IJMMS 2003:35, 2241–2253
PII. S0161171203204348
http://ijmms.hindawi.com

THE DIOPHANTINE EQUATION $ax^2 + 2bxy - 4ay^2 = \pm 1$

LIONEL BAPOUNGUÉ

Received 30 April 2002

We discuss, with the aid of arithmetical properties of the ring of the Gaussian integers, the solvability of the Diophantine equation $ax^2 + 2bxy - 4ay^2 = \pm 1$, where a and b are nonnegative integers. The discussion is relative to the solution of Pell's equation $v^2 - (4a^2 + b^2)w^2 = -4$.

2000 Mathematics Subject Classification: 11D09.

1. Introduction. The objective of this paper is the expansion and also the extension of [1, Section 2]. More precisely, it deals with the complete treatment of the solvability of the Diophantine equation

$$ax^2 + 2bxy - 4ay^2 = \pm 1, \tag{1.1}$$

where a and b are positive integers. From [2, Proposition 1], (1.1) is always solvable if $a = 1$. Hence, we may assume that $a > 1$. Moreover, we restrict oneself to $\gcd(a, 2b) = 1$. In the opposite case, (1.1) is insolvable.

We denote by $\delta = 4a^2 + b^2$ the discriminant of the quadratic form $ax^2 + 2bxy - 4ay^2$.

If $a > 1$, $b \geq 0$, and $\gcd(a, 2b) = 1$, [2, Theorem 1] shows that (1.1) is insolvable if δ is a square in $\mathbb{Z}$. Hence, we will assume also that $\delta = 4a^2 + b^2$ is a nonsquare in $\mathbb{Z}$, which requires b to be odd. Then δ verifies $\delta \equiv 5 \pmod 8$. Thus, (cf. [4]) the algebraic integers of $\mathbb{Q}(\sqrt{\delta})$ are the numbers $(1/2)(v + w\sqrt{\delta})$ with $v, w \in \mathbb{Z}$ of the same parity. Consequently, if $(1/2)(v + w\sqrt{\delta})$ is a unit of $\mathbb{Q}(\sqrt{\delta})$, we must have

$$v^2 - \delta w^2 = \pm 4. \tag{1.2}$$

Conversely, if (v, w) is an integer solution of (1.2), then $(1/2)(v + w\sqrt{\delta})$ is an integer of $\mathbb{Q}(\sqrt{\delta})$ (its trace is v and its norm, by (1.2), is ± 1) and, hence, a unit of $\mathbb{Q}(\sqrt{\delta})$. Writing $(1/2)(v_0 + w_0\sqrt{\delta})$ for the fundamental unit of $\mathbb{Q}(\sqrt{\delta})$, we see that the solutions in pairs of natural numbers (v, w) of (1.2) comprise the values of the sequence (v_n, w_n) $(n \geq 1)$ defined by setting

$$\frac{1}{2}\left(v_n + w_n\sqrt{\delta}\right) = \left(\frac{v_0 + w_0\sqrt{\delta}}{2}\right)^n. \tag{1.3}$$

Hence, we remark easily (cf. [2]) that if (x,y) is a solution of (1.1), then

$$v = -bx^2 + 8axy + 4by^2, \qquad w = x^2 + 4y^2 \tag{1.4}$$

verify with $\delta = 4a^2 + b^2$ ($a > 1$, $b \geq 1$, and $\gcd(a,2b) = 1$) the Pell's equation

$$v^2 - \delta w^2 = -4 \quad \text{with } v,w \text{ odd.} \tag{1.5}$$

Hence, our study will be based on (1.5). Thus, assuming its solvability, we give in Section 2 a necessary and sufficient condition for (1.1) to be solvable (Theorem 2.3) by methods using the arithmetic of the order $\mathbb{Z}[2i]$ of index 2, included in the principal ring $\mathbb{Z} + \mathbb{Z}[i]$. In the remainder of Section 2, we establish that if (1.1) is solvable, then $\pm a$ is the norm of an element of $\mathbb{Z}[\sqrt{\delta}]$ (Proposition 2.6). Next, we prove in Section 3 that when δ is given, among all the pairs of positive coprime odd integers (a,b) satisfying $\delta = 4a^2 + b^2$, there is exactly one pair for which (1.1) is solvable (Theorem 3.1). That unique pair will be constructed (Theorem 4.1) in Section 4 with the aid of the following result proved in [5].

