Proceedings of the Edinburgh Mathematical Society (1996) 39, 97–114 ©

ON A QUARTIC DIOPHANTINE EQUATION

by R. J. STROEKER and B. M. M. DE WEGER

(Received 9th June 1994)

In this paper we consider the quartic diophantine equation $3(y^2-1)=2x^2(x^2-1)$ in integers x and y. We show that this equation does not have any other solutions (x,y) with $x\geqq 0$ than those given by $x=0,1,2,3,6,91$. Two approaches are emphasized, one based on diophantine approximation techniques, the other depends on the structure of certain quartic number fields.

1991 *Mathematics subject classification*: Primary, 11D25; Secondary, 11Y50.

1. Introduction

The diophantine equation referred to in the title is the following inhomogeneous quartic equation

$$3(y^2-1)=2x^2(x^2-1). \tag{1}$$

The wish to determine the complete set of rational integral solutions of (1) was expressed by Diaconis and Graham in [2, p. 328]. Apparently, the solutions to this diophantine problem correspond to values of $k\in\mathbb{N}$ for which the Radon transform based on the set of all $x\in\mathbb{Z}_2^k$ with exactly four ones is not invertible.

We thank Hendrik Lenstra who communicated the problem to Jaap Top, to whom we are equally grateful for pointing it out to us.

In the sequel we shall solve equation (1) completely by reducing this equation to a finite set of Thue equations, which are subsequently dealt with individually. In fact we have to solve five different quartic Thue equations. We feel the original equation to be sufficiently interesting to warrant a twofold solution process, emphasizing algebraic as well as diophantine approximation techniques.

The diophantine approximation approach rests on the theory of linear forms in the logarithms of algebraic numbers and follows the lines set out in [7] and [6], and the algebraic approach is based on the properties of certain binary sequences with values in a quadratic subfield of the biquadratic number field associated with the relevant Thue equation (see [3]).

We shall prove

Theorem. *The only integral solutions* (x, y) *of* (1) *are those associated with* $|x| = 0, 1, 2, 3, 6,$ *and* 91.

It is remarkable—this was pointed out by Hendrik Lenstra, who got it from Neville Robbins—that the positive x-values of the solutions of (1) coincide with those of the well-known Ramanujan–Nagell equation

$$2^n - 7 = (2x-1)^2.$$

This is probably a mere coincidence; at least, we fail to see an explanation. Another noteworthy aspect of equation (1) is that the minimal Weierstrass equation of the corresponding elliptic curve has very many integral solutions.

The birational transformation given by

$$X = \frac{18y + 18 - 2x^2}{x^2}, \quad Y = \frac{108y + 108 - 36x^2}{x^3} \tag{2}$$

sends (1) to

$$Y^2 = X^3 - 228X + 848. \tag{3}$$

The elliptic curve $E/\mathbb{Q}$ with (minimal) Weierstrass equation (3) has rank 2, torsion group $E(\mathbb{Q})_{\text{tors}} = \{O, (4, 0)\}$—here O is the group identity—and the free component of the Mordell–Weil group $E(\mathbb{Q})$ is generated by the points $P_1 = (2, 20)$, and $P_2 = (-2, 36)$. So, for any integral point P on $E/\mathbb{Q}$ we have

$$P = m_1 P_2 + m_2 P_2 + T, \text{ where } T = O \text{ or } (4, 0) \tag{4}$$

for suitable integers m_1 and m_2. In [5] it is shown that such information as given in (4) generally suffices to recover all integral points on the original Weierstrass equation by finding effective upper bounds for the coefficients of a certain linear form in elliptic logarithms, which corresponds to finding upper bounds for coefficients like m_1 and m_2 in (4). A definite advantage of this method is that it can be avoided having to deal with many Thue equations separately.

Note that many integral points on (3) are mapped to non-integral points on (1) by the birational transformation (2), and vice versa, not all integral points on (1) are mapped to integral points on (3).

