Linear Diophantine Equation: Solution and Applications

U.N. Roy[#1], R. P. Sah[#2], A. K. Sah[#3]and S. K. Sourabh[#4]
[#1]*Dept of Mathematics, BRM College, Munger, Bihar, India*
[#2]*Dept of Mathematics, R Lal College, Lakhisarai, Munger, Bihar, India*
[#3]*Head, Department of Mathematics, Marwari College, Bhagalpur, Bihar, India*
[#4] *UDCA, T.M. Bhagalpur University, Bhagalpur, Bihar, India*

Abstract

This paperinvestigates the integer solution of Diophantine Equation (DE). We also discuss the different applications of DE

Keywords – *Number theory, Diophantine, Linear equation, Set of integer.*

I. INTRODUCTION

The Theory of Numbers has been a favorite subject of study and research by leading mathematicians and thousands of amateurs ([1], [6]-[12]). The subject matter is very concrete set of whole numbers though the solutions of certain problems of linear Diophantine equation involve use of higher arithmetical theories real or complex numbers. In which encounters greater variety in type of proofs or in which find more simple problems to stimulate for interest, challenge ability and increase the mathematical strength ([2]-[5], [13]-[16]) .

A. *Greatest Common Divisor*

If the integers a, b > 0, then we define greatest common divisor of a andb, as the largest number that divides both a and b. It is used by (a, b) = c or gcd(a, b) = c. We use (a, b) to denote the greatest common divisor.

Example: Find gcd of 15 and 35. The divisors of 15 are ±1, ±3, ±5, ±15 and the divisors of 35 are ±1, ±5, ±7, ±35. So the common divisors of 15 and 35 are ±1, ±5. Thus the greatest common divisor is 5 .So the gcd of 15 and 35 is 5 and by notation (15, 35) = 5.

1) Theorem: *The Diophantine equation$ax + by = c$, has solution if gcd(a,b) | c. If so, it has infinitely many solutions and any one solution can be used to generate the other entire one.*

Proof: Since the gcd(a,b) divides both ax and by, hence divides c if there is a solution . This gives the necessity of the condition.

From the extended Euclidean Algorithm, gives any integers a and b, we can find s and t such that

$$as + bt = gcd\ (a,b\ ) \qquad (1)$$

the numbers s and t are not unique . Once we find s and t.

Since we are assuming that $gcd(a,b)$ divides c, there exits an integer k such that

$$gcd(a,b)k = c$$

Multiplying by k in (1), we get

$$a(sk\ )+ b(tk) = gcd\ (a,b)\ \ = c$$

So this gives one solution with $x = sk$ *and* $y = tk.$

Now suppose that $a\,x_1 + b\,y_1 = c$ is a solution and $ax + by = c$ is some other solution . Then

$$(ax_1 - x\ )\ + b\ (y_1 - y\ ) = 0$$

Therefore,

$$a\ (x_1 - x\ )\ =\ b\ (\ y - y_1) \qquad (2)$$

This means that a divides$b\ (\ y - y_1)$ and therefore $\frac{a}{gcd\ (a,b)}$divides $(y - y_1)$

So, $y = y_1 + r\frac{a}{gcd\ (a,b)}$, for some integer r.

Hence,equation (1) becomes

$$a(x_1 - x) = rb.\frac{a}{gcd\ (a,b)}$$

So, $$x= x_1 - r.\frac{b}{gcd\ (a,b)}$$

Thus if $a\,x_1 + b\,y_1 = c$ is any solution, then all solutions are of the form

$$x= x_1 - r.\frac{b}{gcd\ (a,b)},\ \ y = y_1 + r\frac{a}{gcd\ (a,b)}$$

Example: We consider an equation $258x + 147y\ =\ 369$

From Euclidean Algorithm, first we have to find gcd(147,258), the primitive equation on the far right is how we will use this equality after we are done with the computation.

$$258 = 147(1) + 111, \qquad \text{equivalently, } 111 = 258 - 147$$
$$147 = 111(1) + 36, \qquad \text{equivalently, } 36 = 147 - 111$$
$$111 = 36(3) + 3, \qquad \text{equivalently , } 3 = 111 - 3(36)$$

