c)m$ and $bc - bd = (k_2 b)m$

So, $ac - bd = (ac - bc) + (bc - bd) = (k_1 c)m + (k_2 b)m$

$= (k_1 c + k_2 b)m = k'm$ where $k' = k_1 c + k_2 b$ is an integer.

So, $ac \equiv bd \pmod m$

(iii) We prove this result by induction on n. Suppose $n = 1$,

Since $a \equiv b \pmod m$, it follows that $a^n \equiv b^n \pmod m$ for $n = 1$

Suppose $a^k \equiv b^k \pmod m$ for some positive integer $k \geq 1$

Since $a \equiv a \pmod m$, by (ii) we find that

$$a^{k+1} \equiv a b^k \pmod m \quad \text{---} \quad (A)$$

Again as $a \equiv b \pmod m$ and $b^k \equiv b^k \pmod m$, by (ii) we get

$$ab^k \equiv b^{k+1} \pmod m \quad \text{---} \quad (B)$$

So, from (A) and (B) by (iii) Theorem 15, we have

$a^{k+1} \equiv b^{k+1} \pmod m$. So, by principle of mathematical induction $a^n \equiv b^n \pmod m$ for any positive integer n.

Note: Theorem 16 is a corollary of Theorem 17.

Note: $a \equiv b \pmod m$ implies $f(a) \equiv f(b) \pmod m$ where $f(x)$ is any polynomial with integral coefficients. (This follows as a corollary of Theorem 17.)

Proof: Let $f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ where $a_0, a_1, \ldots, a_n$ are integers. Let $a \equiv b \pmod m$. Then $a^i \equiv b^i \pmod m$, $i = 1, 2, \ldots, n$

and $a_i a^{n-i} \equiv b_i b^{n-i} \pmod m$ $\quad i = 0, 1, \ldots n$

Then $(a_0 a^n + a_1 a^{n-1} + \cdots + a_n) \equiv (a_0 b^n + a_1 b^{n-1} + \cdots + a_n) \pmod m$

(by Theorem 17)

Hence $f(a) \equiv f(b) \pmod m$

Theorem 18 Let a, b, c be integers and m a positive integer. Then (i) $ab \equiv ac \pmod m$ if and only if $b \equiv c \pmod{\frac{m}{\gcd(a,m)}}$

(ii) If $a \equiv ac \pmod m$ and $\gcd(a, m) = 1$, then

$b \equiv c \pmod m$

Proof: (i) Let $\gcd(a,m) = d$. Since $m > 0$, $d \neq 0$, there exist integers r and s such that $a = dr$ and $m = ds$ and $\gcd(r, s) = 1$. Now $ab \equiv ac \pmod m$ implies that m divides $ab - ac$ i.e., ds divides $ab - ac = drb - drc$ i.e., s divides $r(b-c)$. Since s and r are relatively prime, it follows that s divides $b - c$

Hence $b \equiv c \pmod s$ $\quad (s > 0$ as $m > 0)$

or, $b \equiv c \pmod{\frac{m}{d}}$

Conversely, assume that $b \equiv c \pmod{\frac{m}{d}}$. Then

$b - c = k\frac{m}{d}$ for some integer k. Hence

$$ab - ac = k\frac{m}{d}a = km\frac{a}{d} = kmr = (kr)m$$

So, $ab \equiv ac \pmod m$,

(ii) It follows from (i).

Some worked out problems: 1. Let a, b, c, d be integers and m a positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then prove that $ax + cy = bx + dy \pmod m$ for any integer x, y.

Proof: Suppose $a \equiv b \pmod m$. Then $a - b = km$

Then $(a-b)x = (kx)m$. Let $c \equiv d \pmod m$ Then $(c-d)x = k'm$

So, $(c-d)y = (k'y)m$ (k, k' are integers)

Now $(ax + cy) - (bx + dy) = (a-b)x + (c-d)y = (kx + k'y)m$

$= k''m$, where $k'' = kx + k'y$ is an integer.

So, $(ax + cy) \equiv (bx + dy) \pmod m$

2. What is the remainder when 7^{30} is divided by 4?

Solution: Let r be the required remainder. Then $0 \le r < 4$ and $7^{30} - r$ is divisible by 4. Hence $7^{30} \equiv r \pmod 4$

Now $7 \equiv 3 \pmod 4$. Hence $7^2 \equiv 3^2 \pmod 4$ But $3^2 \equiv 1 \pmod 4$

Hence $7^2 \equiv 1 \pmod 4$. This implies $(7^2)^{15} \equiv 1^{15} \pmod 4$

Or, $7^{30} \equiv 1 \pmod 4$

Hence the remainder is 1.

3. What is the remainder when $6 \cdot 7^{32} + 7 \cdot 9^{45}$ is divided by 4?

Solution: $7^2 \equiv 1 \pmod 4$. Hence $(7^2)^{16} \equiv 1^{16} \pmod 4$

or, $7^{32} \equiv 1 \pmod 4$. So, $6 \cdot 7^{32} \equiv 6 \pmod 4$

Again $9 \equiv 1 \pmod 4$. Hence $9^{45} \equiv 1 \pmod 4$

So, $7 \cdot 9^{45} \equiv 7 \pmod 4$. So, it follows that

$6 \cdot 7^{32} + 7 \cdot 9^{45} \equiv (6+7) \pmod 4$

or, $6 \cdot 7^{32} + 7 \cdot 9^{45} \equiv 13 \pmod 4$

But $13 \equiv 1 \pmod 4$. Hence $6 \cdot 7^{32} + 7 \cdot 9^{45} \equiv 1 \pmod 4$. So, the remainder is 1.

Exercises: 1. What is the remainder when 11^{72} is divided by 6?

2. What is the remainder when 3^{36} is divided by 77?

Congruence classes

Definition: Let m be a positive integer and a an integer. Then the subset $= \{b \in \mathbb{Z} : b \equiv a \pmod m\}$ is called the congruence class modulo m of the integer a. We denote this congruence class by $[a]$ or $\bar{a}$

Example: Let $m = 6$ and $a = 4$. Then the congruence class modulo 6 of 4 is the subset

$$\begin{aligned}[4] &= \{b \in \mathbb{Z} : b \equiv 4 \pmod 6\} \\ &= \{b \in \mathbb{Z} : b - 4 = 6k \text{ for some integer } k\} \\ &= \{b \in \mathbb{Z} : b = 6k + 4 \text{ for some integer } k\} \\ &= \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}\end{aligned}$$

In the following theorem we prove some basic properties of congruence class modulo m.

Theorem 19 Let m be a positive integer. The congruence classes modulo m satisfy the following:

(i) $[a]$ is non-empty for all integers a

(ii) If $b \in [a]$, then $[b] = [a]$ for all integers a, b

(iii) For all integers a, b, either $[a] \cap [b] = \phi$ or $[a] = [b]$, ϕ is the null set

Proof (i) As $a \equiv a \pmod m$. So, $a \in [a]$ and $[a] \neq \phi$.