2. The Thue equations

In this section we shall derive the Thue equations that can be associated with (1). The result of this derivation has been laid down in the following lemma.

Lemma. *Let (x, y) be an integral solution of* (1). *Then integers u and v exist satisfying one of the following equations:*

$$\begin{aligned}
&(L1)\quad 5u^4+2u^2v^2-v^4 &&=6 && \text{with } x=uv,\\
&(L2)\quad 5u^4-4u^2v^2-4v^4 &&=-3 && \text{with } x=2uv,\\
&(L3)\quad u^4+12u^2v^2-180v^4 &&=1 && \text{with } x=6uv,\\
&(L4)\quad 9u^4+12u^2v^2-20v^4 &&=1 && \text{with } x=6uv,\\
&(L5)\quad 9u^4-6u^2v^2-5v^4 &&=-2 && \text{with } x=3uv.
\end{aligned}$$

Proof. Let $(x,y)\in\mathbb{Z}^2$ be a solution of the original equation (1). After rewriting (1), factorization in $\mathbb{F}:=\mathbb{Q}(\sqrt{-5})$ yields

$$6y^2=(2x^2-\lambda)(2x^2-\bar{\lambda}), \tag{5}$$

where $\lambda:=1+\sqrt{-5}$ and $\bar{\lambda}$ denotes the complex conjugate of λ in $\mathbb{F}$. We shall work in the ring of integers of the number field $\mathbb{F}$. This field has class number 2 and the non-principal ideal class $\mathscr{C}$ contains the prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$, where the index refers to the underlying rational prime. The following ideal relations are easily checked:

$$\begin{aligned}
\mathfrak{p}_2^2&=[2] & \mathfrak{p}_3\bar{\mathfrak{p}}_3&=[3],\\
\mathfrak{p}_2\mathfrak{p}_3&=[1-\sqrt{-5}], & \mathfrak{p}_2\bar{\mathfrak{p}}_3&=[1+\sqrt{-5}],\\
\mathfrak{p}_3^2&=[2+\sqrt{-5}], & \bar{\mathfrak{p}}_3^2&=[2-\sqrt{-5}].
\end{aligned} \tag{6}$$

As $y^2\equiv(2x^2-1)^2\not\equiv 0 \pmod 5$, it follows from (5) and (6) that the principal ideals $[2x^2-\lambda]$ and $[2x^2-\bar{\lambda}]$ can have no other common prime ideal divisor than $\mathfrak{p}_2$. This leaves the following two possibilities:

$$\text{(I) } [2x^2-\lambda]=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{a}^2, \text{ and } (\bar{\text{I}})\ [2x^2-\lambda]=\mathfrak{p}_2\bar{\mathfrak{p}}_3\mathfrak{a}^2$$

for some integral ideal $\mathfrak{a}$. Cases (I) and ($\bar{\text{I}}$) will be called *conjugate* cases. Now either $\mathfrak{a}$ belongs to the principal ideal class or $\mathfrak{a}$ belongs to class $\mathscr{C}$ in which case $\mathfrak{p}_2\mathfrak{a}$ is a principal ideal. This gives

$$\text{(I)}\quad [2^h(2x^2-\lambda)]=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{a}^2=[1-\sqrt{-5}][a+b\sqrt{-5}]^2, \tag{7}$$

where $h\in\{0,1\}$, and a and b are arbitrary rational integers. The conjugate case ($\bar{\text{I}}$) can be expressed similarly.

We first consider (I). Equating coeffients in (7) yields the quadratic system of equations

$$\text{(I)}\quad \begin{cases} a^2+10ab-5b^2=\delta 2^h(2x^2-1)\\ a^2-2ab-5b^2=\delta 2^h \end{cases}, \quad \text{with } \delta=\pm 1. \tag{8}$$

Taking the second equation in (8) mod 3 shows that $\delta=(-1)^h$ and $a-b\not\equiv 0 \pmod 3$. It is also clear that $\gcd(a,b)=1$. Adding the equations of (8) yields

$$(a-b)(a+5b)=(-2)^h x^2.$$

As $\gcd(a-b,a+5b)=1$ or 2, we deduce that $|a-b|$ is a perfect square or twice a perfect square. Without loss of generality we may choose the signs of a and b such that

$$a-b=u^2, \text{ or } a-b=2u^2$$

for a suitable integer u. The former choice forces h to vanish, and leads via the second equation of (8) to the quartic (L1). The latter choice is only possible when $h=1$, and we find in this case equation (L2).

