On the Diophantine equation \( ax^2 - by^2 = c \)

By A. GRELAK (Zielona Góra) and A. GRYTCZUK (Zielona Góra)

1. Introduction

In the paper [3] there has been given a matrix method for the study of some properties of the solutions in integers \( x, y \) of the Diophantine equation

\[
ax^2 - by^2 = c. 
\]

The study of (1.1) was begun by Lagrange and continued by several authors, see C. U. Jensen [5], P. Kaplan [6], J. C. Lagarias [7], H. Lienen [8], T. Nagell [9], [10], [11] and many others.

From Theorems 2 and 3 of our paper [3] we get the following solvability criteria in integers \( x, y \) for (1.1) when \( c = 1 \) or \( c = 2 \):

**Criterion 1.** Let \( a > 1, b \) be positive integers such that \( (a, b) = 1 \) and \( d = ab \) is not a square of a natural number. Moreover let \( \langle u_0, v_0 \rangle \) denote the least positive integer solution of Pell’s equation

\[
u^2 - dv^2 = 1. \tag{1.2}
\]

Then equation (1.1) with \( c = 1 \) has a solution in positive integers \( x, y \) iff

\[
2a \mid u_0 + 1 \quad \text{and} \quad 2b \mid u_0 - 1. \tag{1.3}
\]

We note that this result has been proved also by W. Górzny [2], but in another way.

**Criterion 2.** Let \( a, b \) be positive integers such that \( (a, b) = (a, 2) = (b, 2) = 1 \) and \( d = ab \) is not a square of a natural number and let \( \langle u_0, v_0 \rangle \) denote the least positive integer solution of (1.2). Then the equation (1.1) with \( c = 2 \) has a solution in positive integers \( x, y \) iff

\[
a \mid u_0 + 1 \quad \text{and} \quad b \mid v_0 - 1. \tag{1.4}
\]
By using an idea contained in [3] we give in this paper a solvability criterion for (1.1) when \( c > 2 \). Namely, we reduce the problem of the solvability of (1.1) in integers \( x, y \) to the investigation of the integer solutions of the following Diophantine equation

\[
u^2 - abv^2 = c^2.\]

We conclude the introduction by expressing our thanks to referee for the remarks incorporated in the present version of the paper.

2. Notations and Lemmas

Let \( d = ab \) and suppose that \((a,b) = (b,c) = (c,a) = 1\). In a similar way as in [3] we introduce the matrix

\[
S = \begin{bmatrix}
\sqrt{a}x & d & \sqrt{a}y \\
1 & \sqrt{a}y & \sqrt{a}x
\end{bmatrix}
\]

associated with the Diophantine equation (1.1). The matrix \( S \) will be called a solvable matrix if \( x, y \) are integers such that \((x,c) = 1\) and

\[
\det S = ax^2 - by^2 = c.
\]

In the case \( a = c = 1 \) the solvable matrix \( S \) will be called Pell’s solvable matrix. Hence

\[
P = \begin{bmatrix}
u & dv \\
v & u
\end{bmatrix}
\]

and

\[
\det P = u^2 - dv^2 = 1.
\]

Let \( \langle u_0, v_0 \rangle \) denote the least positive integer solution of (2.4), such a solution we will be called a primitive Pell’s solution. Now we can define the primitive solution of (1.1).

The solution \( \langle x_0, y_0 \rangle \) of (1.1) will be called primitive solution, if \( ax_0^2 - by_0^2 = c \) and \( x_0 \leq x \) for any positive integer \( x \) satisfying (1.1). Let \( S_0, P_0 \) be matrices associated with a primitive solution of (1.1) and a primitive Pell’s solution, respectively.
By (2.1) and (2.3) we have
\begin{equation}
S_0 = \begin{bmatrix}
\sqrt{a} x_0 & d \\
\sqrt{a} y_0 & \sqrt{a} x_0
\end{bmatrix}
\end{equation}
\begin{equation}
P_0 = \begin{bmatrix}
u_0 & dv_0 \\
v_0 & u_0
\end{bmatrix}
\end{equation}
From (2.5) and (2.6) we obtain
\begin{equation}
S_1 = S_0 P_0 = P_0 S_0 = \begin{bmatrix}
\sqrt{a} x_1 & d \\
\sqrt{a} y_1 & \sqrt{a} x_1
\end{bmatrix}
\end{equation}
where
\begin{equation}
x_1 = x_0 u_0 + by_0 v_0, \quad y_1 = y_0 u_0 + ax_0 v_0.
\end{equation}
From (2.7) and Cauchy’s Theorem on the product of determinants we get
\begin{equation}
\det S_1 = \det S_0 \cdot \det P_0 = \det P_0 \cdot \det S_0 = ax_1^2 - by_1^2 = c,
\end{equation}
because \( \det S_0 = c \) and \( \det P_0 = 1 \). From (2.9) it follows that the numbers \( x_1, y_1 \) given in (2.8) are solutions of (1.1).

