A METHOD TO SOLVE THE DIOPHANTINE EQUATION

\[ ax^2 - by^2 + c = 0 \]

Florentin Smarandache, Ph D
Associate Professor
Chair of Department of Math & Sciences
University of New Mexico
200 College Road
Gallup, NM 87301, USA
E-mail: smarand@unm.edu

ABSTRACT
We consider the equation

\[ (1) \ ax^2 - by^2 + c = 0, \text{ with } a, b \in \mathbb{N}^* \text{ and } c \in \mathbb{Z}^*. \]

It is a generalization of the Pell’s equation: \( x^2 - Dy^2 = 1 \). Here, we show that: if the equation has an integer solution and \( a \cdot b \) is not a perfect square, then (1) has an infinitude of integer solutions; in this case we find a closed expression for \( (x_n, y_n) \), the general positive integer solution, by an original method. More, we generalize it for any Diophantine equation of second degree and with two unknowns.

INTRODUCTION
If \( ab = k^2 \) is a perfect square \( (k \in \mathbb{N}) \) the equation (1) has at most a finite number of integer solutions, because (1) become:

\[ (2) \ (ax - ky)(ax + ky) = -ac \]

If \( (a, b) \) does not divide \( c \), the Diophantine equation does not have solutions.

METHOD TO SOLVE. Suppose that (1) has many integer solutions. Let \( (x_0, y_0), \ (x_1, y_1) \) be the smallest positive integer solutions for (1), with \( 0 \leq x_0 < x_1 \). We construct the recurrent sequences:

\[ \begin{cases} 
  x_{n+1} = ax_n + \beta y_n \\
  y_{n+1} = \gamma x_n + \delta y_n 
\end{cases} \]

making condition (3) verify (1). It results:

\[ \begin{cases} 
  a \alpha \beta = b \gamma \delta \\
  a\alpha^2 - b\gamma^2 = a \\
  a\beta^2 - b\delta^2 = -b
\end{cases} \]

having the unknowns \( \alpha, \beta, \gamma, \delta \).

We pull out \( a\alpha^2 \) and \( a\beta^2 \) from (5), respectively (6), and replace them in (4) at the square; we obtain

\[ a\delta^2 - b\gamma^2 = a \]  

We subtract (7) from (5) and find:

\[ \alpha = \pm \delta \]  

Replacing (8) in (4) we obtain:

1
\[ \beta = \pm \frac{b}{a} \gamma \]  
(9).

Afterwards, replacing (8) in (5), and (9) in (6) we find the same equation:

\[ a\alpha^2 - b\gamma^2 = a \]  
(10).

Because we work with positive solutions only, we take

\[
\begin{align*}
\alpha_{n+1} &= a_0\alpha_n + b\gamma_0\gamma_n \\
\gamma_{n+1} &= \gamma_0\gamma_n + a_0\gamma_n \\
\end{align*}
\]

where \((a_0, \gamma_0)\) is the smallest, positive integer solution of (10) such that \(a_0\gamma_0 \neq 0\).

Let \(\left(\begin{array}{c}
\alpha_0 \\
\gamma_0 \\
\end{array}\right) \in M_2(\mathbb{Z})\). It is evident that if \((x', y')\) is an integer solution for (1) then

\[
A \left(\begin{array}{c}
x' \\
y'
\end{array}\right), \quad A^{-1} \left(\begin{array}{c}
x' \\
y'
\end{array}\right)
\]
is another one – where \(A^{-1}\) is the inverse matrix of \(A\), i.e. \(A^{-1} \cdot A = A \cdot A^{-1} = I\) (unit matrix). Hence, if (1) has an integer solution it has an infinity. (Clearly \(A^{-1} \in M_2(\mathbb{Z})\)).

The \textbf{general positive integer solution} of the equation (1) is:

\[
(GS_1) \quad \text{with} \quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}, \text{ for all } n \in \mathbb{Z},
\]

where by convention \(A^0 = I\) and \(A^{-k} = A^{-1} \ldots A^{-1}\) of \(k\) times.

In problems it is better to write \((GS)\) as:

\[
(GS_2) \quad \text{and} \quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \text{ for } n \in \mathbb{N}^*
\]

We prove, by reduction at absurdum that \((GS_2)\) is a general positive integer solution for (1).