Next we consider the conjugate case. Equating coefficients in the conjugate case yields the quadratic system of equations

$$(\bar{\mathrm{I}}) \quad \begin{cases} a^2-10ab-5b^2=-\delta 2^h(2x^2-1) \\ a^2+2ab-5b^2=\delta 2^h \end{cases}, \quad \text{with } \delta=\pm 1. \tag{9}$$

Taking the second equation in (9) mod 3 again shows that $\delta=(-1)^h$. Subtracting this time the equations of (9) yields

$$6ab=(-2)^h x^2.$$

From the second equation of (9) it follows that a must be odd, for even a forces $b^2\equiv -2^h \pmod 4$ which is clearly impossible. As $\gcd(a,b)=1$, we deduce that $|a|$ is a perfect square or three times a perfect square. Without loss of generality we may choose the sign of a such that

$$a=u^2, \text{ or } a=3u^2$$

for a suitable integer u. In case $a=u^2$, we may write $b=3(-1)^h 2^{1-h}v^2$ for some rational integer v. Then $x=3\cdot 2^{1-h}uv$ and the choice $h=0$ leads to the quartic (L3), whereas $h=1$ gives an impossible equation mod 4. Similarly, for $a=3u^2$, we have $b=(-1)^h 2^{1-h}v^2$ and again $x=3\cdot 2^{1-h}uv$. The choice $h=0$ yields (L4) and $h=1$ gives the quartic (L5).

This completes the proof of the Lemma. □

In view of the Lemma it is clear that in order to prove the Theorem it is sufficient to solve each of the quartic equations appearing in this Lemma. The integral solutions of these five Thue equations are the subject of the following proposition.

Proposition. *The only integral solutions* (u, v) *with non-negative* u *and* v *of the five quartic Thue equations of the Lemma are given in the table below.*

$\mathbb{Z}^2_{\geqq 0}$	L1	L2	L3	L4	L5
(u, v)	$(1,1)$ $(7,13)$	$(1,1)$	$(1,0)$	$(1,1)$	$(1,1)$

Before we start on the actual proof, we shall collect the necessary information from the quartic number fields associated with these Thue equations. In this compilation of facts we were assisted by the following programs for performing the actual computations, and for checking the computed results.

- KANT version 2: a collection of numerical routines for calculations in algebraic number fields,
- GP/PARI-1.38: a collection of numerical and symbolic routines for (algebraic) number theory,
- MapleV version 2: the computer algebra package.

Adopting the following notations for polynomials and constants

$$\begin{aligned} g_1(x,y) &= x^4 - 2x^2y^2 - 5y^4 & m_1 &= -6, \\ g_2(x,y) &= x^4 + 4x^2y^2 - 20y^4 & m_2 &= 12, \\ g_3(x,y) &= x^4 + 12x^2y^2 - 180y^4 & m_3 &= 1, m_4 = 9, \\ g_5(x,y) &= x^4 - 6x^2y^2 - 45y^4 & m_5 &= -18, \end{aligned}$$

we see that the equations of the Lemma may be rewritten as:

$$\begin{aligned} &(\mathrm{L1}) \Leftrightarrow g_1(v,u) = m_1, \\ &(\mathrm{L2}) \Leftrightarrow g_2(2v,u) = m_2, \\ &(\mathrm{L3}) \Leftrightarrow g_3(u,v) = m_3, \\ &(\mathrm{L4}) \Leftrightarrow g_3(3u,v) = m_4, \\ &(\mathrm{L5}) \Leftrightarrow g_5(3u,v) = m_5. \end{aligned} \tag{10}$$

