

ON DIOPHANTINE EQUATIONS OF TYPE

$$X^4 - 2aX^2Y^2 - bY^4 = 1$$

R.J.STROEKER
Econometric Institute
Erasmus University
P.O. Box 1738
3000 DR Rotterdam
Holland

ABSTRACT. The title equations are investigated for values of a and b satisfying the restrictions: $a^2 + b = t^2d$ with squarefree $d \equiv 3 \pmod{4}$ and positive b . An algorithm is discussed for solving such equations, which uses the 2-divisibility properties of certain binary recurrences defined over the integers of $\mathbb{Q}(\sqrt{d})$. Examples are given and a table lists some equations for which the method gives complete solutions.

1. Introduction

The title equations are so-called *Thue equations*, i.e. diophantine equations of the form

$$f(x, y) = k, \quad (1)$$

where $f \in \mathbb{Z}[x, y]$ is homogeneous and of degree at least 3, and $k \in \mathbb{Z}$ is a given constant. When f is irreducible, such equations are known to admit at most finitely many solutions in rational integers. Clearly, for $a, b \in \mathbb{Z}$

$$f_{a,b}(x, y) := x^4 - 2ax^2y^2 - by^4 \quad (2)$$

is irreducible over \mathbb{Q} iff $4(a^2 + b)$ is not a perfect square.

We shall be concerned with solving equations of type

$$f_{a,b}(x, y) = 1, \quad (3)$$

where $f_{a,b}$ is as defined in (2) with $a, b \in \mathbb{Z}$, and $D := 4(a^2 + b) > 0$ and not a perfect square. For otherwise (3) is either trivially solvable or reduces to a pair of Pell equations in case $a > 0$ and $D = 0$. Henceforth, we assume D to be positive and not a perfect square.

We write $D = 4(a^2 + b) = 4t^2d$, where d is squarefree, and we also make the assumption that $d \equiv 3 \pmod{4}$. The main reason for this choice is a practical one: the prime 2 ramifies in $\mathbb{Q}(\sqrt{d})$ when $d \equiv 3 \pmod{4}$ and this fact is used in the algorithm below.

The associated number field K of equation (3), by which we mean the field

generated by a root of $f_{a,b}(x,1)=0$, will be of $(r,s)=(2,1)$ -type, that is to say, K has two real embeddings and 1 pair of embeddings in the complex numbers. It is easy to see that this will be the case iff $b > 0$.

Summarizing, we choose the parameters a and b such that

$$b > 0, \quad a^2 + b = t^2 d, \quad \text{with squarefree } d \equiv 3 \pmod{4}, \tag{4}$$

and we choose the corresponding t to be positive. We further assume the associated field K to be embedded in the reals and we write $L := \mathbb{Q}(\sqrt{d})$ to indicate the real quadratic subfield of K . The rings of integers of K and L will be denoted by \mathcal{O}_K and \mathcal{O}_L respectively.

In the sequel we intend to give a practical method to solve equations of type (3), subject to the restrictions (4). The method ultimately boils down to the application of the divisibility properties of a second order linear recurrence with values and coefficients in \mathcal{O}_L by powers of the unique prime ideal divisor of 2. Under certain conditions, this procedure enables us to determine the complete set of solutions, but unfortunately this is not always the case. In section 3, examples illustrate both situations. Also a table is provided, listing a few equations that have been solved by this method.

2. Solving the title equations: an algorithm

In this section we shall outline a procedure to solve (3), subject to (4). Complete proofs may be found in [6].

First, equation (3) may be written as

$$Norm_{K/\mathbb{Q}}(x - y\alpha) = 1, \tag{5}$$

so that integers x, y are sought for which $x - y\alpha$ is a unit of K . Here $\alpha := \sqrt{a + t\sqrt{d}} \in \mathbb{R}$ (as t is chosen with positive sign) and $K = \mathbb{Q}(\alpha)$.

The usual approach now is to calculate a set of generators for the positive unit group $U_K^+ := \{\xi \in \mathcal{O}_K \mid Norm_{K/\mathbb{Q}} \xi = 1, \xi > 0\}$, where $U_K := \langle \pm 1 \rangle \times U_K^+$ is the full unit group of K . In our case the rank of U_K^+ equals $r + s - 1 = 2$. There are standard ways of calculating such sets of fundamental units, but these usually are devised to deal with individual cases only, that is to say, one case at the time. As we are dealing with a class of equations, we have to approach this problem differently.