Let \((u, v)\) be a positive integer particular solution for (1). If

\[ \exists k_0 \in \mathbb{N} : (u, v) = A^{k_0} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \quad \text{or} \quad \exists k_1 \in \mathbb{N}^* : (u, v) = A^{k_1} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \text{ then } (u, v) \in (GS_1). \]

Contrary to this, we calculate \((u_{i+1}, v_{i+1}) = A^{-1} \begin{pmatrix} u_i \\ v_i \end{pmatrix}\), for \(i = 0, 1, 2, \ldots\) where \(u_0 = u, v_0 = v\). Clearly \(u_{i+1} < u_i\) for all \(i\). After a certain rank \(x_0 < u_0 < x_i\) it finds either \(0 < u_0 < x_0\), but that is absurd.

It is clear that we can put
\[(GS_3)\quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_0 \\ \varepsilon y_0 \end{pmatrix}, \quad n \in \mathbb{N}, \text{ where } \varepsilon = \pm 1.\]

Now we shall transform the general solution \((GS_3)\) in a closed expression.

Let \(\lambda\) be a real number. \(\text{Det}(A - \lambda \cdot I) = 0\) involves the solutions \(\lambda_{1,2}\) and the proper vectors \(V_{1,2}\) (i.e., \(A V_i = \lambda_i V_i, \ i \in 1,2\)). Note \(P = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in M_2(\mathbb{C})\)

Then \(P^{-1} A P = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\), whence \(A^n = P \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} P^{-1}\), and replacing it in \((GS_3)\)

and doing the computations we find a closed expression for \((GS_3)\).

**EXAMPLES**

1. For the Diophantine equation \(2x^2 - 3y^2 = 5\) we obtain

\[
\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix}^n \cdot \begin{pmatrix} 2 \\ \varepsilon \end{pmatrix}, \quad n \in \mathbb{N} \quad \text{and} \quad \lambda_{1,2} = 5 \pm 2\sqrt{6}, \quad v_{1,2} = (\sqrt{6}, \pm 2),
\]

whence a closed expression for \(x_n\) and \(y_n\):

\[
\begin{align*}
    x_n &= \frac{4 + \varepsilon \sqrt{6}}{4} (5 + 2\sqrt{6})^n + \frac{4 - \varepsilon \sqrt{6}}{4} (5 - 2\sqrt{6})^n \\
y_n &= \frac{3\varepsilon + 2\sqrt{6}}{6} (5 + 2\sqrt{6})^n + \frac{3\varepsilon - 2\sqrt{6}}{6} (5 - 2\sqrt{6})^n
\end{align*}
\]

for all \(n \in \mathbb{N}\).

2. For equation \(x^2 - 3y^2 - 4 = 0\) the general solution in positive integer is:

\[
\begin{align*}
x_n &= (2 + \sqrt{3})^n + (2 - \sqrt{3})^n \\
y_n &= \frac{1}{\sqrt{3}} (2 + \sqrt{3})^n + (2 - \sqrt{3})^n
\end{align*}
\]

for all \(n \in \mathbb{N}\),

that is \((2,0), (4,2), (14,8), (52,30), \ldots\)

**EXERCICIES FOR RADERS.**

Solve the Diophantine equations:

3. \(x^2 - 12y^2 + 3 = 0\)

[Remark: \(\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ \varepsilon \end{pmatrix} = ?, \quad n \in \mathbb{N}\)]

4. \(x^2 - 6y^2 - 10 = 0\)

[Remark: \(\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 2 & 5 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ \varepsilon \end{pmatrix} = ?, \quad n \in \mathbb{N}\)]

5. \(x^2 - 12y^2 - 9 = 0\)
[Remark: \( \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ \varepsilon \end{pmatrix} = ?, \quad n \in \mathbb{N} \)]

6. \( 14x^2 - 3y^2 - 18 = 0 \)

GENERALIZATIONS

If \( f(x,y) = 0 \) is a Diophantine equation of second degree and with two unknowns, by linear transformation it becomes

\[
(12) \quad ax^2 + by^2 + c = 0, \quad \text{with} \quad a, b, c \in \mathbb{Z}.
\]

If \( ab \geq 0 \) the equation has at most a finite number of integer solutions which can be found by attempts.