Here (Li) refers to the corresponding equation of the Lemma. It usually pays to choose the most natural irreducible polynomial—i.e. having the smallest possible coefficients—defining a given number field. Now $g_1(x,1)$ and $g_2(x,1)$ satisfy this requirement, but

$g_3(x,1)$ and $g_5(x,1)$ do not. Apart from symmetry reasons, that is why we prefer to define new polynomials in these two cases. Also note that (L3) and (L4) of the Lemma correspond to the same number field. These new polynomials are:

$$h_1(x) := g_1(x,1), \qquad h_2(x) := g_2(x,1),$$
$$h_3(x) := x^4 + 2x^2 - 5, \quad h_5(x) := x^4 - 4x^2 - 20.$$

For fixed $i = 1, 2, 3$, or 5, let θ be a root of $h_i(x) = 0$ and let ψ be a root of $g_i(x) = 0$, both real or both non-real. The number fields generated by θ and ψ are isomorphic, and the isomorphisms between the corresponding $\mathbb{Q}(\theta)$ and $\mathbb{Q}(\psi)$ can be made explicit by:

$$\psi = \theta \quad \text{and} \quad \theta = \psi \quad \text{for } i = 1, 2,$$
$$\psi = \theta + \theta^3 \quad \text{and} \quad \theta = \tfrac{1}{6}\psi + \tfrac{1}{36}\psi^3 \quad \text{for } i = 3,$$
$$\psi = -\tfrac{1}{2}\theta + \tfrac{1}{4}\theta^3 \quad \text{and} \quad \theta = -\tfrac{1}{3}\psi + \tfrac{1}{9}\psi^3 \quad \text{for } i = 5.$$

The four number fields $\mathbb{K} := \mathbb{Q}(\theta) = \mathbb{Q}(\psi)$ are quartic fields with two real and one pair of complex conjugate embeddings in $\mathbb{C}$. All four discriminants coincide with $-46080 = 2^{10}3^2 5$. Further, each field is a quadratic extension of $\mathbb{L} := \mathbb{Q}(\sqrt{6})$. Table 1 contains the following information on each field:

- an integral basis $\{1, \theta, \phi, w\}$,
- a system of fundamental units $\{\varepsilon, \eta\}$,
- the generator $\xi > 1$ of the relative unit group $\{\zeta \mid \mathrm{Norm}_{\mathbb{K}/\mathbb{L}}(\zeta) = 1, \zeta > 0\}$,
- the regulator $\mathscr{R}_{\mathbb{K}}$,
- generators of the prime ideals dividing 2 and 3 with their norms.

All fields have trivial class groups, and no two fields are isomorphic, as their regulators differ.

Let us denote the two real conjugates of any $\alpha \in \mathbb{K}$ by α_1 and α_2, and the two complex conjugates by α_3 and $\alpha_4 := \bar{\alpha}_3$. Note that for all fields $\theta_2 = -\theta_1$ and $\psi_2 = -\psi_1$, and also $\theta_4 = -\theta_3$ and $\psi_4 = -\psi_3$. In Table 2 we give the values of θ_1, θ_3, ψ_1, and ψ_3 explicitly.

Each one of the equations $g_i(X, Y) = m_i$ for $i = 1, 2, 3, 5$, and $g_3(X, Y) = m_4$ gives rise to an equation of the form

$$X - Y\psi = \pm \mu \varepsilon^a \eta^b, \tag{11}$$

where μ is a $\mathbb{K}$-integer of norm m_i, which is determined up to a unit, and a and b are unknown rational integers. Observe that we may drop the $\pm$ sign, as solutions (X, Y) of (11) come in foursomes $(\pm X, \pm Y)$.

From this observation and from the entries of Tables 1 and 2 it is easy to deduce that the possible values of μ may be restricted as follows—also it should be noted that μ has been chosen such that $a = b = 0$ always corresponds to one of the solutions.