So ,gcd(147, 258) . Since 3 |369, the equation has integral solutions.
Now we have to find a way of writing 3 as a linear combination of 147 and 258 by the Euclidean Algorithm computation above and the equalities on the far right, we get

$$\begin{aligned} 3 &= 111 - 3(36) \\ &= 111 - 3(147 - 111) = 4(111) - 3(147) \\ &= 4(258 - 147) - 3(147) \\ &= 4(258) - 7(147) \end{aligned}$$

Then we take $258(4) + 147(-7) = 3$, and multiplying by 123; why 123 ?
Because $3(123) = 369$,we get

$$258(492) + 147(-861) = 369 ,$$

So, the solution is $x = 492$ and $y = -861$
All other solutions will have the form

$$X = 492 - 147r/3 = 492 - 49r$$
$$Y = -861 + 258r/3 = 86r - 861 \;, r \in Z$$

Here we take choose, $r = t + 10$ then reduce those constants by making a simple change of variable, we have

$$X = 492 - 49(t+10) = 2 - 49t$$
$$Y = 86(t+10) - 861 = 86t - 1, \quad t \in Z$$

The solution of the linear Diophantine equation in other perform via row- reduction on augmented matrix – analogous to methods used in linear algebra.
For instance, $mx + ny = gcd(x,y)$
One begins with two rows (n 1 0) and (n 0 1) representing the two equations

$$n = 1n + 0n,$$
$$n = 0n + 1n$$

Then one executes the Euclidean algorithm on the numbers in first column, doing the same operations in parallel on the other columns.
Here we take an example: $d = x(80) + y(62)$

In equation form	In row form		
$80 = 1(80) + 0(62)$	80	1	0
$62 = 0(80) + 1(62)$	62	0	1
row1 - row2 =>$18 = 1(80) - 1(62)$	18 1	-1	
row2 - 3 row3 => $8 = -3(80) + 4(62)$	8	-3	4
row3 -2 row 4 => $2 = 7(80) - 9(62)$	2	7	-9
row4 - 4row5 => $0 = -31(80) - 40(62)$	0	-31	40

=> row2 – row 3 = row 4 on the identity –augmented matrix.
In effect we have row– reduced the first two rows to the last two. The matrix effecting the reduction is in the bottom right corner.It starts as the identity, and is multiplied by such elementary row operation matrix. Henceit accumulates the product of all the row operation, namely:
The 1st row is the particular solution: $2 = 7(80)-9(62)$
The 2nd row is the homogenous solution: $0 = -31(80) + 40(62)$
So the solution is my linear combination of the two:
$n$row 1 + m row 2 => $2n = (7n-31m)\,80 + (40m - 9n)\;62$
The same row/ column reduction techniques tackle arbitrary systems of linear Diophantine equation. Such techniques generalize easily to similar coefficient rings possessing a Euclideanalgorithm, e.g. polynomial rings $F(x)$ over a filed, Gaussian integers Z .There are many analogous interesting methods.

Another method: It does not require finding an initial solution, but it may require finding a modular multiplicative inverse. We take an example instead of a generalization.
Example: Solve $2x + 3y = 5$
Solution: We can write ,$2x = 5 (mod\ 3)$
Divide both sides by 2 ,$gcd(3,2) = 1$
$x = 1\ (mod\ 3)$ =>$x = 3n + 1$,$n \in Z$
Substitute this value of x into the original equation:
$2(3n + 1) + 3y = 5$ =>$y = 1-2n$, $n \in Z$
Ans: $(x,y) = (3n + 1, 1-2n)$, $n \in Z$.

2) Theorem: *A solution to the linear Diophantine equation*

$$m_1\, x_1 + m_2 x_2 + \ldots\ldots + m_p\, x_p = l,$$

wherethe solution will depend on (p –1)parameters exactly as expect from linear algebra.

Proof: We consider the linear Diophantine equation

$$m.x + n.y = l$$

Case 1: Suppose $(m,n) \nmid l$,then

$$(m,n) \mid (mx + ny) = l$$

Which contradicts our supposition?This shows that there cannot be a solution.

