Linear Diophantine Equations

Def A linear Diophantine equation is of the form $ax + by = c$,

where a, b, c are given integers and a, b are not both zero.

* A sol. of this equation is a pair of integers x_0, y_0, that when substituted in the equation, satisfy it i.e. $ax_0 + by_0 = c$.

Note A linear Diophantine equation can have many solutions or no solution at all.

for example $3x + 6y = 18$ has many sol. like

$(4,1)$, $(-6,6)$, $(10,-2)$ etc.

but eq. $2x + 10y = 17$ has no sol. as LHS is always even but RHS is odd.

Theorem The linear Diophantine equation $ax + by = c$ has a solution iff $d \mid c$ where $d = \gcd(a,b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by

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

where t is an arbitrary integer.

Proof Firstly assume that $ax+by=c$ has a solution x_0, y_0 and $d = \gcd(a,b)$

$\Rightarrow \exists$ integers r and s s.t.

$a = dr, \quad b = ds$

as $ax_0 + by_0 = c \Rightarrow \quad drx_0 + dsy_0 = c$

$\Rightarrow d(rx_0 + sy_0) = c$

$\Rightarrow d \mid c$

Conversely let $d \mid c \Rightarrow c = dt$ for some integer t.

as $d = \gcd(a,b)$

$\Rightarrow \exists$ integers x_0 and y_0 s.t.

$d = ax_0 + by_0$

$\Rightarrow \quad dt = ax_0t + by_0t$

$\Rightarrow \quad c = a(tx_0) + b(ty_0)$

$\Rightarrow tx_0, ty_0$ is solution of equation $ax+by=c$.

All other solutions: Now let x_0, y_0 is a known solution of linear Diophantine equation

$ax + by = c$

and if x', y' is any other solution, then

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

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

as $d = \gcd(a,b) \Rightarrow$ ~~$d=a$~~ $a = dr, \quad b = ds$

where $(r,s) = 1$

Putting this value in ①, we get

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

$$\Rightarrow r(x'-x_0) = s(y_0-y') \quad -②$$

$\Rightarrow r \mid s(y_0-y')$ & as $(r,s)=1$, we get

$r \mid y_0-y' \Rightarrow y_0-y' = rt$ for some integer t

and then from ② $r(x'-x_0) = srt$

$$\Rightarrow x'-x_0 = st$$

hence $x' = x_0 + st$, $y' = y_0 - rt$

$$x' = x_0 + \left(\frac{b}{d}\right)t, \quad y' = y_0 - \left(\frac{a}{d}\right)t$$

Hence proved.

Cor If $\gcd(a,b)=1$ and if x_0, y_0 is a particular solution of linear Diophantine eq. $ax+by=c$, then all solutions are given by $x = x_0+bt$, $y = y_0-at$ for integral values of t.

Proof. Obvious from above theorem.

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

Sol.

" " oranges = y

and cost of orange = 2.

then by the question,

$(2+3)x + 2y = 132$ and $x + y = 12$

$\Rightarrow 2(x+y) + 3x = 132$ & $x + y = 12$

$\Rightarrow 3x + 12 \cdot 2 = 132$

$\Rightarrow x + 4 \cdot 2 = 44$, which is linear Diophantine eq.

as $(1,4) = 1$ and $1 \mid 44 \Rightarrow$ ∃ sol. of this eq.

as $1 = 1(-3) + 4(1)$

$\Rightarrow 44 = 1(-3 \times 44) + 4(44)$

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

$\Rightarrow x_0 = -132$, $z_0 = 44$ is one sol. of above eq.

and other sol. are

$x = -132 + 4t$, $z = 44 - t$ where t is arbitrary integer

note that $6 < x \leq 12$

so we will find t, so that $6 < x \leq 12$.

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

$\Rightarrow 138 < 4t \leq 144$

$\Rightarrow 34\frac{1}{2} < t \leq 36 \Rightarrow t = 35$ or 36.

for $t = 35$, $x = 8$ for $t = 36$, $x = 12$.

Hence either all apples were purchased at cost 14 Rs each ($\because z = 8$ if $t = 36$) or 8 apples and 4 oranges were purchased at cost 12 Rs and 9 Rs respectively.