Let $U_L := \langle \pm 1 \rangle \times U_L^+$ be the unit group of L , where $U_L^+ = \langle \varepsilon \rangle$ is generated by the positive fundamental unit ε . Further, the relative unit group $U_{K/L}^+$ is defined as $U_{K/L}^+ := \{\eta \in \mathcal{O}_K \mid Norm_{K/L} \eta = 1, \eta > 0\}$. Clearly, $U_{K/L}^+$ has rank 1, so that we may write $U_{K/L}^+ = \langle \xi \rangle$, for a generator $\xi > 1$.

It is a well-known fact (see [1]) that $U_K^+ = \langle \varepsilon, \xi \rangle$, where ε and ξ are generators of U_L^+ and $U_{K/L}^+$ respectively, provided both $\sqrt{\varepsilon}$ and $\sqrt{\varepsilon\xi}$ do not belong to K .

Lemma 1 *If $U_L^+ = \langle \varepsilon \rangle$ and $U_{K/L}^+ = \langle \xi \rangle$, then $U_K^+ = \langle \varepsilon, \xi \rangle$ or $U_K^+ = \langle \varepsilon, \sqrt{\varepsilon\xi} \rangle$. If $\xi + \xi^{-1} = p + q\sqrt{d}$ for positive odd rational integers p and q , then $U_K^+ = \langle \varepsilon, \xi \rangle$.*

A proof follows the lines set out in [6]; the arguments used are elementary. Here we restrict ourselves to a brief outline. To show that

$\sqrt{\varepsilon} \notin \mathcal{O}_K$, consider the minimal polynomial $x^2 - 2wx + 1$ of ε . If ε were a perfect square in K , then the minimal polynomial of $\sqrt{\varepsilon}$ would be $x^4 - 2wx^2 + 1$. But then all field conjugates of $\sqrt{\varepsilon}$ would be real, an obvious contradiction. The proof of the statement $\sqrt{\varepsilon\xi} \notin \mathcal{O}_K$ in case p and q are odd, is based on the fact that, given $\sqrt{\varepsilon\xi} \in \mathcal{O}_K$, the coefficients of the minimal polynomial of $\varepsilon\xi$ can be expressed in terms of those of $\sqrt{\varepsilon\xi}$. Let

$$x^4 - s_\delta x^3 + t_\delta x^2 - u_\delta x + 1 \text{ be the minimal}$$

polynomial of the unit $\delta \in \mathcal{O}_K$. Put $\vartheta := \xi + \xi^{-1}$ and $\delta := \sqrt{\varepsilon\xi}$, then (provided $\delta \in \mathcal{O}_K$)

$$s_\delta \xi = \vartheta \varepsilon + \bar{\vartheta} \varepsilon^{-1} = s_\delta^2 - 2t_\delta, \quad t_\delta \xi = \varepsilon^2 + \varepsilon^{-2} + \vartheta \bar{\vartheta} = t_\delta^2 - 2s_\delta u_\delta + 2, \quad u_\delta \xi = \bar{\vartheta} \varepsilon + \vartheta \varepsilon^{-1} = u_\delta^2 - 2t_\delta,$$

where $\bar{\vartheta}$ is the L -conjugate of ϑ . This leads to a contradiction by considering these relations modulo 4, as a consequence of the fact that both p and q are odd. □

The question that remains is: how does one construct a generator ξ for $\mathcal{U}_{K/L}^+$? The answer we can give is to first find an element $\eta \in \mathcal{U}_{K/L}$ of the form $\eta := u + v\alpha \neq 1$ with $u, v \in \mathcal{O}_L$. This means solving the equation

$$u^2 - v^2 \alpha^2 = 1, \tag{6}$$

with $(u, v) \in \mathcal{O}_L^2$. Having computed a solution η of (6), we know that $\eta = \xi^k$ for some $k \in \mathbb{Z}$. The following lemma shows that $|k|$ can not be too large.

Lemma 2 (Nakamura) *If $\eta = \xi^k$ with $\xi \in \mathcal{U}_{K/L}^+$ and $k \in \mathbb{N}$, then*

$$k < k_0(\eta) := 2 \log \eta / \log \left[\sqrt[3]{\frac{1}{4} |\mathcal{D}_K| + 8^3 - 7} \right],$$

where \mathcal{D}_K is the absolute discriminant of K .

For a proof we refer to [3]. □

As α is the root of $f_{a,b}(x, 1) = 0$, $\mathcal{D}(\alpha)$ is seen to have the value $-2^8 b t^4 d^2$ and \mathcal{D}_K divides $\mathcal{D}(\alpha)$. Standard techniques can now be used to calculate \mathcal{D}_K (for instance, see [10]).