Now we define the singular solution of (1.1).

**Definition 1.** The solution \( \langle u, v \rangle \) of (1.1) will be called a singular solution of (1.1) if
\begin{equation}
x_0 < u < x_1
\end{equation}
where \( x_1 \) is given by (2.8) and \( \langle x_0, y_0 \rangle \) is the primitive solution of (1.1).

We can prove the following

**Lemma 1.** Let \( c > 2 \) not be a square of a natural number and suppose that equation (1.1) has a primitive solution in positive integers \( x_0, y_0 \) such that \( (x_0, c) = 1 \). Then there exists a singular solution \( \langle u, v \rangle \) of (1.1).

**Proof.** Let \( d = ab \) and
\begin{equation}
u = x_0 u_0 - by_0 v_0, \quad v = y_0 u_0 - ax_0 v_0.
\end{equation}
It is easy to see that by (2.6) we have
\begin{equation}
P_0^{-1} = \begin{bmatrix}
u_0 & -dv_0 \\
-v_0 & u_0
\end{bmatrix}
\end{equation}
and \( \det P^{-1} = 1 \), thus by (2.7) and (2.8) it follows that the \( \langle u, |v| \rangle \) given by (2.11) is a solution of (1.1).

Since \( u_0^2 - abv_0^2 = 1 \) then \( u_0 > \sqrt{ab} v_0 \) and

\[
u = x_0 u_0 - by_0 v_0 > \sqrt{ab} v_0 x_0 - by_0 v_0 = v_0 \sqrt{b} (\sqrt{a} x_0 - \sqrt{b} y_0).
\]

On the other hand from the \( ax_0^2 - by_0^2 = c \), \( c > 2 \) follows that \( \sqrt{a} x_0 - \sqrt{b} y_0 > 0 \) and we obtain \( u > 0 \). Then from (2.11) and (2.8) we have

\[
0 < u < x_1.
\]

We remark that \( v \neq 0 \). Indeed, suppose that \( v = 0 \) then by (1.1) we have \( au^2 = c \). Since \( (a, c) = 1 \) thus \( a = 1 \) and \( u^2 = c \) contradicting our assumption that \( c \) is not a square of a positive integer. Since \( \langle x_0, y_0 \rangle \) is a primitive solution of (1.1), by (2.13) and the definition of a primitive solution we obtain

\[
x_0 \leq u < x_1.
\]

Suppose that in (2.14) we have \( u = x_0 \). Then by (2.11) it follows that

\[
x_0 (u_0 - 1) = by_0 v_0.
\]

On the other hand, since \( \langle u, |v| \rangle \) is a solution of \( ax^2 - by^2 = c \) by (2.11) we have

\[
a x_0^2 - b (ax_0 v_0 - y_0 u_0)^2 = c.
\]

From the last equality we obtain

\[
ax_0^2 - ax_0^2 (abv_0^2) + 2 au_0 x_0 (by_0 v_0) - u_0^2 (by_0^2) = c.
\]

From the assumptions we have \( ax_0^2 - by_0^2 = c \) and \( u_0^2 - abv_0^2 = 1 \) and therefore \( by_0^2 = ax_0^2 - c \) and \( abv_0^2 = u_0^2 - 1 \).

Substituting the last equality and (2.15) into (2.16) we obtain

\[
ax_0^2 - ax_0^2 (u_0^2 - 1) + 2 au_0 x_0^2 (u_0 - 1) - u_0^2 (ax_0^2 - c) = c.
\]

From (2.17) we get

\[
2 ax_0^2 - 2 ax_0^2 u_0 = c (1 - u_0^2)
\]

and consequently

\[
2 ax_0^2 (1 - u_0) = c (1 - u_0) (1 + u_0).
\]

Since \( u_0 \neq 1 \), the last equality implies

\[
2 ax_0^2 = c (u_0 + 1).
\]

Since \( (a, c) = 1 \) and \( (x_0, c) = 1 \), by (2.18) we get \( c \mid 2 \), thus \( c \leq 2 \), and this is impossible, because \( c > 2 \). Therefore \( u \neq x_0 \) and by (2.14) and the Definition 1 our Lemma follows.
Lemma 2. Let $S_1, S_2$ be the matrices associated with the solutions $\langle x_1, y_1 \rangle$ and $\langle x_2, y_2 \rangle$ of (1.1). Then the matrix $R = S_1 S_2 = S_2 S_1$ has the form

$$R = \begin{bmatrix} x_3 & dy_3 \\ y_3 & x_3 \end{bmatrix}$$

where

$$x_3 = ax_1 x_2 + by_1 y_2, \quad y_3 = x_1 y_2 + y_1 x_2$$

and $R$ is associated with the solution $\langle x_3, y_3 \rangle$ of the Diophantine equation

$$u^2 - dv^2 = c^2$$

where $d = ab$.