Ex. (1) Which of the following Diophantine equations can not be solved?

(a) $6x + 51y = 22$

(b) $33x + 14y = 115$

(c) $14x + 35y = 93$.

(2) Determine all sol. in the integers of the following Diophantine equations:

(a) $56x + 72y = 40$

(b) $24x + 138y = 18$

(c) $221x + 35y = 11$

Non-Linear Diophantine Equations

Fermat's last Theorem: Fermat stated that if $n > 2$, then the non-linear Diophantine equation

$$x^n + y^n = z^n$$

has no solution in the integers, other than the trivial solutions in which atleast one of the variables is 0.

In this topic, we will learn a proof in case $n = 4$.

To carry through the argument, we first undertake the task of identifying all solutions in the +ve integers of the equation

$$x^2 + y^2 = z^2$$

Def. A Pythagorean triple is a set of three integers x, y, z such that $x^2 + y^2 = z^2$.

The triple is said to be primitive if $\gcd(x, y, z) = 1$.

For example $3, 4, 5$; $5, 12, 13$; $12, 35, 37$ all are primitive Pythagorean triple.

Lemma 1 If x, y, z is a primitive Pythagorean triple, then one of the integers x or y is even, while the other is odd.

Proof. If both x & y are even

then $2 \mid (x^2 + y^2) \Rightarrow 2 \mid z^2 \Rightarrow 2 \mid z$

$\Rightarrow \gcd(x, y, z) \neq 1$

$\longrightarrow\!\leftarrow$.

If both x & y are odd

then $x^2 \equiv 1 \pmod 4$

& $y^2 \equiv 1 \pmod 4$

$\Rightarrow z^2 = x^2 + y^2 \equiv 2 \pmod 4$

which can not be true, as square of any integer must be congruent to 0 or $1 \bmod 4$.

Hence one of x & y is even and the other is odd.

(7)

Lemma 2 If $ab = c^n$, where $\gcd(a, b) = 1$, then a and b are n^{th} powers; that is $\exists$ positive integers a_1, b_1 for which $a = a_1^n$, $b = b_1^n$.

Proof. We can assume that $a > 1$ and $b > 1$ (∵ otherwise lemma is clearly true)

let $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, $b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$

be prime factorizations of a and b

as $\gcd(a, b) = 1 \Rightarrow$ no p_i can be equal to any q_j.

$\Rightarrow ab = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$

is a prime factorization of ab.

let $c = u_1^{l_1} u_2^{l_2} \cdots u_t^{l_t}$ be prime factorization of c.

Then as $ab = c^n$

$\Rightarrow p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s} = u_1^{nl_1} u_2^{nl_2} \cdots u_t^{nl_t}$

$\Rightarrow$ Primes $u_1, \cdots, u_t$ are $p_1, \cdots, p_r, q_1, \cdots, q_s$ in some order and $nl_1, nl_2, \cdots, nl_t$ are the corresponding exponents $k_1, \cdots, k_r, j_1, \cdots, j_s$.

$\Rightarrow$ Each of the integers k_i and j_i is divisible by n.

let $a_1 = p_1^{k_1/n} p_2^{k_2/n} \cdots p_r^{k_r/n}$

$b_1 = q_1^{j_1/n} q_2^{j_2/n} \cdots q_s^{j_s/n}$

then $a_1^n = a$, $b_1^n = b$

Theorem All the solutions of the Pythagorean equation $x^2+y^2=z^2$, satisfying the condition $\gcd(x,y,z)=1$, $2|x$; $x>0, y>0, z>0$ are given by the formulas

$$x = 2st, \quad y = s^2-t^2, \quad z = s^2+t^2$$

for integers $s>t>0$ such that $\gcd(s,t)=1$ and $s \not\equiv t \pmod 2$

Proof Let x, y, z be a (positive) primitive Pythagorean triple.

As $2|x \Rightarrow x$ is even and so by lemma 1, y must be odd and hence z must be odd

$\Rightarrow z-y$ and $z+y$ are even.