Theorem 1.1 (Thue). *If α and δ are integers satisfying $\delta > 1$, $\gcd(\alpha,\delta) = 1$, and m the least integer greater than $\sqrt{\delta}$, there exist x and y in $]0,m[$ such that $\alpha y \equiv \pm x \pmod{\delta}$.*

When solutions exist, we show using any of them in Section 5 that (1.1) possesses an infinity of solutions (Theorem 5.1); afterwards, we describe using it a family (Proposition 5.2). We give the conclusion of our paper in Section 6 with some numerical examples.

2. The case $a > 1$, δ odd nonsquare, and (1.5) solvable with v, w odd

2.1. Preliminaries. Let v, w be *odd* integers greater than or equal to 1 such that $v^2 - \delta w^2 = -4$. It is clear that

$$\gcd(v,w) = 1 \tag{2.1}$$

because if v and w have a common prime factor d, then d divides $v^2 - \delta w^2 = -4$ and, therefore, d divides also 2. Write (1.5) in the form

$$\delta w^2 = (v+2i)(v-2i). \tag{2.2}$$

The two factors of the right-hand side of (2.2) are relatively prime in $\mathbb{Z}[i]$ since any common divisor would divide $4i$, but w is *odd*, hence, $\gcd(w,4i) = 1$. Hence, in $\mathbb{Z}[i]$, we have

$$\gcd(v+2i, v-2i) = 1. \tag{2.3}$$

Moreover, since (1.5) is written in the form (2.2), we will manipulate the elements of the nonmaximal order $\mathbb{Z}[2i]$ of index 2, for which we have shown in [3] that the half group **F** defined by

$$\mathbf{F}=\{v+2i\in\mathbb{Z}[2i]:\gcd(N(v+2i),2)=1\} \tag{2.4}$$

is factorial, where $N(\alpha)$ denotes the norm of α. Thus, the remark of [2, Proposition 4] applied to **F** enables us to state the following definition.

Definition 2.1. An odd solution $(v,w)\in\mathbb{Z}^2$ of (1.5) is said to be
(i) violain if, in **F**, $b+2ai$ divides $v+2i$ or $v-2i$;
(ii) monic if, in **F**, $b+2ai=\gcd(v+2i,\delta)$ or $\gcd(v-2i,\delta)$.

Proposition 2.2. *Any odd violain solution $(v,w)\in\mathbb{Z}^2$ of (1.5) is monic.*

2.2. One criterion of solvability for (1.1). We prove the following theorem.

Theorem 2.3. *If $a\geq 3$ and $b\geq 1$ are odd integers with $\gcd(a,2b)=1$ and $\delta=4a^2+b^2$ nonsquare in $\mathbb{Z}$, the following statements are equivalent:*
(i) *(1.1) has a solution $(x,y)\in\mathbb{Z}^2$;*
(ii) *(1.5) has an odd violain solution $(v,w)\in\mathbb{Z}^2$;*
(iii) *the odd minimal solution $(v_0,w_0)\in\mathbb{Z}^2$ $(v_0>0,\ w_0>0)$ of (1.5) is monic.*

Proof. (i)⇒(ii). Let $(x,y)\in\mathbb{Z}^2$ be a solution of (1.1). We set

$$\begin{gathered}\varepsilon=\operatorname{sgn}(ax^2+2bxy-4ay^2),\\ v=\varepsilon(bx^2-8axy-4by^2),\qquad w=x^2+4y^2.\end{gathered} \tag{2.5}$$

As b and x are odd, v and w are also odd. Then we have

$$v+2i=\varepsilon(bx^2-8axy-4by^2)+2\varepsilon(ax^2+2bxy-4ay^2)i \tag{2.6}$$

so that

$$v+2i=\varepsilon(b+2ai)(x+2iy)^2, \tag{2.7}$$

where we see that $(v,w)\in\mathbb{Z}^2$ is an odd violain solution of (1.5). Further, taking the norm of the two sides of (2.7), we obtain

$$v^2+4=(b^2+4a^2)(x^2+4y^2)^2=\delta w^2 \tag{2.8}$$

so that (v,w) is an odd integer solution of (1.5).