It is easier to present an example:

7. The Diophantine equation

\[
(13) \quad 9x^2 + 6xy - 13y^2 - 6x - 16y + 20 = 0
\]

becomes

\[
(14) \quad 2u^2 - 7v^2 + 45 = 0, \quad \text{where}
\]

\[
(15) \quad u = 3x + y - 1 \quad \text{and} \quad v = 2y + 1
\]

We solve (14). Thus:

\[
(16) \quad \begin{cases} u_{n+1} = 15u_n + 28v_n \\ v_{n+1} = 8u_n + 15v_n \end{cases}, \quad n \in \mathbb{N} \quad \text{with} \quad (u_0, v_0) = (3, 3\varepsilon)
\]

First solution:

By induction we prove that for all \( n \in \mathbb{N} \) we have that \( v_n \) is odd, and \( u_n \) as well as \( v_n \) are multiples of 3. Clearly \( v_0 = 3\varepsilon, u_0 \). For \( n + 1 \) we have:

\[
v_{n+1} = 8u_n + 15v_n = \text{even} + \text{odd} = \text{odd}, \quad \text{and of course} \quad u_{n+1}, v_{n+1} \quad \text{are multiples of 3 because} \quad u_n, v_n \quad \text{are multiple of 3 too}.
\]

Hence, there exist \( x_n, y_n \) in positive integers for all \( n \in \mathbb{N} \):

\[
(17) \quad \begin{cases} x_n = (2u_n - v_n + 3) / 6 \\ y_n = (v_n - 1) / 2 \end{cases}
\]

(from (15)). Now we’ll find the \( \langle GS_1 \rangle \) for (13) as closed expression, and by means of (17) it results the general integer solution of the equation (13).

Second solution:

Another expression of the \( \langle GS_1 \rangle \) for (13) will be obtained if we transform (15) as \( u_n = 3x_n + y_n - 1 \) and \( v_n = 2y_n + 1 \) for all \( n \in \mathbb{N} \). Whence, using (16) and doing the computation, we find

\[
(18) \quad \begin{cases} x_{n+1} = 11x_n + 11x_n + \frac{52}{3}y_n + \frac{11}{3} \\ y_{n+1} = 12x_n + 19y_n + 3 \end{cases}, \quad n \in \mathbb{N} \quad \text{with} \quad (x_0, y_0) = (1, 1) \text{ or } (2, -2)
\]

(two infinitude of integer solutions).
Let \( A = \begin{pmatrix} 11 & 52 & 11 \\ 3 & 3 \\ 0 & 0 & 1 \end{pmatrix} \), then \( \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \) or

\[
(19) \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}, \text{ always } n \in \mathbb{N}.
\]

From (18) we have always \( y_{n+1} \equiv y_n \equiv \ldots \equiv y_0 \equiv 1 \pmod{3} \), hence always \( x_n \in \mathbb{Z} \). Of course, (19) and (17) are equivalent as general integer solution for (13).

[The reader can calculate \( A^n \) (by the same method liable to the start on this note) and find a closed expression for (19).]

More generally:

This method can be generalized for the Diophantine equations:

\[
(20) \quad \sum_{i=1}^{n} a_i X_i^2 = b, \quad \text{with all } a_i, b \in \mathbb{Z}.
\]

If always \( a_i a_j \geq 0, \quad 1 \leq i < j \leq n \), the equation (20) has at most a finite number of integer solutions.

Now, we suppose \( \exists i_0, j_0 \in \{1, \ldots, n\} \) for which \( a_{i_0} a_{j_0} < 0 \) (the equation presents at least a variation of sign). Analogously, for \( n \in \mathbb{N} \), we define the recurrent sequences:

\[
(21) \quad x_h^{(n+1)} = \sum_{i=1}^{n} \alpha_{ih} x_i^{(n)} , \quad 1 \leq h \leq n
\]

considering \((x_1^0, \ldots, x_n^0)\) the smallest positive integer solution of (20). Replacing (21) in (20), it identifies the coefficients and it looks for \( n^2 \) unknowns \( \alpha_{ih} , \quad 1 \leq i, h \leq n \). (This calculation is very intricate, but it can be done by means of a computer.) The method goes on similarly, but the calculations become more and more intricate – for example to calculate \( A^n \), one must use a computer.

(The reader will be able to try this for the Diophantine equation \( ax^2 + by^2 - cz^2 + d = 0 \), with \( a, b, c \in \mathbb{N}^+ \) and \( d \in \mathbb{Z} \).

REFERENCES


[5] N. Ivășchescu - Rezolvarea ecuațiilor în numere întregi - This is his work for obtaining the title of professor grade 2, (coordinator G. Vraciu), Univ. Craiova, 1985.