Let $z-y = 2u$ and $z+y = 2v$.

$$x^2+y^2 = z^2 \Rightarrow x^2 = z^2-y^2 = (z-y)(z+y)$$

$$\Rightarrow \left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv \quad \text{— (1)}$$

Let $d = \gcd(u,v)$

then $d|u, d|v \Rightarrow d|u-v$ and $d|u+v$

$\Rightarrow d|y$ and $d|z$

but $\gcd(y,z)=1 \Rightarrow d=1$.

now by lemma 2, (1) implies that

$u = t^2$, $v = s^2$ for some +ve integers s, t

$\Rightarrow z = u+v = s^2+t^2$

$y = v-u = s^2-t^2$, $x^2 = 4uv = 4s^2t^2$.

$\Rightarrow x = 2st$.

also as $\gcd(y,z)=1$

$\Rightarrow \gcd(s,t)=1$

Also if both s and t are even or both s and t are odd, then

$z = s^2+t^2$, $y = s^2-t^2$ will be both even

$\Rightarrow \gcd(z,y) \geq 2$ $\longrightarrow \leftarrow$.

$\Rightarrow$ one of s and t is even and the other is odd.

$\Rightarrow s-t$ can't be even.

$\Rightarrow 2 \nmid s-t$

$\Rightarrow s \not\equiv t \pmod 2$

Hence proved.

Conversely let s,t be two +ve integers s.t. $\gcd(s,t)=1$, $s \not\equiv t \pmod 2$ and

$x = 2st$, $y = s^2-t^2$, $z = s^2+t^2$.

T.P. x, y, z is primitive Pythagorean triple.

$$x^2+y^2 = 4s^2t^2 + s^4+t^4-2s^2t^2 = s^4+t^4+2s^2t^2$$
$$= (s^2+t^2)^2 = z^2$$

$\Rightarrow x,y,z$ is Pythagorean triple.

let $\gcd(x,y,z)=d>1$

and p be any prime divisor of d.

then $p \neq 2$

$\because p \mid d \Rightarrow p \mid z$ and z is odd, as $s \not\equiv t \pmod 2$ implies one of s & t is even & one is odd

as $p|y$ and $p|z$

$\Rightarrow p|y+z$ and $p|z-y$

$\Rightarrow p|2s^2$ & $p|2t^2$

$\Rightarrow p|s^2$ & $p|t^2$ $\quad \because p \neq 2$

$\Rightarrow p|s$ & $p|t$

$\rightarrow\leftarrow$ as $\gcd(s,t)=1$

$\Rightarrow d=1$

hence x, y, z is a primitive Pythagorean triple.

Note: If x, y, z is any Pythagorean triple and $d = \gcd(x, y, z)$ then $x = dx_1$, $y = dy_1$, $z = dz_1$ for some integers x_1, y_1, z_1

and $x_1^2 + y_1^2 = \frac{x^2+y^2}{d^2} = z_1^2$

with $\gcd(x_1, y_1, z_1) = 1$

$\Rightarrow x_1, y_1, z_1$ is primitive Pythagorean triple.

Hence from a primitive Pythagorean triple, one can obtain arbitrary Pythagorean triple by multiplying the primitive Pythagorean triple with suitable non-zero integer.

This is the reason, we found only all primitive Pythagorean triple in above theorem.

Theorem (Fermat) The Diophantine equation $x^4+y^4=z^2$ has no solution in the integers x, y, z.

Proof. Suppose there exists a positive solution x_0, y_0, z_0 of $x^4+y^4=z^2$.

If $\gcd(x_0, y_0)=d$, then $x_0=dx_1$, $y_0=dy_1$ for some integers x_1, y_1

$$x_0^4+y_0^4=z_0^2 \Rightarrow d^4(x_1^4+y_1^4)=z_0^2$$

$$\Rightarrow d^4 \mid z_0^2 \Rightarrow d^2 \mid z_0$$

$$\Rightarrow z_0=d^2z_1 \text{ for some integer } z_1$$

$$\Rightarrow d^4(x_1^4+y_1^4)=d^4z_1^2 \Rightarrow x_1^4+y_1^4=z_1^4$$

with $\gcd(x_1, y_1)=1$.

Hence x_1, y_1, z_1 is a primitive sol of $x^4+y^4=z^2$.

$$\Rightarrow (x_1^2)^2+(y_1^2)^2=z_1^2.$$

$\Rightarrow x_1^2, y_1^2, z_1$ is primitive Pythagorean triple.