(ii)⇒(iii). Let $(v,w)\in\mathbb{Z}^2$ be an odd integer violain solution of (1.5). Then from equality (2.7), we have

$$\gcd(v+2i,\delta)=(b+2ai)\gcd((x+2iy)^2,b-2ai). \tag{2.9}$$

Now, we show that

$$\gcd((x+2iy)^2,b-2ai)=1. \tag{2.10}$$

If there exists $\alpha \in \mathbf{F}$, α is not a unit, that is, $\alpha \neq \pm 1$ such that

$$\alpha | x + 2iy, \qquad \alpha | b - 2ai, \tag{2.11}$$

then as (2.7) implies

$$v = \varepsilon(bx^2 - 8axy - 4by^2), \qquad w = x^2 + 4y^2, \tag{2.12}$$

we deduced that, in $\mathbf{F}$,

$$\begin{aligned} v &\equiv \varepsilon[b(-2iy)^2 - 8a(-2iy)y - 4by^2] \\ &\equiv -8\varepsilon y^2(b - 2ai) \equiv 0 (\bmod \alpha), \\ w &\equiv 0 (\bmod \alpha), \end{aligned} \tag{2.13}$$

that is, α is also a divisor of v and w, contradicting the fact that $\gcd(v,w) = 1$ according to (2.1). Hence, we have

$$\gcd(v + 2i, \delta) = b + 2ai. \tag{2.14}$$

Then we show that (2.14) is true for v_0 arising from the odd minimal solution of (1.5). As (v,w) is an odd solution of (1.5), we have by the theory of the Pellian equation

$$\frac{v + w\sqrt{\delta}}{2} = \begin{cases} \left(\dfrac{v_0 + w_0\sqrt{\delta}}{2}\right)^{2n+1}, & \text{if } v > 0, \\ -\left(\dfrac{v_0 - w_0\sqrt{\delta}}{2}\right)^{2n+1}, & \text{if } v < 0, \end{cases} \tag{2.15}$$

for some integer $n \geq 0$. Developing (2.15), we obtain

$$4^n v = \begin{cases} v_0^{2n+1} + \dbinom{2n+1}{2} v_0^{2n-1} w_0^2 \delta + \cdots, & \text{if } v > 0, \\ -v_0^{2n+1} - \dbinom{2n+1}{2} v_0^{2n-1} w_0^2 \delta - \cdots, & \text{if } v < 0, \end{cases} \tag{2.16}$$

where the terms are all divisible by δ except v_0^{2n+1}. Hence, as $v_0^2 \equiv -4 (\bmod \delta)$, we have

$$v \equiv \begin{cases} (-1)^n v_0 (\bmod \delta), & \text{if } v > 0, \\ (-1)^{n+1} v_0 (\bmod \delta), & \text{if } v < 0. \end{cases} \tag{2.17}$$

From (2.14) and (2.17), we deduce that

$$b + 2ai = \gcd(v + 2i, \delta) = \gcd(\pm v_0 + 2i, \delta) = \gcd(v_0 \pm 2i, \delta) \tag{2.18}$$

as required. This proves that (v_0, w_0) is a monic solution of (1.5).

(iii)⇒(i). Suppose that (v_0,w_0) is a monic solution of (1.5). The equality

$$v_0^2-\delta w_0^2=-4 \tag{2.19}$$

may be expressed in the form

$$\left(\frac{v_0+2i}{b+2ai}\right)\left(\frac{v_0-2i}{b-2ai}\right)=w_0^2, \tag{2.20}$$

where, from (2.3), $(v_0+2i)/(b+2ai)$ and $(v_0-2i)/(b-2ai)$ are coprime in $\mathbf{F}$. Hence, for some unit $\varepsilon=\pm 1$ and integers x, y, we have

$$\frac{v_0+2i}{b+2ai}=\varepsilon(x+2iy)^2, \qquad w_0=x^2+4y^2. \tag{2.21}$$

Taking

$$v_0+2i=\varepsilon(b+2ai)(x+2iy)^2 \tag{2.22}$$

and equating coefficients of i on both sides of (2.22), we obtain

$$ax^2+2bxy-4ay^2=\varepsilon, \tag{2.23}$$

showing that $(x,y)\in\mathbb{Z}^2$ is a solution of (1.1). □

Remark 2.4. The proof above also confirms the following result.