Case 2: Suppose $(m,n) \mid l$. Write$l = k\,(m,n)$, *for* $k \in Z$. . There are integers m and n such that

$$mu + nv = (m,n)$$

Then

$$muk + nvk = (m,n)k$$

Hence, $x = uk$, y = vk , is a solution.

Suppose $x = x_o, y = y_o$, is a particular solution. Then

$$m\left(\frac{n}{gcd\,(m,n)}k + x_o\right) + n\left(-\frac{m}{gcd\,(m,n)}\, k + y_o\right) = \frac{mn}{gcd\,(m,n)} - \frac{mn}{gcd\,(m,n)} + m\, x_o + n\, y_o = 0 + l$$

This proves that $x = \frac{n}{gcd\,(m,n)}\, k + x_o$, y = $-\frac{m}{gcd\,(m,n)}\, k + y_o$is a solution for every $k \in Z$.

Finally, we want to show that every solution has this form. Suppose then that $(x, y)$is a solution. Then $mx + ny = l$ and $mx_0 + n\, y_0 = l$

$$\Rightarrow m\,(x - x_0) + n(\,y - y_0) = l - l = 0$$

Therefore,

$$\frac{m}{gcd\,(m,n)}(\,x - x_0) + \frac{n}{gcd\,(m,n)}\left(\frac{m}{gcd\,(m,n)}\right) = 0$$

$$\frac{m}{gcd\,(m,n)}(\,x - x_0) = -\quad \frac{n}{gcd\,(m,n)}(\,y - y_0) \ldots\ldots\ldots\ldots\ldots \quad (1)$$

Now $\frac{m}{gcd\,(m,n)}$ divides the left side, so it divides the right side. However,

$$\left(\frac{m}{(m,n)}\ ,\ \frac{n}{(m,n)}\right) = 1$$

Therefore,

$\frac{m}{gcd\,(m,n)} \mid (\,y - y_0)$, or $(\,y - y_0) = k.\,\frac{m}{gcd\,(m,n)}$, for some k

Thus,

$$y = y_0 + k.\frac{m}{gcd\,(m,n)}$$

From equation (1)

$$\frac{m}{gcd\,(m,n)}(x - x_0) = -\quad \frac{n}{gcd\,(m,n)}(\,y - y_0) = -\quad \frac{n}{gcd\,(m,n).}\,\frac{m}{gcd\,(m,n).}k$$

$$x - x_0 = -\quad k\,\frac{n}{gcd\,(m,n)}$$

$$x = x_0 - \quad k\,\frac{n}{gcd\,(m,n)}$$

This is the required solution in the theorem with an unimportant switch of *k* and -*k*.

Example: Find the solution of the linear Diophantine equation

$50\, x + 20\, y = 300$, where initially$(x_0, y_0) = (\,2, 10)$

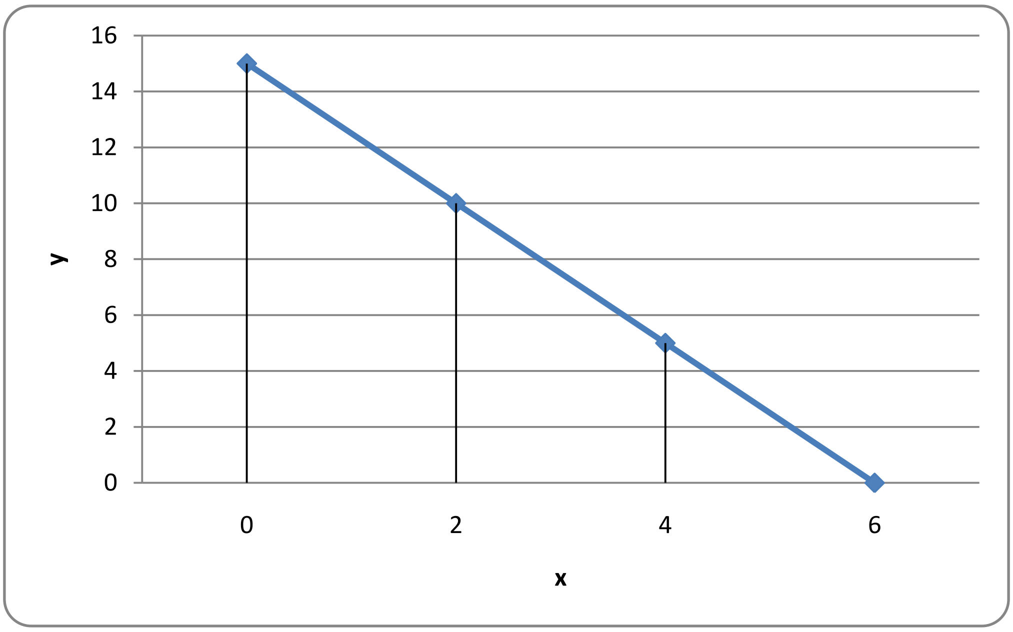
Solution:Since, *gcd* (*m,n*) = *gcd*(50, 20) =10