Proof. We have

$$(2.19) \quad R = S_1 S_2 = S_2 S_1 = \begin{bmatrix} \sqrt{a} x_1 & \frac{d}{\sqrt{a}} y_1 \\ \frac{1}{\sqrt{a}} y_1 & \sqrt{a} x_1 \end{bmatrix} \cdot \begin{bmatrix} \sqrt{a} x_2 & \frac{d}{\sqrt{a}} y_2 \\ \frac{1}{\sqrt{a}} y_2 & \sqrt{a} x_2 \end{bmatrix}. $$

From (2.19) we get

$$(2.20) \quad R = \begin{bmatrix} ax_1 x_2 + by_1 y_2 & d(x_1 y_2 + y_1 x_2) \\ x_1 y_2 + y_1 x_2 & ax_1 x_2 + by_1 y_2 \end{bmatrix}. $$

Putting in (2.20)

$$(2.21) \quad x_3 = ax_1 x_2 + by_1 y_2, \quad y_3 = x_1 y_2 + y_1 x_2$$

we get

$$(2.22) \quad R = \begin{bmatrix} x_3 & dy_3 \\ y_3 & x_3 \end{bmatrix}. $$

From (2.19) and the assumptions of our Lemma we get $\det S_1 = \det S_2 = c$ and therefore by Cauchy’s theorem on the product of determinants we obtain

$$(2.23) \quad \det R = \det S_1 \cdot \det S_2 = c^2. $$

On the other hand by (2.22) it follows that $\det R = x_3^2 - dy_3^2$ and therefore by (2.23) we get

$$x_3^2 - dy_3^2 = c^2, \quad \text{where } d = ab$$

and the proof is complete.
Lemma 3. All positive integral solutions of the equation
\[ x^2 - dy^2 = z^2 \]
are given by the formulas
\[ x = (am^2 + bn^2)\varrho, \quad y = 2mn\varrho, \quad z = (am^2 - bn^2)\varrho \]
if \( d = ab \) is even, or
\[ x = \frac{1}{2}(am^2 + bn^2)\varrho, \quad y = mn\varrho, \quad z = \frac{1}{2}(am^2 - bn^2)\varrho \]
if \( d = ab \) is odd and \( \varrho \) is any integer when \( m \) and \( n \) are odd, but \( \varrho \) is even when one of \( m \) and \( n \) is even and the other is odd. In all cases \( m, n \) are positive integers and relatively prime.

For the proof see [1], Th. 40, p. 41.

3. Result

In this part of our paper we prove the following

Theorem. Let \( a, b \) and \( c > 2 \) be positive integers such that \( (a, b) = (b, c) = (c, a) = 1 \) and \( d = ab \) is not a square of an integer. Then the equation
\[ ax^2 - by^2 = c \]
has a solution in positive integers \( x, y \) with \( (x, y) = 1 \) iff there exists an integer solution \( \langle u, v \rangle \) of the equation
\[ u^2 - dv^2 = c^2 \]

Proof. Suppose that the assumptions of our Theorem are fulfilled and let the equation (3.2) have an integer solution \( \langle u, v \rangle \). By Lemma 3 it follows that all positive integer solutions of (3.2) are given by the formulae
\[ u = (am^2 + bn^2)\varrho, \quad v = 2mn\varrho, \quad c = (am^2 - bn^2)\varrho \]
if \( d = ab \) is even, or
\[ u = \frac{1}{2}(am^2 + bn^2)\varrho, \quad v = mn\varrho, \quad c = \frac{1}{2}(am^2 - bn^2)\varrho \]
if \( d = ab \) is odd, where \( \varrho \) is any integer when \( m \) and \( n \) are odd, but \( \varrho \) is even when one of \( m \) and \( n \) is even and the other is odd. In all cases \( (m, n) = 1 \).

Let \( d = ab \) be even. Then by (3.3) in the case \( \varrho = 1 \) we obtain
\[ u = am^2 + bn^2, \quad c = am^2 - bn^2 \]
On the Diophantine equation $ax^2 - by^2 = c$ and consequently

$$\frac{u + c}{2} - \frac{u - c}{2} = am^2 - bn^2 = c,$$

so denote that the equation $ax^2 - by^2 = c$, has a solution in positive integers $m, n$ such that $(m, n) = 1$.