Theorem 2.5. *If $a\geq 3$ and $b\geq 1$ are odd integers with $\gcd(a,2b)=1$ and $\delta=4a^2+b^2$ nonsquare in $\mathbb{Z}$, the following statements are equivalent:*

(i) *(1.1) has a solution $(x,y)\in\mathbb{Z}^2$;*

(ii) *(1.5) has an odd violain solution $(v,w)\in\mathbb{Z}^2$;*

(iii) *(1.5) has an odd monic solution $(v,w)\in\mathbb{Z}^2$.*

We have also the following proposition.

Proposition 2.6. *Let $a\geq 3$ and $b\geq 1$ be odd integers with $\gcd(a,2b)=1$ and $\delta=4a^2+b^2$ nonsquare in $\mathbb{Z}$. If the Diophantine equation (1.1) has any solution $(x,y)\in\mathbb{Z}^2$, then*

$$a=\pm N(y\sqrt{\delta}+\mu) \qquad \text{or} \qquad \pm\frac{1}{4}N(x\sqrt{\delta}+\sigma), \quad \mu,\sigma\in\mathbb{Z}. \tag{2.24}$$

In other words, $\pm a$ (resp., $\pm 4a$) is the norm of an element of $\mathbb{Z}[\sqrt{\delta}]$.

Proof. We suppose that $(x,y)\in\mathbb{Z}^2$ is any solution of (1.1). Then the equation

$$at^2+2bty-4ay^2-\varepsilon=0 \quad (\varepsilon=\pm 1) \tag{2.25}$$

has an integer root, hence its discriminant is a square in $\mathbb{Z}$:

$$b^2y^2+4a^2y^2-\varepsilon a=\mu^2, \quad \mu\in\mathbb{Z}, \tag{2.26}$$

whence

$$\varepsilon a = y^2(b^2+4a^2)-\mu^2 = \delta y^2-\mu^2, \quad \mu \in \mathbb{Z}, \tag{2.27}$$

so that

$$\varepsilon a = N(y\sqrt{\delta}+\mu), \quad \mu \in \mathbb{Z}. \tag{2.28}$$

Exchanging the roles of x and y, we obtain also

$$4\varepsilon a = N(x\sqrt{\delta}+\sigma), \quad \sigma \in \mathbb{Z}. \tag{2.29}$$

□

3. Uniqueness of the pair (a,b), δ given. We assume in this section that δ is given and can be factorized into several sums of two squares in $\mathbb{Z}$. Then we use Theorem 2.3 to show that among all the pairs of positive integers (a,b), there is exactly one pair for which (1.1) is solvable.

Theorem 3.1. *Let δ be an odd nonsquare positive integer for which (1.5) has an odd solution $(v,w) \in \mathbb{Z}^2$. Then among all the pairs of odd positive coprime integers (a,b) satisfying $\delta = 4a^2+b^2$, there is exactly one pair $(a,b) = (A,B)$ such that (1.1) is solvable.*

Proof. Let $(v,w) \in \mathbb{Z}^2$ be any odd violain solution of (1.5). We define positive integers A and B as follows:

$$A = |a|, \qquad B = b. \tag{3.1}$$

Let $g = \gcd(a,b)$. Then

$$v+2i = g(\alpha+2i\beta) \Longrightarrow 1 = g\beta, \tag{3.2}$$

hence $g = 1$. Since $(v,w) \in \mathbb{Z}^2$ is an odd solution of (1.5), we have $\delta \equiv 5 \pmod 8$, and thus a and b are odd. Hence, we have

$$\gcd(A,B) = 1 \tag{3.3}$$

with both A and B all odd. Then we show that $\delta = 4A^2+B^2$.