Also, knowing η and $k < k_0(\eta)$, we have to know how to construct ξ , where $\eta = \xi^k$. The next lemma provides a solution.

Lemma 3 (Nakamura) *If $\eta \in \mathcal{U}_{K/L}^+$, $\eta > 1$ and $\eta = \xi^k$ for some $k \in \mathbb{N}$ and $\xi \in \mathcal{U}_{K/L}^+$, then the minimal polynomial of ξ can be explicitly constructed from the minimal polynomial of η .*

In [6] a proof is given, and also an algorithm is provided. Both depend on the relations between the coefficients of the minimal polynomial of η and those of the minimal polynomial of ξ , like the relations given in the proof of Lemma 1. □

Under the conditions given in (4) and applying Lemma 1, we know that a solution (x, y) of (5) satisfies

$$x - y\alpha = \epsilon^m \xi^n \text{ for } m, n \in \mathbb{Z}, \tag{7}$$

if the signs of x and y are chosen suitably.

From the construction of a generator ξ for $U_{K/L}^+$ we may derive an expression of type $x - y\alpha = X + Y\xi^k$, where X and Y are linear expressions in x and y with coefficients in L . From $X + Y\xi^k = \epsilon^m \xi^n$ (see (7)) we obtain

$$-X\epsilon^{-m} = (\xi^{n-k} - \xi^{-(n-k)})/(\xi^k - \xi^{-k}) \text{ and } Y\epsilon^{-m} = (\xi^n - \xi^{-n})/(\xi^k - \xi^{-k})$$

or

$$-X\epsilon^{-m} = S_{n-k}/S_k \text{ and } Y\epsilon^{-m} = S_n/S_k, \tag{8}$$

where the sequence $(S_n)_{n \geq 0}$, defined by $S_n = (\xi^n - \xi^{-n})/(\xi - \xi^{-1})$, has values in \mathcal{O}_L . Other properties of this sequence, which is a second order linear recurrence, are listed in the following lemma.

Lemma 4 *Let \wp be the unique prime ideal divisor of 2 in \mathcal{O}_L . If $U_{K/L}^+ = \langle \xi \rangle$ and $\xi + \xi^{-1} = p + q\sqrt{d}$ for odd rational integers p and q , then*

- $\wp \mid s_n$ iff n is even,
- $\wp \parallel s_n$ iff $2 \parallel n$,
- if $n = 2^e m$ with odd m and $e \geq 2$, then $\wp^{2e} \parallel s_n$.

The proof of this lemma follows directly from the relation

$$S_{n+1} = \wp S_n - S_{n-1} \text{ for } n \geq 1, S_0 = 0 \text{ and } S_1 = 1, \text{ where } \wp := \xi + \xi^{-1}.$$

A complete proof is given in [6]. □

Remark *If p and q are not both odd, similar divisibility properties of (S_n) by powers of \wp may be derived.*

It follows from (8) and Lemma 4 that one may obtain information on the values of x and y by looking at the divisibility properties of X and Y by powers of \wp . Sometimes, e.g. when $k \equiv 2 \pmod{4}$, XY is forced to vanish, which results in the complete set of solutions of the original equation (see Theorem 1 of [6]). This is also illustrated in Example 1 below.

Summarizing, the following steps can be distinguished:

Algorithm

- **Construct an element of $U_{K/L}^+$**
Search for an element $\eta = u + v\alpha \neq 1$ of $U_{K/L}^+$ with $u, v \in \mathcal{O}_L$, i.e. solve $u^2 - v^2\alpha^2 = 1$ for $(u, v) \in \mathcal{O}_L^2$, $(u, v) \neq (1, 0)$.
- **Construct a generator ξ for $U_{K/L}^+$**
Use the element η constructed above to solve $\eta = \xi^k$ for ξ and maximal k with $k < k_0(\eta)$ (the Nakamura bound). Also calculate the coefficients of the minimal polynomial for ξ .
- **Check that $U_{K/L}^+ = \langle \epsilon, \xi \rangle$**
Check that $\xi + \xi^{-1} = p + q\sqrt{d}$ where p and q are both odd.
- **Check the divisibility of XY by powers of \wp**
Rewrite $x - y\alpha = X + Y\xi^k$ and check the divisibility of XY by powers of \wp . If

$k \equiv 2 \pmod{4}$ then $XY=0$, and the complete set of x, y -values can be obtained. Otherwise, only certain conditions on the solutions (x, y) are found.