So by previous thm., $\exists$ relatively prime integers $s>t>0$ s.t.

$$x_1^2=2st, \quad y_1^2=s^2-t^2, \quad z_1=s^2+t^2 \quad \text{---} (\Delta)$$

where exactly one of s and t is even.

If s is even then

$$1 \equiv y_1^2=s^2-t^2 \equiv 0-1 \pmod 4$$

$$\equiv 3 \pmod 4$$

[$\because$ square of an odd integer is $\equiv 1 \bmod 4$]

$\Rightarrow$ s is odd and t is even.

let $t = 2r$ — (1)

then $x_1^2 = 2st = 4sr$

$\Rightarrow \left(\frac{x_1}{2}\right)^2 = sr$

as $\gcd(s,t) = 1 \Rightarrow \gcd(s,r) = 1$

Hence by lemma 2, $s = z_2^2$, $r = w_2^2$ — (2) for positive integers z_2, w_2.

now $t^2 + y_1^2 = s^2$

and $\gcd(s,t) = 1 \Rightarrow \gcd(s,t,y_1) = 1$

$\Rightarrow$ t, y_1, s is primitive Pythagorean triple with t even.

So again by previous theorem,

$t = 2uv$, $y_1 = u^2 - v^2$, $s = u^2 + v^2$ — (*)

for relatively prime integers $u > v > 0$

$t = 2uv \Rightarrow uv = \frac{t}{2} = r = w_2^2$ (from (1) and (2))

$\Rightarrow u = x_2^2$, $v = y_2^2$ for some integers x_2, y_2. — (3)

(by lemma 2)

from (*) $s = u^2 + v^2$

$\Rightarrow z_2^2 = x_2^4 + y_2^4$ (from (2) and (3))

as z_2 and t are +ve., we have

$0 < z_2 \le z_2^2 = s \le s^2 < s^2 + t^2 = z_1$ (from Δ)

$\Rightarrow 0 < z_2 < z_1$

So starting with one solution x_1, y_1, z_1 of $x^4+y^4=z^2$, we have constructed another solution x_2, y_2, z_2 s.t.

$$0 < z_2 < z_1.$$

Repeating the whole argument, again we can construct a solution x_3, y_3, z_3 s.t.

$$0 < z_3 < z_2.$$

and so on.

This process can be carried out as many times as desired to produce an infinite decreasing sequence of +ve integers

$$z_1 > z_2 > z_3 > \cdots$$

as z_1 is an integer so there can be only finitely many integers less than z_1,

so contradiction occurs.

Hence $x^4+y^4=z^2$ is not solvable for +ve integers.

Cor. The equation $x^4+y^4=z^4$ has no solution in +ve integers.

Pf: If x_0, y_0, z_0 is a +ve sol. of

$$x^4+y^4=z^4$$

then x_0, y_0, z_0^2 is a +ve sol of $x^4+y^4=z^2$

which is not possible.

Hence $x^4 + y^4 = z^4$ has no solution in +ve integers.

Gauss lemma : Let p be an odd prime and let $\gcd(a,p)=1$. If n denotes the number of integers in the set

$$S = \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\},$$ whose remainders upon division by p, exceeds $p/2$, then $\left(\frac{a}{p}\right) = (-1)^n$.

[Firstly let's understand with an example.

Let $p = 11$ and $a = 5$.

Then $S = \{5, 10, 15, \ldots, \left(\frac{11-1}{2}\right)\cdot 5\}$

$= \{5, 10, 15, 20, 25\}$.

Dividing each element of S by 11, we see that the remainders are

5, 10, 4, 9, 3

$\frac{p}{2} = 5.5$, so here we have two integers whose remainder exceeds 5.5

$\Rightarrow \left(\frac{5}{11}\right) = (-1)^2 = 1$.].

Proof : Integers in the set S are of the form ka, where $1 \le k \le \frac{p-1}{2}$.