So, $x = x_0 + \frac{n}{(m,n)}.k$, $y = y_0 - \frac{m}{(m,n)}.k$, $k \in Z$.

Therefore, $x = 2 + \frac{20}{10}.k = 2 + 2k$, $y = 10 - \frac{50}{10}.k = 10 - 5k$, $k \in Z$.

Thus , $\{\,(x, y) : x = 2 + 2k\,, y = 10 - 5k\,\}$, $k \in \{\,-1, 0, 1, 2\}$

Figure: Graphical Solution of DE



II. CONCLUSION

In this paper, we have investigated the integer solution of Diophantine Equation (DE). We also discussed the different applications of DE

REFERENCES

[1]. Hardy,G.H., and Wright,E.M., An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, Oxford, New York, 1979.

[2]. Mendelsohn, N. S., A Linear Diophantine Equation with Applications to Non- Negative Matrices, Annals of the New York Academy of Science, September 1970, pp. 287-294.

[3]. Bond, J., Calculating the General Solution of a Linear Diophantine equation, The American Mathematical Monthly, 1967 – JSTOR.

[4]. David Papp, Effective Solution of Linear Diophantine Equation Systems with an Application in Chemistry, Journal of Mathematical Chemistry, Vol. 39, No. 1, January 2006.

[5]. U. Banerjee, Dependence Analysis for Supercomputing, Chapter-5. Linear Diophantine Equations, Kluwer Academic Publishers, 1988, pp. 67-99.

[6]. Joseph H.Silverman, A Friendly Introduction To Number Theory, Precentice-Hall,Inc., New Jersey, 2001

[7]. H.E.Rose, A Course In Number Theory,Clarendon Press, New York, 1994

[8]. William Judson Leveque, Topics In Number Theory, Addison-Wesley Publishing Company, USA, 1958

[9]. Ivan Niven, Herbert S.Zuckerman, An Introduction To The Theory Of Numbers, John Wiley Sons,Inc., USA, 1967

[10]. Kenneth H.Rosen, Elemantary Number Theory And Its Applications, Greg Tobin, USA, 2005

[11]. Peter J.Eccles, An Introduction To Mathematical Reasoning:Numbers,Sets And Functions, Cambridge University Press, United Kingdom, 1997

[12]. Neville Robins, Beginning Number Theory, Jones And Barlett Publishers, USA, 2006

[13]. M. Clausen, A. Fortenbacher: Efficient solution of linear Diophantine equations. J. Symbolic Comput. 8 (1989), 201–216.

[14]. M. Filgueiras, A. P. Tom´as: A fast method for finding the basis of non-negative solutions to a linear Diophantine equation. J. Symbolic Comput., 19 (1995), 507– 526.

[15]. M. Henk, R. Weismantel: On minimal solutions of linear Diophantine equations. Beitr. Alg. Geom. 41 (2000), 49–55.

[16]. R. Stanley: Linear homogeneous Diophantine equations and and magic labelings of graphs. Duke Math. J. 40 (1973), 607–632.