Diophantine Equation

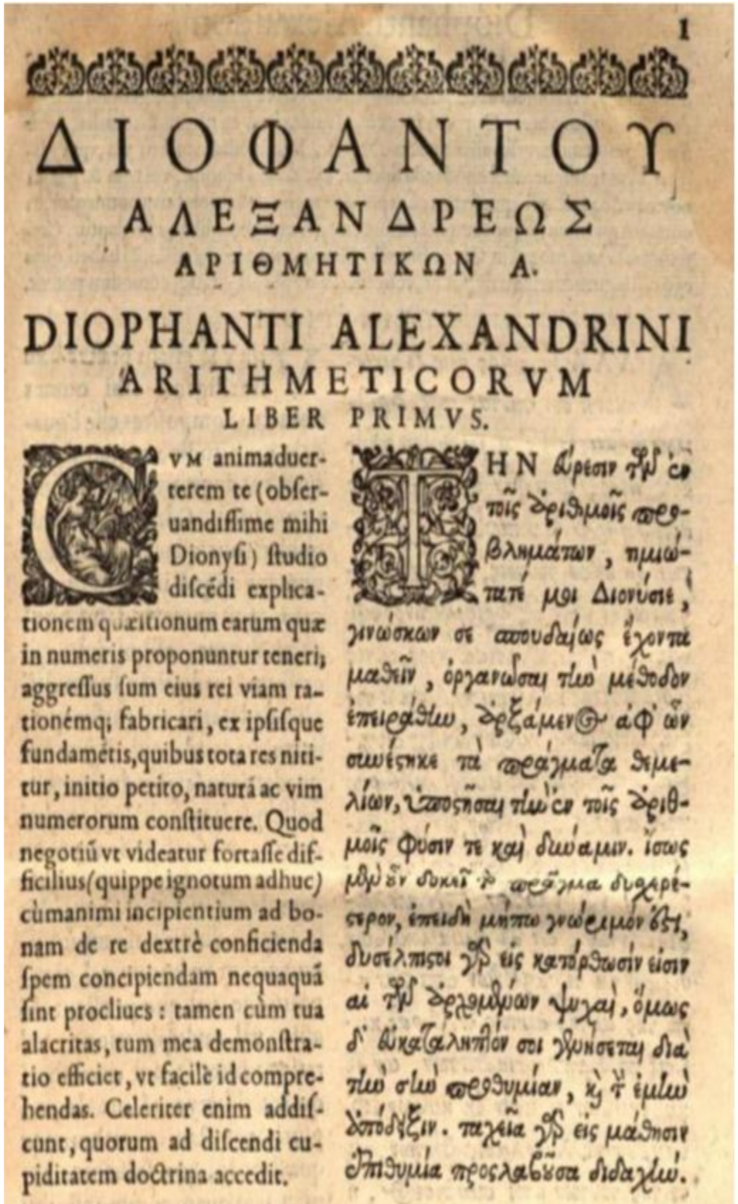
Linear Equation ---- $ax+by=c$

Mr.Raut S.R.
Head, Dept. of Mathematics
Mrs.K.S.K.College Beed.

Great Mathematician Diophantus:

Diophantus of Alexandria,

dedication to Dionysius in The Arithmetica
3rd Century AD


1

ΔΙΟΦΑΝΤΟΥ
ΑΛΕΞΑΝΔΡΕΩΣ
ΑΡΙΘΜΗΤΙΚΩΝ Α.

DIOPHANTI ALEXANDRINI
ARITHMETICORVM
LIBER PRIMVS.

CVM animaduerterem te (obseruandissime mihi Dionysi) studio discédi explicationem quaestionum earum quae in numeris proponuntur teneri; aggressus sum eius rei viam rationémq; fabricari, ex ipsisque fundamētis, quibus tota res nititur, initio petito, naturā ac vim numerorum constituere. Quod negotiū vt videatur fortasse difficilius (quippe ignotum adhuc) cùm animi incipientium ad bonam de re dextrè conficienda spem concipiendam nequaquā sint procliues: tamen cùm tua alacritas, tum mea demonstratio efficiet, vt facilè id comprehendas. Celeriter enim addiscunt, quorum ad discendi cupiditatem doctrina accedit.