From the definition of A and B, we see that $B+2Ai \mid v+2i$ or $v-2i$. Hence, we may assume, for example, that $B+2Ai \mid v+2i$. Then (1.5) may be expressed in the form

$$\frac{v+2i}{B+2Ai}(v-2i) = \frac{\delta}{B+2Ai}w^2, \tag{3.4}$$

where $(v+2i)/(B+2Ai)$ and $\delta/(B+2Ai)$ are coprime elements of **F** (since v, δ, and B are odd). Equation (3.4) shows that $\delta/(B+2Ai)$ divides $v-2i$, but

$\delta/(B+2Ai)$ also divides δ, therefore $\delta/(B+2Ai)$ divides

$$\gcd(v-2i,\delta)=B-2Ai, \tag{3.5}$$

in **F**, and so

$$\delta \mid B^2+4A^2. \tag{3.6}$$

On the other hand, since $B+2Ai\mid\delta$, taking conjugates, we obtain $B-2Ai\mid\delta$. Let $\pi\in\mathbb{Z}[i]$ be any prime factor of $B+2Ai$ and $B-2Ai$. Then we have

$$\frac{B^2+4A^2}{\pi}\,\bigg|\,\delta. \tag{3.7}$$

Since (v,w) is any odd violain solution of (1.5), we have

$$\pi\,\bigg|\,\frac{v+2i}{B+2Ai}, \qquad \pi\,\bigg|\,\frac{v-2i}{B-2Ai}, \tag{3.8}$$

and as $v\equiv B(\bmod 2)$, [2, Lemma 2] applied to $\mathbb{Z}[i]$ shows that $\pi=1$, then the relation (3.7) becomes

$$B^2+4A^2\mid\delta. \tag{3.9}$$

Thus, $\delta=4A^2+B^2$ follows from (3.6) and (3.9). Hence, $\delta=4A^2+B^2$ is a decomposition of δ which satisfies statement (ii) of Theorem 2.3. So, by Theorem 2.3, the equation

$$Ax^2+2Bxy-4Ay^2=\pm 1 \tag{3.10}$$

is solvable. A and B are unique. □

Applying Theorems 2.3 (or 2.5) and 3.1, we obtain the following corollary.

Corollary 3.2. *If $\delta\equiv 5(\bmod 8)$ is a prime number for which (1.5) is solvable, d, e denote integers such that $\delta=4d^2+e^2$ (they are odd, unique, and positive), then the Diophantine equation*

$$dx^2+2exy-4dy^2=\pm 1 \tag{3.11}$$

is solvable.

Proof. This results from the fact that any prime number δ of the form $4m+1$ may be represented as the sum of two squares (cf. [5]). □

4. Construction of (A,B), δ given. We show in this section how the pair (A,B) can be constructed.

Theorem 4.1. *Let δ be an odd nonsquare positive integer such that (1.5) is solvable in odd integers $(v,w)\in\mathbb{Z}^2$. Then there exists a unique pair of coprime odd integers (a,b) satisfying*

$$\begin{gathered} b\pm av\equiv 0(\operatorname{mod}\delta),\\ 0<a<\sqrt{\delta},\qquad 0<b<\sqrt{\delta},\\ \delta=4a^2+b^2. \end{gathered}\tag{4.1}$$

Then, for that unique pair (a,b), (1.1) is solvable in $(x,y)\in\mathbb{Z}^2$.

Proof. Taking $\alpha=v$ in Theorem 1.1, we see that there exist integers $a>0$ and $b>0$ such that

$$b\pm av\equiv 0(\operatorname{mod}\delta),\quad a<\sqrt{\delta},\ b<\sqrt{\delta}.\tag{4.2}$$

Since $(v,\delta)=1$, we have

$$b^2+4a^2\equiv a^2v^2+4a^2\equiv -4a^2+4a^2\equiv 0(\operatorname{mod}\delta).\tag{4.3}$$

But $0<b^2+4a^2<5\delta$, hence the equations

$$b^2+4a^2=2\delta,3\delta,4\delta\tag{4.4}$$

are insolvable in $\mathbb{Z}$ since, modulus 4, the first and the second congruences $b^2\equiv 2,3$ are impossible and the third imposes b to be even. Hence, we have

$$\delta=4a^2+b^2,\tag{4.5}$$

which verifies $\delta\equiv 5(\operatorname{mod}8)$ since $(v,w)\in\mathbb{Z}^2$ is an odd solution of (1.5), and thus a and b are both odd.