Let $d = ab$ be odd. Then by (3.4) in the case $\varrho = 2\varrho_1$ we have

$$u = (am^2 + bn^2)\varrho_1, \quad c = (am^2 - bn^2)\varrho_1$$

where $(m, n) = 1$ and $m, n$ are different parity. Thus for $\varrho_1 = 1$ we obtain

$$\frac{u + c}{2} - \frac{u - c}{2} = am^2 - bn^2 = c,$$

and we get a solution in positive integers $m, n$ of the equation $ax^2 - by^2 = c$. Now we can assume that the equation (3.1) has a primitive solution $\langle x_0, y_0 \rangle$ such that $(x_0, y_0) = 1$ and $(x_0, c) = 1$. Then there exists a solution $\langle x_1, y_1 \rangle$ given by (2.8). Since $(x_0, c) = 1$ then by Lemma 1 we obtain that there exists a singular solution $\langle u, v \rangle$ of (3.1).

By Lemma 2 it follows that there exists a solution in positive integers of the equation (3.2). The proof is complete.

4. Application

Let $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ be a given quadratic number field and let $h$ denote the class-number of this field. Then from well-known results of C. S. Herz [4], (Cf. [12], p. 483) it follows that if $h = 1$ then

$$d = p, \ 2q, \ qr$$

where $p$ is a prime and $q \equiv r \equiv 3 \pmod{4}$ are primes.

From this results follows that for the investigation of the famous Gauss problem concerning the existence of infinitely many real quadratic number fields with class-number $h = 1$ it suffices to consider one of the cases given in (4.1). Consider the case $d = p \equiv 3 \pmod{4}$. Then if $R_K$ is the ring of all integers of $K = \mathbb{Q}(\sqrt{p})$ and if $\alpha \in R$ then for some rational integers $x, y$ we have

$$\alpha = x + y\sqrt{p} \quad \text{and} \quad N(\alpha) = x^2 - py^2.$$

On the other hand it is well-known that if $D_K$ is the discriminant of $K$ then for every rational prime $q$ we have

$$q = P^2, \quad N(P) = q \quad \text{if} \quad q \mid D_K$$
and if \( q \nmid D_K \) then

\[
(q) = P_1P_2, \quad P_1 \neq P_2, \quad N(P_1) = N(P_2) = q \text{ if } \left( \frac{D_K}{q} \right) = +1
\]

\[
(q) = P, \quad N(P) = q^2 \text{ if } \left( \frac{D_K}{q} \right) = -1
\]

where \( P, P_1, P_2 \) are prime ideals in \( R_K \) and \( \left( \frac{q}{p} \right) \) denotes the Legendre symbol. In the case \( d = p \equiv 3 \pmod{4} \) we have \( D = 4d = 4p \). From (4.3) we have \( q = 2 \) or \( p \) and if \( P = (\alpha) \) then \( N(P) = N((\alpha)) = |N(\alpha)| \) and conversely. By (4.2) we obtain that this condition is equivalent to the condition that the equation \( |x^2 - py^2| = 2 \) or \( p \) has a solution in integers \( x, y \). But it is easy to see that the equation \( |x^2 - py^2| = p \) always has the solution \( x = 0, y = \pm 1 \) and it remains to investigate the equations

\[
x^2 - py^2 = 2, \quad x^2 - py^2 = -2.
\]

Let \( \langle u_0, v_0 \rangle \) be the primitive solutions of Pell’s equation \( u^2 - pv^2 = 1 \), then we have \( (u_0 - 1)(u_0 + 1) = pv_0^2 \) and we obtain

\[
p \mid u_0 - 1 \quad \text{or} \quad p \mid u_0 + 1.
\]

From (4.7) and Criterion 2 we get that one of the equations (4.6) has a solution in integers \( x, y \). Therefore we can investigate the cases (4.4) and (4.5). Similarly as in the above case we obtain that if one of the equations

\[
x^2 - py^2 = q, \quad x^2 - py^2 = -q.
\]

has a solution in integers \( x, y \) for every odd prime \( q \neq p \) such that \( \left( \frac{q}{p} \right) = -1 \) then every prime ideal \( P \) of \( R_K \) is principal and consequently any integer ideal is also principal and we get that in this case \( h = 1 \).

Applying our Theorem to (4.8) we get the following

**Corollary.** Let \( K = \mathbb{Q}(\sqrt{p}) \), where \( p \equiv 3 \pmod{4} \) is a prime. If the equation

\[
u^2 - pv^2 = q^2
\]

has an integer solution \( \langle u, v \rangle \) for every odd prime \( q \neq p \), such that \( \left( \frac{q}{p} \right) = +1 \), then \( h = 1 \).

**References**

On the Diophantine equation \( ax^2 - by^2 = c \)