Publ. Math. Debrecen
44 / 3-4 (1994), 291–299

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

$$ax^2 - by^2 = c\,. \tag{1.1}$$

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

$$S = \begin{bmatrix} \sqrt{a}\, x & \dfrac{d}{\sqrt{a}}\, y \\ \dfrac{1}{\sqrt{a}}\, y & \sqrt{a}\, x \end{bmatrix} \tag{2.1}$$

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

$$\det S = ax^2 - by^2 = c\,. \tag{2.2}$$

In the case $a = c = 1$ the solvable matrix S will be called Pell's solvable matrix. Hence

$$P = \begin{bmatrix} u & dv \\ v & u \end{bmatrix} \tag{2.3}$$

and

$$\det P = u^2 - dv^2 = 1\,. \tag{2.4}$$

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

$$S_0 = \begin{bmatrix} \sqrt{a}\, x_0 & \dfrac{d}{\sqrt{a}}\, y_0 \\ \dfrac{1}{\sqrt{a}}\, y_0 & \sqrt{a}\, x_0 \end{bmatrix} \tag{2.5}$$

$$P_0 = \begin{bmatrix} u_0 & dv_0 \\ v_0 & u_0 \end{bmatrix} \tag{2.6}$$

From (2.5) and (2.6) we obtain

$$S_1 = S_0 P_0 = P_0 S_0 = \begin{bmatrix} \sqrt{a}\, x_1 & \dfrac{d}{\sqrt{a}}\, y_1 \\ \dfrac{1}{\sqrt{a}}\, y_1 & \sqrt{a}\, x_1 \end{bmatrix} \tag{2.7}$$

where

$$x_1 = x_0 u_0 + b y_0 v_0, \quad y_1 = y_0 u_0 + a x_0 v_0\,. \tag{2.8}$$

From (2.7) and Cauchy's Theorem on the product of determinants we get

$$\det S_1 = \det S_0 \cdot \det P_0 = \det P_0 \cdot \det S_0 = a x_1^2 - b y_1^2 = c\,, \tag{2.9}$$

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

$$x_0 < u < x_1 \tag{2.10}$$

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

$$u = x_0 u_0 - b y_0 v_0, \quad v = y_0 u_0 - a x_0 v_0\,. \tag{2.11}$$

It is easy to see that by (2.6) we have

$$P_0^{-1} = \begin{bmatrix} u_0 & -dv_0 \\ -v_0 & u_0 \end{bmatrix} \tag{2.12}$$

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

$$u = x_0u_0 - by_0v_0 > \sqrt{ab}\, v_0x_0 - by_0v_0 = v_0\sqrt{b}\,(\sqrt{a}\, x_0 - \sqrt{b}y_0).$$

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

$$0 < u < x_1\,. \tag{2.13}$$

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 $u^2 = c$ concradicting 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

$$x_0 \leq u < x_1\,. \tag{2.14}$$

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

$$x_0(u_0 - 1) = by_0v_0\,. \tag{2.15}$$

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

$$ax^2 - b(ax_0v_0 - y_0u_0)^2 = c\,.$$

From the last equality we obtain

$$ax_0^2 - ax_0^2(abv_0^2) + 2au_0x_0(by_0v_0) - u_0^2(by_0^2) = c\,. \tag{2.16}$$

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) in to (2.16) we obtain

$$ax_0^2 - ax_0^2(u_0^2 - 1) + 2au_0x_0^2(u_0 - 1) - u_0^2(ax_0^2 - c) = c\,. \tag{2.17}$$

From (2.17) we get

$$2ax_0^2 - 2ax_0^2u_0 = c(1 - u_0^2)$$

and consequently

$$2ax_0^2(1 - u_0) = c(1 - u_0)(1 + u_0).$$

Since $u_0 \neq 1$, the last equality implies

$$2ax_0^2 = c(u_0 + 1). \tag{2.18}$$

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 $R = S_1S_2 = S_2S_1$ has the form*

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

where

$$x_3 = ax_1x_2 + by_1y_2, \quad y_3 = x_1y_2 + y_1x_2$$

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

$$R = S_1S_2 = S_2S_1 = \begin{bmatrix} \sqrt{a}\,x_1 & \dfrac{d}{\sqrt{a}}\,y_1 \\ \dfrac{1}{\sqrt{a}}\,y_1 & \sqrt{a}\,x_1 \end{bmatrix} \cdot \begin{bmatrix} \sqrt{a}\,x_2 & \dfrac{d}{\sqrt{a}}\,y_2 \\ \dfrac{1}{\sqrt{a}}\,y_2 & \sqrt{a}\,x_2 \end{bmatrix}. \tag{2.19}$$

From (2.19) we get

$$R = \begin{bmatrix} ax_1x_2 + by_1y_2 & d(x_1y_2 + y_1x_2) \\ x_1y_2 + y_1x_2 & ax_1x_2 + by_1y_2 \end{bmatrix}. \tag{2.20}$$

