International Review of Pure and Applied Mathematics
Volume 14 • Number 2 • July-December 2018

Solution of Linear Diophantine Equation

Rajesh Kumar

Abstract: In this paper, we have discussed the Linear Diophantine Equation *ax* + *by* = *c*, where *a*, *b*, *c* are integers and a, b are not both zero. Some of the tools introduced, however, will be useful in many other parts of the subject.

Keywords: Diophantine Equation and Integral solution

1. LINEAR DIOPHANTINE EQUATION

An equation in one or more unknowns which is to be solved in integers is called Diophantine Equation, named after the Greek Mathematician Diophantus. See ([2])

A linear Diophantine equation of the form $ax + by = c$ may have many solutions in integers or may not have even a single solution.

2. NECESSARY AND SUFFICIENT CONDITION FOR EXISTENCE OF LINEAR DIOPHANTINE EQUATION

If a, b, c are integers and a, b are not both zero, then the linear diophantine equation $ax + by = c$ has an integral solution if and only if $\gcd(a, b)$ is a divisor of c.

Proof. Let one integral solution of the equation $ax + by = c$ be (x_1, y_1). Then $ax_1 + by_1 = c$, where (x_1, y_1) are integers. Let $\gcd(a, b) = d$ and so $d|a$ and $d|b$ which implies $d|(ax_1 + by_1)$, i.e., $d|c$.

Conversly, let $\gcd(a, b)$ be a divisor of c. Let $\gcd(a, b) = d$ and so $a = dm, b = dn$ where m, n are integers prime to each other. Let $c = dp$ where p is an integer. Now since m, n are prime to each other, there exist integers u, v such that $mu + nv = 1$.Then

$$dmup + dnvp = dp$$

$$\Rightarrow a(up) + b(vp) = c$$

This implies that (up, vp) is a solution of the equation $ax + by = c$ where up and vp are integers. Hence the equation $ax + by = c$ has an integral solution.

Theorem 2.1. The linear Diophantine Equation $ax + by = c$ has a solution if and only if $d|c$, where $d = \gcd(a, b)$ and if (x_0, y_0) by any particular solution of the equation, then all other solutions will be

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

Where t is an arbitrary integer.

Proof. To prove the second part of the theorem, let us suppose that (x_0, y_0) be a known solution of the given equation. Now if x', y' is any other solution, then

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

Which is equivalent to

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

So there exist relatively prime integers r and s such that $a = dr,\ b = ds$. Substituting these value into the last equation and canceling the common factor d, we get $r(x' - x_0) = s(y_0 - y')$. Then $r|s\ (y_0 - y')$, with $\gcd(r, s) = 1$. Using Euclid's lemma, we get $r|(y_0 - y')$; or in other words $(y_0 - y') = rt$ for some integer t and so $(x' - x_0) = st$. form this we get $x' = x_0 + st = x_0 + \left(\frac{b}{d}\right)t, y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t$ which satisfy the Diophantine equation

$$\begin{aligned} ax' + by' &= a\left[x_o + \left(\frac{b}{d}\right)t\right] + b[y_o - \left(\frac{a}{d}\right)t] \\ &= (ax_o + by_o) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t \\ &= c + o.t \\ &= c \end{aligned}$$

Hence there are infinite number of solutions of the given equation, one for each value of t.

Example 2.2. Let us take the linear Diophantine equation

$$172r + 20s = 1000$$

Solution 2.3. First applying the Euclidean's Algorithm we find that

$$172 = 8.20 + 12$$

$$20 = 1.12 + 8$$

$$12 = 1.8 + 4$$

$$8 = 2.4$$

Therefore $\gcd(172{,}20) = 4$. Now, Since $4|1000, a$ solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backward through the previous calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2.12 - 12 \\ &= 2(172 - 8.20) - 20 \\ &= 2.172 + (-17)20 \end{aligned}$$

Multiplying this relation by 250, we get

$$1000 = 250.4 = 250[2.172 + (-17)20] = 500.172 + (-4250)20$$

so $r = 500$ and $s = 4250$ provide one solution to the Diophantine equation. All other Solutions are

$$r = 500 + \left(\frac{20}{4}\right)t = 500 + 5t \quad s = -4250 - \left(\frac{172}{4}\right)t = -4250 - 43t$$

for some integer t and for positive integers solutions, if exist, t must be chosen to satisfy simultaneously the inequalities

$$5t + 500 > 0, \quad -43t - 4250 > 0$$

or,

$$-98\frac{36}{43} > t > -100$$

Next, we are looking for the non-trivial solution of the nonlinear Diophantine equation.