Next, we show that if (a,b) satisfies (4.2) and (4.5), then $\gcd(a,b)=1$.

Let $g=\gcd(a,b)$, and set $a=ga'$, $b=gb'$. Then (4.5) becomes

$$(b')^2+4(a')^2=\delta_1\tag{4.6}$$

with $\delta_1=\delta/g^2$. Relations (4.2) show that there exists $\lambda\in\mathbb{Z}$ such that $b=\pm av+\lambda\delta$, and thus $b'=\pm a'v+\lambda g\delta_1$. Replacing b' in (4.6), we obtain

$$(\pm a'v+\lambda g\delta_1)^2+4(a')^2=\delta_1,\tag{4.7}$$

and, using (1.5), we deduce from it that

$$g(w^2(a')^2\pm 2a'\lambda v+\lambda^2 g\delta_1)=1,\tag{4.8}$$

proving that $g=1$.

Now, we show that (a,b) is unique. We suppose that (a_1,b_1) is another solution of (4.2). Then from congruences

$$b+av \equiv b_1+a_1v \equiv 0 (\bmod \delta) \tag{4.9}$$

or

$$b-av \equiv b_1-a_1v \equiv 0 (\bmod \delta), \tag{4.10}$$

we see that

$$bb_1+4aa_1 \equiv 0 (\bmod \delta), \qquad ab_1-a_1b \equiv 0 (\bmod \delta). \tag{4.11}$$

From the product of the two following expressions:

$$b^2+4a^2=\delta, \qquad b_1^2+4a_1^2=\delta, \tag{4.12}$$

we deduce that

$$(bb_1+4aa_1)^2+4(ab_1-a_1b)^2=\delta^2 \tag{4.13}$$

so that (dividing by δ^2)

$$\left(\frac{bb_1+4aa_1}{\delta}\right)^2+4\left(\frac{ab_1-a_1b}{\delta}\right)^2=1, \tag{4.14}$$

which gives

$$bb_1+4aa_1=\pm\delta, \qquad ab_1-a_1b=0. \tag{4.15}$$

Relations (4.15) impose

$$(a_1,b_1)=\pm(a,b). \tag{4.16}$$

Thus, there exists a unique solution of (4.2) satisfying $a>0$, $b>0$.

Finally, our last assertion is to prove that (a,b) defined by (4.1) satisfies Theorem 2.3(ii). We suppose that

$$b\pm av \equiv 0 (\bmod \delta). \tag{4.17}$$

As $v^2 \equiv -4 (\bmod \delta)$, multiplying (4.17) by v, we obtain

$$bv \equiv \pm av^2 \equiv \pm 4a (\bmod \delta), \tag{4.18}$$

and so

$$\frac{v\pm 2i}{b+2ai}=\frac{bv\pm 4a}{\delta}-2\left(\frac{\pm b+av}{\delta}\right)i \tag{4.19}$$

is an element of **F**. Thus

$$b+2ai \mid v \pm 2i. \tag{4.20}$$

This proves that (v,w) is an odd violain solution of (1.5). So, from Theorem 2.3, (1.1) is solvable in integers $(x,y)\in\mathbb{Z}^2$. □

Remark 4.2. Denoting by (v_0,w_0) the odd minimal solution of (1.5), we can easily determine A and B, such that $B+2Ai$ is the $\gcd(v_0\pm 2i,\delta)$, using the following algorithm:

(1) (i) factorize δ in $\mathbb{Z}$;
  (ii) calculate the norm of v_0+2i and factorize it in $\mathbb{Z}$;
(2) factorize the prime factors obtained in **F**;
(3) deduce from (2) the common divisors of δ and v_0+2i.