If $p \mid ka$, then either $p \mid k$ or $p \mid a$

but p can not divide k as $1 \le k \le \frac{p-1}{2}$

and $p \nmid a$ as $\gcd(a,p)=1$

$\Rightarrow p \nmid ra$

$\Rightarrow ka \not\equiv 0 \pmod{p}$

$\Rightarrow$ no element of set S is completely divisible by p. — ①

also if $ia \equiv ja \pmod{p}$ for some $1 \le i, j \le \frac{p-1}{2}$

then $(i-j)a \equiv 0 \pmod{p}$

$\Rightarrow p \mid (i-j)a \Rightarrow p \mid (i-j)$

which is again not possible as bro earlier.

$\Rightarrow$ no two elements of S are congruent to each other modulo p — ②

From ① and ②, we can say that all elements of S leave non-zero remainders on division by p.

Hence no. of remainders is $\frac{p-1}{2}$. — ③

(i.e equal to no. of elements in S)

Let $r_1, r_2, \ldots r_m$ be those remainders upon division by p s.t. $0 < r_i < p/2$ — (*)

and let $s_1, s_2, \ldots, s_n$ be those remainders such that

$$\frac{p}{2} < s_i < p$$

(Note that remainder can't be $\frac{p}{2}$ as $\frac{p}{2}$ is not an integer)

Then by ③, $m+n = \frac{p-1}{2}$.

as $\frac{p}{2} < s_i < p$

$\Rightarrow -\frac{p}{2} > -s_i > -p$

$\Rightarrow p - \frac{p}{2} > p - s_i > p - p$

$\Rightarrow \frac{p}{2} > p - s_i > 0$

$\Rightarrow 0 < p - s_i < p/2$ —(**)

from (*) and (**), we see that

$s_1, s_2, \ldots, s_m, p-s_1, \ldots, p-s_n$ are all positive and less than $p/2$.

Now we prove that, these integers are all distinct.

Assume that $p - s_i = s_j$ for some $i \neq j$.

then $s_i \equiv ua \pmod p$ and $s_j \equiv va \pmod p$

for some $1 \leq u, v \leq \frac{p-1}{2}$.

$\Rightarrow (u+v)a \equiv s_i + s_j = p \pmod p$

$= 0 \pmod p$

$\Rightarrow p \mid (u+v)a \Rightarrow p \mid (u+v)$ as $(a,p)=1$

but $1 \leq u \leq \frac{p-1}{2}$, $1 \leq v \leq \frac{p-1}{2}$

$\Rightarrow 2 \leq u+v \leq p-1 \Rightarrow p \nmid u+v$.

Hence all $\frac{p-1}{2}$ remainders, @

$r_1, r_2, \ldots, r_m, p-s_1, \ldots, p-s_n$ are different

as each $r_i < p/2 \Rightarrow r_i \leq \frac{p-1}{2}$

each $p - s_i < \frac{p}{2} \Rightarrow p - s_i \leq \frac{p-1}{2}$

$\Rightarrow r_1, r_2, \ldots, r_m, p-s_1, \ldots, p-s_n$ are simply integers $1, 2, \ldots, \frac{p-1}{2}$ (but may not be in order as seen in example)

$\Rightarrow r_1 r_2 \ldots r_m (p-s_1) \ldots (p-s_n) = 1.2.3 \ldots \frac{p-1}{2}$

$= \left(\frac{p-1}{2}\right)!$

$\Rightarrow \left(\frac{p-1}{2}\right)! \equiv r_1 r_2 \ldots r_m (p-s_1) \ldots (p-s_n) \pmod{p}$

$\equiv r_1 r_2 \ldots r_m (-s_1) \ldots (-s_n) \pmod{p}$

$= (-1)^n r_1 \ldots r_m s_1 \ldots s_n \pmod{p}$ — (4)

also $r_1 r_2 \ldots r_m s_1 s_2 \ldots s_n \equiv a \cdot 2a \cdot 3a \ldots \left(\frac{p-1}{2}\right) a \pmod{p}$

$= \left(\frac{p-1}{2}\right)! \; a^{\frac{p-1}{2}} \pmod{p}$ — (5)

from (4) and (5)

$\left(\frac{p-1}{2}\right)! \equiv (-1)^n \left(\frac{p-1}{2}\right)! \; a^{\frac{p-1}{2}} \pmod{p}$

as $\left(\left(\frac{p-1}{2}\right)!, p\right) = 1 \Rightarrow 1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p}$