Putting in (2.20)

$$x_3 = ax_1x_2 + by_1y_2, \quad y_3 = x_1y_2 + y_1x_2 \tag{2.21}$$

we get

$$R = \begin{bmatrix} x_3 & dy_3 \\ y_3 & x_3 \end{bmatrix}. \tag{2.22}$$

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

$$\det R = \det S_1 \cdot \det S_2 = c^2\,. \tag{2.23}$$

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

$$x = \tfrac{1}{2}(am^2 + bn^2)\varrho, \quad y = mn\varrho, \quad z = \tfrac{1}{2}(am^2 - bn^2)\varrho$$

if $d = ab$ is odd and ϱ is any integer when m and n are odd, but ϱ 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

$$ax^2 - by^2 = c \tag{3.1}$$

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

$$u^2 - dv^2 = c^2 \tag{3.2}$$

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

$$u = (am^2 + bn^2)\varrho, \quad v = 2mn\varrho, \quad c = (am^2 - bn^2)\varrho \tag{3.3}$$

if $d = ab$ is even, or

$$u = \tfrac{1}{2}(am^2 + bn^2)\varrho, \quad v = mn\varrho, \quad c = \tfrac{1}{2}(am^2 - bn^2)\varrho \tag{3.4}$$

if $d = ab$ is odd, where ϱ is any integer when m and n are odd, but ϱ 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

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

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 $K = Q(\sqrt{d})$, $d > 0$ 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

$$d = p, \ 2q, \ qr \tag{4.1}$$

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 $K = Q(\sqrt{p})$ and if $\alpha \in R$ then for some rational integers x, y we have

$$\alpha = x + y\sqrt{p} \quad \text{and} \quad N(\alpha) = x^2 - py^2\,. \tag{4.2}$$

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

$$(q) = P^2, \quad N(P) = q \ \text{ if } \ q \mid D_K \tag{4.3}$$

and if $q \nmid D_K$ then

$$(4.4)\quad (q) = P_1 P_2, \quad P_1 \neq P_2, \quad N(P_1) = N(P_2) = q \text{ if } \left(\frac{D_K}{q}\right) = +1$$

$$(4.5)\quad (q) = P, \quad N(P) = q^2 \text{ if } \left(\frac{D_K}{q}\right) = -1$$

where P, P_1, P_2 are prime ideals in R_K and $\left(\frac{a}{b}\right)$ 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 $|x^2 - py^2| = p$ has always the solution $x = 0$, $y = \pm 1$ and it remains to investigate the equations

$$(4.6)\quad x^2 - py^2 = 2, \quad x^2 - py^2 = -2\,.$$

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

$$(4.7)\quad p \mid u_0 - 1 \quad \text{or} \quad p \mid u_0 + 1\,.$$

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

$$(4.8)\quad x^2 - py^2 = q, \quad x^2 - py^2 = -q\,.$$

has a solution in integers x, y for every odd prime $q \neq p$ such that $\left(\frac{D_K}{q}\right) = \left(\frac{p}{q}\right) = +1$ 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 $K = Q(\sqrt{p}\,)$, 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

[1] L. E. Dickson, Introduction to the Theory of Numbers, *New York*, 1957.

[2] W. Górzny, On the equation $D_1 x^2 - D_2 y^2 = 1$, *Discuss. Math.* **4** (1981), 109–111.

[3] A. Grelak and A. Grytczuk, Some remarks on matrices and Diophantine equation $A^2 - By^2 = C$, *Discuss. Math.* **10** (1990), 13–27.

[4] C. S. Herz, Construction of class fields, Seminar on Complex Multiplication, Lectures Notes in Math. 21, *Springer– Verlag*, 1966.
[5] C. U. Jensen, On the solvability of a certain class of non-Pellian equations, *Math. Scand.* **10** (1962), 71–84.
[6] P. Kaplan, A propos des équations antipelliennes, *Enseign. Math.* (1983), 323–328.
[7] J. C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, *Trans. Amer. Math. Soc.* **260** (1980), 485–508.
[8] H. Lienen, The quadratic form $x^2 - 2py^2$, *J. Number Theory* (1978), 10–15.
[9] T. Nagell, On a special class of Diophantine equations of the second degree, *Arkiv. Math.* (1954), 51–65.
[10] T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Soc. Sci. Uppsala* (1955), 1–38.
[11] T. Nagell, Sur la solubilité en nombres entiers des équations du second degré a deux inderterminées, *Acta Arith.* (1971), 105–114.
[12] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, *PWN, Warszawa*, 1990.

A. GRELAK
DEPARTMENT OF MATHEMATICS
PEDAGOGICAL UNIVERSITY
ZIELONA GÓRA
POLAND

A. GRYTCZUK
DEPARTMENT OF MATHEMATICS
PEDAGOGICAL UNIVERSITY
ZIELONA GÓRA
POLAND

(Received November 10, 1992; revised March 26, 1993)