5. Complete set of solutions of (1.1). First of all, we prove the following theorem.

Theorem 5.1. *Under the conditions of Theorem 2.3, the Diophantine equation (1.1) has an infinity of solutions in $\mathbb{Z}$.*

Proof. We assume that (1.1) has a solution $(x_0,y_0)\in\mathbb{Z}^2$. Then we have $\gcd(x_0,y_0)=1$, hence there exists $(a,b)\in\mathbb{Z}^2$ such that

$$ax_0+by_0=1. \tag{5.1}$$

We set

$$\begin{gathered}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x_0 & -\beta\\ y_0 & \alpha\end{pmatrix}\begin{pmatrix}X\\Y\end{pmatrix},\\ g(X,Y)=f(x,y)=ax^2+2bxy-4ay^2.\end{gathered} \tag{5.2}$$

Then g and f are two equivalent quadratic forms. Further

$$g(X,Y)=\varepsilon X^2-2BXY-CY^2,\quad B,C\in\mathbb{Z}, \tag{5.3}$$

with

$$\begin{aligned}\varepsilon&=ax_0^2+2bx_0y_0-4ay_0^2,\\ B&=(a\beta-b\alpha)x_0+(b\beta+4a\alpha)y_0,\\ C&=a\beta^2+2b\alpha\beta+4a\alpha^2.\end{aligned} \tag{5.4}$$

But the equations

$$f(x,y)=\varepsilon,\qquad g(X,Y)=\varepsilon \tag{5.5}$$

are equivalent, hence as

$$g(X,Y)=\varepsilon N(X-\theta Y), \tag{5.6}$$

where θ is a root of the equation

$$t^2-\varepsilon Bt+\varepsilon C=0, \tag{5.7}$$

we conclude that if $f(x,y)=\varepsilon$ has a solution in $\mathbb{Z}$, it has an infinity of solutions in $\mathbb{Z}$. □

Now, we describe the family of solutions of (1.1).

Proposition 5.2. *Under the conditions of Theorem 2.3, let (x_0,y_0) be a particular solution of (1.1). Then the set of solutions (x,y) of (1.1) is given by*

$$ax+by+y\sqrt{\delta}=\pm\left(\frac{v_0+w_0\sqrt{\delta}}{2}\right)^{3n}(ax_0+by_0+y_0\sqrt{\delta}) \tag{5.8}$$

in which (v_0,w_0) is the minimal solution of (1.5) and $n\in\mathbb{Z}$.

Proof. Let (x_0,y_0) be a particular solution of (1.1). We show how all the solutions (x,y) of (1.1) may be obtained in terms of (x_0,y_0) and the minimal solution (v_0,w_0) of (1.5). If (x,y) is any solution of (1.1) and if we set

$$J=\frac{ax+by+y\sqrt{\delta}}{ax_0+by_0+y_0\sqrt{\delta}}, \tag{5.9}$$

the norm of J is

$$\frac{(ax+by)^2-\delta y^2}{(ax_0+by_0)^2-\delta y_0^2}=\frac{a(ax^2+2bxy-4ay^2)}{a(ax_0^2+2bx_0y_0-4ay_0^2)}, \tag{5.10}$$

that is, ± 1.

Moreover, J is of the form $D+E\sqrt{\delta}$, where D and E are integers given by

$$\begin{aligned} D&=axx_0+b(xy_0+x_0y)-4ayy_0,\\ E&=x_0y-xy_0. \end{aligned} \tag{5.11}$$

Hence, by the theory of the Pellian equation, we have

$$J=\pm\left(\frac{v_0+w_0\sqrt{\delta}}{2}\right)^{3n}, \tag{5.12}$$

where $n\in\mathbb{Z}$. Thus, we have shown the existence of an integer n such that we have (5.8).

Conversely, let x and y be defined by (5.8) for some $n\in\mathbb{Z}$. Taking norms of both sides of (5.8), we see that x and y verify (1.1). It remains to show that they are both integers.