3. FERMAT'S LAST THEOREM

The equation

$$x^n + y^n = z^n \tag{2.1}$$

where n is an integer greater than 2, has no integral solutions, except the trivial solutions in which one of the variables is 0.See([3])

The theorem had never been proved for all n. Later this has been resolved and proved for all n. In this chapter we are giving the solution of Fermat's last theorem i.e. the equation (2.1) is soluble for $n = 2$ and also the equation (2.1) has no integral solution for $n = 3$ and 4.

Theorem 3.1. The general solution of the equation

$$x^2 + y^2 = z^2 \tag{2.2}$$

Satisfying the conditions

$$x > 0, y > 0, z > 0, (x, y) = 1, 2|x, \tag{2.3}$$

is

$$x = 2ab, y = a^2 - b^2, z = a^2 + b^2, \tag{2.4}$$

where a, b are integer's and

$$(a, b) = 1, a > b > 0, \tag{2.5}$$

There is a one to one correspondence between different values of a, b and different values of x, y, z.

Proof. First, we assume that $x^2 + y^2 = z^2$ and $x > 0, y > 0, Z > 0, (x, y) = 1, 2|\ x$. Now since $2|x$ and $(x, y) = 1, y$ and z are odd and $(y, z) = 1$. So $\frac{1}{2}(z - y)$ and $\frac{1}{2}(z + y)$ are integral and

$$\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$$

Then by (2.2),

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$$

and the two factors on the right, being coprime, must both be squares. So

$$\frac{z+y}{2} = a^2, \frac{z-y}{2} = b^2$$

where

$$a > 0, b > 0, a > b, (a, b) = 1$$

Also

$$a + b \equiv (a^2 + b^2) = z \equiv 1(mod2)$$

Where a and b are of opposite parity. Therefore any solution of (2.2), satisfying (2.3), is of the form (2.4); and a and b are of opposite parity and satisfy (2.5).

Next, we assume that a and b are of opposite parity and satisfy (2.5). Then

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2,$$

$$x > 0, Y > 0, z > 0, 2|x$$

$$\text{If } (x, y) = d, then\ d|\ z, and\ so$$

$$d|y = (a^2 - b^2), d|z = (a^2 + b^2)$$

Therefore $d|2a^2, d|2b^2. Since\ (a, b) = 1, d$ must be 1 or 2, and the second alternative is excluded because y is odd. Hence $(x, y) = 1$ and if y and z are given, a^2 and b^2 are uniquely determined, so that different values of x, y and z correspond to different values of a and b.

Theorem 3.2. There are no positive integral solutions of the equation

$$x^4 + y^4 = z^2 \tag{2.6}$$

Proof. Let u be the least number for which

$$x^4 + y^4 = u^2(x > 0, y > 0, u > 0) \tag{2.7}$$

has a solution. Then $(x, y) = 1$, otherwise we can divide through by $(x, y)^4$ and so replace u by a smaller number. Therefore at least one of x and y is odd, and $u^2 = x^4 + y^4 \equiv$ 1 or 2 (mod4).

Since $u^2 \equiv 2(mod4)$ is impossible, so u is odd, and one of x and y is even. Now if x is even, then by (2.3.1),

$$x^2 = 2ab, y^2 = a^2 - b^2, u = a^2 + b^2,$$

$a > 0, b > 0, (a.b) = 1$ and a and b are of opposite parity. Again if a is even and b is odd. then

$y^2 \equiv (-1)(mod4)$ which is impossible; so a is odd and b is even, say $b = 2c$. Next we get

$$(\frac{1}{2}x)^2 = ac(a,c) = 1$$

and so

$$a = d^2, c = f^2, d > 0, f > 0, (d,f) = 1$$

and d is odd. Therefore

$$y^2 = a^2 - b^2 = d^4 - 4f^2$$

$$(2f^2)^2 + y^2 = (d^2)^2$$

and no two $2f^2, y, d^2$ have a common factor.