Remark If STEP 3 of the algorithm fails, there still is a possibility of using (S_n) , or a similar binary recurrence, to determine all solutions (x, y) of (3), or at least some conditions on the possible solutions. But if (the equivalent of) STEP 4 also fails, one has to turn to other devices; Skolem's p -adic method very likely will help out in that case (see [4], [7] or [9]).

3. Examples

In this section we give two examples to illustrate the procedure discussed in the previous section.

Example 1 We choose $a=5$, $b=3$ in (4) and hence $d=7$ and $t=2$. Equation (3) may be written as

$$x^4 - 10x^2y^2 - 3y^4 = 1. \quad (9)$$

Searching for a solution $(u, v) \in \mathcal{O}_L^2$ of (6) results in $\eta = u + v\alpha$ with $u = 7 + 3\sqrt{7}$ and $v = 2 + \sqrt{7}$. The discriminant of $K = \mathbb{Q}(\alpha)$ equals $\mathfrak{D}_K = -2^6 \cdot 3 \cdot 7^2$, so that the Nakamura bound $k_0(\eta)$ of Lemma 2 has value 3.50. Checking $\eta = \xi^k$ with $k < k_0(\eta)$, we find the maximal k to be 2, so that $\eta = \xi^2$ with $\xi = \frac{1}{2}(3 + \sqrt{7} + (12 + 6\sqrt{7})^{\frac{1}{2}})$. Hence $\xi + \xi^{-1} = 3 + \sqrt{7}$, so that Lemma's 3 and 4 can be applied.

From (9) it is clear that any solution (x, y) satisfies $x \equiv 0 \pmod{3}$. Put $3z := y$, then

$$x - y\alpha = X + Y\xi^2 \text{ with } X = x + (7 + \sqrt{7})z \text{ and } Y = (2 - \sqrt{7})z.$$

It also follows from (9) that y is even, hence also z is even. Consequently, $\mathfrak{p} \nmid Y$, $\mathfrak{p} \nmid X$. From (8) we deduce that n is divisible by 4, so that $\mathfrak{p}^{2e-1} \parallel Y$, where $n = 2^e m$ with $e \geq 2$ and odd m (see Lemma 4). As this is clearly impossible, we must have $Y = 0$ and hence $(x, y) = (1, 0)$ is the only solution of (9) with $x > 0$.

Example 2 Next we choose $a = -1$ and $b = 2$ in (4) so that $d = 3$ and $t = 1$. The resulting equation is

$$x^4 + 2x^2y^2 - 2y^4 = 1. \quad (10)$$

It is immediately clear that $(x, y) = (1, 0)$ and $(1, 1)$ are solutions of (10).

A solution of (6) is given by $\eta = 3 + 2\sqrt{3} + (4 + 2\sqrt{3})\alpha$ with $\alpha = (-1 + \sqrt{3})^{\frac{1}{2}}$. With $\mathfrak{D}_K = -2^9 \cdot 3^2$ and $k_0(\eta) = 3.23$, we find that η is not a perfect power in K . Hence $\xi := \eta$ is a generator of $\mathcal{U}_{K/L}^+$ and from $\xi + \xi^{-1} = 6 + 4\sqrt{3}$ we see that STEP 4 of the algorithm fails.

From $x - y\alpha = X + Y\xi$ with $X = x + \frac{1}{2}\sqrt{3}y$, $Y = \frac{1}{2}(-2 + \sqrt{3})y$ and the fact that (10) has a solution with odd y , we deduce that \mathcal{U}_K^+ cannot be generated by the pair ε, ξ . Hence $\mathcal{U}_K^+ = \langle \xi, \sqrt{\varepsilon\xi} \rangle$, according to Lemma 1. Thus the alternative to (7) is

$$x - y\alpha = \xi^m (\sqrt{\varepsilon\xi})^n \text{ for } m, n \in \mathbb{Z}. \quad (11)$$

Now $\sqrt{\varepsilon\xi} = (1-\alpha)^{-1}$, as is easily checked, and (11) may be rewritten as

$$x - y\alpha = \Delta\xi^{m+N}\varepsilon^N, \quad (12)$$

with $\Delta=1$ in case $n=2N$, and $\Delta=(\alpha+1)\varepsilon$ in case $n=2N+1$. After some calculations we find that

$$\begin{aligned} 2x\varepsilon^{-N} &= S_{2m+2N}/S_{m+N}, & -y\varepsilon^{-N-1} &= 2S_{m+N} \text{ when } n=2N \text{ and} \\ (x-y)\varepsilon^{-N-1} &= 2S_{m+N+1}, & -(x+y)\varepsilon^{-N-1} &= 2S_{m+N} \text{ when } n=2N+1. \end{aligned}$$