Define integers M and N by

$$M+N\sqrt{\delta} = \pm\left(\frac{v_0+w_0\sqrt{\delta}}{2}\right)^{3n}. \tag{5.13}$$

Then equating coefficients in (5.8), we obtain

$$\begin{aligned} ax+by &= M(ax_0+by_0)+\delta N y_0, \\ y &= My_0+N(ax_0+by_0). \end{aligned} \tag{5.14}$$

Clearly, $y \in \mathbb{Z}$. Using $\delta = 4a^2 + b^2$, we obtain

$$x = (M-bN)x_0+4aNy_0, \tag{5.15}$$

so that x is also an integer. □

6. Numerical examples

Example 6.1. If $a = 19$ and $b = 71$, then $\delta = 4(19)^2+71^2 = 6485 \equiv 5 (\bmod 8)$ is nonsquare such that $(v_0,w_0) = (1369,17)$ is the minimal solution of (1.5). In this case, $\gcd(1369+2i, 6485) = 71+38i$ and Theorem 2.3 shows that (1.1) is solvable; in fact, it is $19x^2+142xy-76y^2 = -1$ ($(x,y) = (1,2)$ is a solution).

Example 6.2. If $a = 3$ and $b = 5$, then $\delta = 4(3)^2 + 5^2 = 61 \equiv 5 (\bmod 8)$ is prime such that $(v,w) = (39,5)$ is a solution of (1.5); Corollary 3.2 shows that (1.1) is solvable; in fact, it is $3x^2+10xy-12y^2 = 1$ ($(x,y) = (1,1)$ is a solution).

Example 6.3. In case $\delta = 2941 = 4(25)^2+21^2 = 4(27)^2+5^2$, we have $\delta \equiv 5 (\bmod 8)$ nonsquare such that $(v_0,w_0) = (705,13)$ is the minimal solution of (1.5). As $\gcd(7054+2i, 2941) = 21-50i$, Theorems 2.3 and 3.1 show that (1.1) is solvable only in the case when $(a,b) = (25,21)$; in fact, it is $25x^2+42xy-100y^2 = -1$ ($(x,y) = (-3,1)$ is a solution).

The equation $27x^2+10xy-108y^2 = \pm 1$ is insolvable.

Example 6.4. Take $\delta = 3077$. We have $\delta \equiv 5 (\bmod 8)$ nonsquare such that $(v_0,w_0) = (943,17)$ is the minimal solution of (1.5). The candidates for the unique pair (a,b) satisfying (4.1) must be solutions of $\delta = 4a^2+b^2$. That is, $(a,b) = \pm(13,49), \pm(23,31)$. The only pair satisfying $b + av_0 \equiv 0 (\bmod \delta)$ is $(a,b) = (13,49)$ so that $(13,49)$ is the unique pair for which (1.1) is solvable; in fact, it is $13x^2+98xy-52y^2 = 1$ ($(x,y) = (1,2)$ is a solution).

The equation $23x^2+62xy-92y^2 = \pm 1$ is insolvable.

References

[1] L. Bapoungué, *Sur la résolubilité de l'équation Diophantienne* $ax^2 + 2bxy - kay^2 = \pm 1$ [*On the solvability of the Diophantine equation* $ax^2+2bxy-$

$kay^2 = \pm 1$], C. R. Acad. Sci. Paris Sér. I Math. **309** (1989), no. 5, 235–238 (French).

[2] ———, *Un critère de résolution pour l'équation Diophantienne* $ax^2+2bxy-kay^2=\pm 1$ [*A criterion for the solution of the Diophantine equation* $ax^2+2bxy-kay^2=\pm 1$], Exposition. Math. **16** (1998), no. 3, 249–262 (French).

[3] ———, *Factorisation dans un ordre non maximal d'un corps quadratique* [*Factorization in a nonmaximal order of a quadratic field*], Exposition. Math. **20** (2002), no. 1, 43–57 (French).

[4] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, Paris, 1967 (French).

[5] D. Shanks, *Solved and Unsolved Problems in Number Theory. Vol. I*, Spartan Books, District of Columbia, 1962.

Lionel Bapoungué: Département de Mathématiques, École Normale Supérieure, Université de Yaoundé 1, BP 47 Yaoundé, Cameroun

E-mail address: lbapou@uycdc.uninet.cm