Now by applying theorem (2.3.1) again, we obtain

$$2f^2 = 2lm,\ d^2 = l^2 + m^2, l > 0, m > 0, (l,m) = 1.$$

Since

$$f^2 = lm, (l,m) = 1$$

we get

$$l = r^2, m = s^2 (r > 0, s > 0)$$

and so

$$r^4 + s^4 = d^2.$$

But

$$d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$$

and u is not the least number for which the equation (2.7) is possible. This is a contradiction which proves the theorem.

4. PYTHAGOREAN TRIPLES AND THE UNIT CIRCLES

We have already described all the solutions to

$$x^2 + y^2 = z^2 \tag{2.8}$$

in whole numbers x, y and z. Now if we divide this equation by z^2, we obtain

$$(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1 \tag{2.9}$$

and so the pair of rational numbers $(\frac{x}{z},\frac{y}{z})$is a solution to the equation

$$u^2+v^2=1 \tag{2.10}$$

Therefore there are four rational solutions to the equation $u^2+v^2=1$ see ([4]) These are $(\pm1,0)$ and $(0,\pm1)$. Now if (x_0,y_0) is a point on the circle with rational coordinates, then the slope of the line joining $(u_0,v_0)$to (-1,0) is rational. Conversely, if a line through (-1,0) with rational slope intersects the circle at another point (u_0,v_0), then u_0 and v_0 are rational.

Let t be a rational number. Let us consider the line with slope t through (-1,0) and it has the equation $\frac{v-0}{u+1}=t$ or $v=t(u+1)$. Substituting this in (2.10) we obtain $u^2+t^2(u+1)^2=1$ or $u^2(1+t^2)+2t^2u+t^2-1=0$. Now we can use the quadratic formula to solve for u, or we observe that one root is -1 and the sum of the roots of the equation $au^2+bu+c=0$ is $-\frac{b}{a}$, hence

$$u-1=-\frac{2t^2}{1+t^2}$$

or

$$u=\frac{1-t^2}{1+t^2}$$

Let $t=\frac{s}{r}$ with $(s,r)=1$ and so

$$u=\frac{x}{z}=\frac{1-\frac{s^2}{r^2}}{1+\frac{s^2}{r^2}}=\frac{r^2-s^2}{r^2+s^2}$$

Since $(x,z)=1$ and if $(r^2-s^2,r^2+s^2)=1$, then

$$x=r^2-s^2, z=r^2+s^2, y=2rs$$

But $(r^2-s^2,r^2+s^2)\neq 1$, we cannot take$x=r^2-s^2, z=r^2+s^2$, because $(r,s)=1$ implies that $(r^2-s^2,r^2+s^2)=1,2$. Again if $(r^2-s^2,r^2+s^2)=2$,

$$x=\frac{r^2-s^2}{2}, z=\frac{r^2+s^2}{2}, y=rs$$

This equation can be written as the from stated in the theorem. Here both r and s must be odd, so we can transform

$$z = (\frac{r+s}{2})^2 + (\frac{r-s}{2})^2$$

$$z = (\frac{r+s}{2})^2 - (\frac{r-s}{2})^2$$

$$y = 2\left(\frac{r+s}{2}\right)\left(\frac{r-s}{2}\right)$$

Now letting $m = \frac{r+s}{2}$ and $n = \frac{r-s}{2}$ and adding switching x and y, we see that the solution is again of the form

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2$$

Conversely, we can easily verify that for any$(m, n) = 1$, these formulas yield a Pythagorean Triple.

REFERENCES

[1] Apostol T.M., "Introduction to Analytic Number Theory", Spinger International Student Edition, Narosa Publishing House (1989)

[2] Burton D.M. "Elementary Number Theory", Tata McGraw-Hill Edition, Sixth Edition (2006)

[3] Hardy G.H., Wright E.M. "An Introduction to the Theory of Numbers" Oxford Science Publications, Fifth Edition (1979)

[4] Kumundury R, Romero C., "Number Theory with Computer Application" Prentice hall (1998)

[5] Mapa S.K. "Higher Algebra", Milinda De for Levant Books, Sixth Revised Edition (2004)

Rajesh Kumar
Research Scholar Deptt. of Mathematics,
V.K.S. University, Ara (Bihar)