In this example the sequence (S_n) does not have the same divisibility properties as its namesake of Lemma 4. In fact, here $\rho \nmid S_{2n+1}$ and $\rho^2 \parallel S_{2n}$ ($n \neq 0$). So the only information we obtain is:

- x odd, $y=0$ or $4 \parallel y$, in case $n=2N$,
- $2 \parallel (x+y)$ and $4 \parallel (x-y)$ unless $x-y=0$, or $2 \parallel (x-y)$ and $4 \parallel (x+y)$ unless $x+y=0$, in case $n=2N+1$.
- $m+2N \equiv 0 \pmod{2}$ in both cases $n=2N$ and $n=2N+1$.

It appears that the algorithm fails altogether. However, Skolem's p -adic method can be applied with $p=2$, working in the order $\mathbb{Z}[1, \varepsilon, \alpha, \varepsilon\alpha]$. To this end one could use the 2-adic expansions

$$(-1)^P \xi^{4P} = 1 + 2^2 P(1-2\varepsilon)(1+\alpha) + 2^4(\dots), \text{ and } \varepsilon^{4Q} = 1 + 2^3 \varepsilon Q + 2^4(\dots).$$

We leave the details as here we are merely concerned with the application of the algorithm. It is found that $(1,0)$ and $(1,1)$ are the only solutions (x,y) with $x \geq 0$, $y \geq 0$. For further information on Skolem's method see [7], [8] or [9].

We have carried out the algorithm for a small selection of (a,b) -values, for which the algorithm provides the full solution set of (5). The results are presented in the table below.

References

- [1] Trygve Nagell (1962), 'Sur quelques questions dans la théorie des corps biquadratiques'. *Arkiv för Math.* 4(26), 347-376.
- [2] Ken Nakamura (1981), 'Class number calculation and elliptic unit II'. *Proc. Japan Acad.* 57A, 117-120.
- [3] Ken Nakamura (1985), 'Class number calculation of a quartic field from the elliptic unit'. *Acta Arithm.* XLV, 215-227.
- [4] T. Skolem (1934), 'Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen'. 8^{de} Skand. Math. Kongr., Stockholm.
- [5] R.J. Stroeker (1981), 'On the diophantine equation $(2y^2-3)^2 = x^2(3x^2-2)$ in connection with the existence of non-trivial tight 4-designs'. *Indag. Math.* 43(3), 353-358.
- [6] R.J. Stroeker (198..), 'On quartic Thue equations with trivial solutions'. *Math. Comput.* (to appear).
- [7] R.J. Stroeker & N. Tzanakis (198..), 'On the application of Skolem's p -adic method to the solution of Thue equations'. *J. Number Th.* (to



- appear).
- [8] Nicholas Tzanakis (1985), 'On the diophantine equation $2x^3+1=py^2$ '. *Manuscripta Math.* **54**, 145-164.
- [9] N. Tzanakis & B.M.M. de Weger (1987), 'On the practical solution of the Thue equation'. Memorandum 668, Fac. Appl. Math., Un. of Twente.
- [10] Theresa P. Vaughan (1983), 'The discriminant of a quadratic extension of an algebraic field'. *Math. Comput.* **40**(162), 685-707.

Table

Solutions of $X^4 - 2aX^2Y^2 - bY^4 = 1$

The equations below have no solutions (X, Y) with $Y \neq 0$

$K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\sqrt{d})$, $\mathcal{U}_{K/L}^* = \langle \xi \rangle$

$\eta = u + v\alpha = \xi^k$, $u = u_1 + u_2\sqrt{d}$, $v = v_1 + v_2\sqrt{d}$, $\xi + \xi^{-1} = p + q\sqrt{d}$

a	b	d	u_1	u_2	v_1	v_2	k	p	q
-1	11	3	5	3	3	2	2	3	1
1	11	3	25	15	12	7	2	5	3
-3	3	3	1	1	2	1	2	1	1
3	3	3	1	1	1	0	2	1	1
-5	3	7	3	1	5	2	2	1	1
5	3	7	7	3	2	1	2	3	1
-9	27	3	37	21	31	18	6	1	1
9	27	3	37	21	8	5	6	1	1
-15	315	15	11	3	4	1	2	3	1
-15	27	7	7	3	8	3	2	3	1
15	27	7	3	1	1	0	2	1	1
179	35	11	9	3	1	0	2	3	1