ΤΗΝ εὕρεσιν τῶν ἐν τοῖς ἀριθμοῖς προβλημάτων, τιμιώτατέ μοι Διονύσιε, γινώσκων σε σπουδαίως ἔχοντα μαθεῖν, ὀργανῶσαι τὴν μέθοδον ἐπειράθην, ἀρξάμενος ἀφ' ὧν συνέστηκε τὰ πράγματα θεμελίων, ὑποστῆσαι τὴν ἐν τοῖς ἀριθμοῖς φύσιν τε καὶ δύναμιν. ἴσως μὲν οὖν δοκεῖ τὸ πρᾶγμα δυσχερέστερον, ἐπειδὴ μήπω γνώριμόν ἐστι, δυσέλπιστοι γὰρ εἰς κατόρθωσιν εἰσὶν αἱ τῶν ἀρχομένων ψυχαί, ὅμως δ' εὐκατάληπτόν σοι γενήσεται διὰ τὴν σὴν προθυμίαν, καὶ τὴν ἐμὴν ἀπόδειξιν. ταχεῖα γὰρ εἰς μάθησιν ἐπιθυμία προσλαβοῦσα διδαχήν.

"Perhaps the subject will appear rather difficult, inasmuch as it is not yet familiar (beginners are, as a rule, too ready to despair of success); but you, with the impulse of your enthusiasm and the benefit of my teaching, will find it easy to master; for eagerness to learn, when seconded by instruction, ensures rapid progress."

THE DIOPHANTINE EQUATION $ax + by = c$

THEOREM 2-9. *The linear Diophantine equation* $ax + by = c$ *has a solution if and only if* $d \mid c$, *where* $d = \gcd(a, b)$. *If* x_0, y_0 *is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t$$

for varying integers t.

Proof:

equation $ax + by = c$ admits a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. We know that there are integers r and s for which $a = dr$ and $b = ds$. If a solution of $ax + by = c$ exists, so that $ax_0 + by_0 = c$ for suitable x_0 and y_0, then

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0),$$

which simply says that $d \mid c$. Conversely, assume that $d \mid c$, say $c = dt$. Using Theorem 2-3, integers x_0 and y_0 can be found satisfying $d = ax_0 + by_0$. When this relation is multiplied by t, we get

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Hence, the Diophantine equation $ax + by = c$ has $x = tx_0$ and $y = ty_0$

Proof: To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

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

which is equivalent to

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

By the Corollary to Theorem 2-4, there exist relatively prime integers r and s such that $a = dr$, $b = ds$. Substituting these values into the last-written equation and cancelling the common factor d, we find that

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

The situation is now this: $r \mid s(y_0 - y')$, with $\gcd(r, s) = 1$. Using Euclid's Lemma, it must be the case that $r \mid (y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st.$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + (b/d)t,$$
$$y' = y_0 - rt = y_0 - (a/d)t.$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for,

$$\begin{aligned} ax' + by' &= a[x_0 + (b/d)t] + b[y_0 - (a/d)t] \\ &= (ax_0 + by_0) + (ab/d - ab/d)t \\ &= c + 0 \cdot t = c. \end{aligned}$$

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

An example:

- Determine all solutions in the positive integers of the following Diophantine Equations:
  - a) $18x + 5y = 48$.
  - b) $54x + 21y = 906$.
  - c) $123x + 360y = 99$.
  - $158x - 57y = 7$.

a)

First we find gcd(18,5)

By Euclidian algorithm

We have,

$$18 = 3 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

- The last non zero remainder is 1,so that

  d=gcd(18,5)= 1.

Now we eliminate remainders 1,2,3 successively ,

We get,

$$
\begin{aligned}
1 &= 3 - 1\times 2 \\
&= 3 - 1(5 - 1\times 3) \\
&= 3\times 2 - 1\times 5 \\
&= (18 - 5\times 3)\times 2 - 1\times 5 \\
&= 18\times 2 + 5(-7)
\end{aligned}
$$

Multiplying on both sides by 48 we get

$$48 = 18 \times 96 + 5(-336)$$

Thus xo =96 and yo = -336 provides one solution of the Diophantine Equation. All other solutions are given by,

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$

c

where t is any integer.

$$x = 96 + 5t \quad \text{and} \quad y = -336 - 18t$$

To find all solutions in the positive integers t must be chosen to satisfy the inequalities,

$$96+5t \succ 0 and -336-18t \succ 0$$

$$5t \succ -96 and -336 \succ 18t$$

$$i.e. t \succ -19\frac{1}{5} and -18\frac{12}{18} \succ t$$

$$-18\frac{12}{18} \succ t \succ -19\frac{1}{5}$$

$$t=-19$$

Hence , $t=-19$

The required positive solution is,

x = 1 and y =6.

Thanks