Integral bases

$\mathbb{K}=\mathbb{Q}(\theta)$, where θ is root of $h_i(x)=0$, $\mathbb{L}=\mathbb{Q}(\sqrt{6})\subset\mathbb{K}$
$\{1,\theta,\phi,\omega\}$ is an integral basis of $\mathbb{K}$, $\mathfrak{R}_{\mathbb{K}}$ is its regulator

i	ϕ	ω	$\mathfrak{R}_{\mathbb{K}}$
1	θ^2	θ^3	20.635
2	$\frac{1}{2}\theta^2$	$-\frac{1}{2}\theta+\frac{1}{4}\theta^3$	25.604
3	θ^2	θ^3	10.913
5	$\frac{1}{2}\theta^2$	$-\frac{1}{2}\theta+\frac{1}{4}\theta^3$	15.385

Unit groups

$U_{\mathbb{L}}/\langle\pm1\rangle=\langle\varepsilon\rangle$, $U_{\mathbb{K}}/\langle\pm1\rangle=\langle\varepsilon,\eta\rangle$, $U_{\mathbb{K}/\mathbb{L}}/\langle\pm1\rangle=\langle\xi\rangle$

i	ε	η	ξ
1	$3+2\phi$	$8-\theta-\phi+\omega$	$\varepsilon\eta$
2	$3-2\phi$	$12+7\theta+\phi+4\omega$	$\varepsilon^{-1}\eta$
3	$3-2\phi$	$4+3\theta+\phi+\omega$	η
5	$3+2\phi$	$2+3\theta-\phi-2\omega$	$-\varepsilon^{-1}\eta^{-1}$

Prime factorizations

$[2]=[\pi_2]^4$ for all i, with $\mathrm{Norm}(\pi_2)=-2$,
$[3]=[\pi_{31}]^2\,[\pi_{32}]^2$ for $i=1,2$ with $\mathrm{Norm}(\pi_{31})=\mathrm{Norm}(\pi_{32})=3$,
$[3]=[\pi_3]^2$ for $i=3,5$ with $\mathrm{Norm}(\pi_3)=9$

i	π_2	π_3 or π_{31}	π_{32}
1	$1+4\theta-\omega$	$2+\theta$	$2-\theta$
2	$4+3\theta+\phi+\omega$	$3+2\theta+\phi+\omega$	$3-2\theta+\phi-\omega$
3	$1+\theta$	$2-\phi$	—
5	$2-\theta+\phi-\omega$	$4-\phi$	—

TABLE 1. Associated number fields

$$
\begin{aligned}
&(i=1)\quad \mu=1-\psi=-\pi_2\pi_{31}\eta^{-1}\\
&(i=2)\quad \mu=2-\psi=\pi_2^2\pi_{32}\varepsilon\eta^{-1}\\
&(i=3)\quad \mu=1\\
&(i=4)\quad \mu=3-\psi=(3+\psi)\eta^{-2}=\pi_3\eta^{-1}\\
&(i=5)\quad \mu=3-\psi=(3+\psi)\varepsilon\eta=\pi_2\pi_3.
\end{aligned}
\tag{12}
$$

Equation (11) is essential for either one of the approaches chosen. But from this point onward, the two methods diverge.

Real conjugates $\mathbb{K}=\mathbb{Q}(\theta)=\mathbb{Q}(\psi)$ $h_i(\theta,1)=0, g_i(\psi,1)=0$				
i	θ_1	θ_3	ψ_1	ψ_3
1	$\sqrt{1+\sqrt{6}}$	$\sqrt{1-\sqrt{6}}$	θ_1	θ_3
2	$\sqrt{-2+2\sqrt{6}}$	$\sqrt{-2-2\sqrt{6}}$	θ_1	θ_3
3	$\sqrt{-1+\sqrt{6}}$	$\sqrt{-1-\sqrt{6}}$	$\sqrt{-6+6\sqrt{6}}$	$-\sqrt{-6-6\sqrt{6}}$
5	$\sqrt{2+2\sqrt{6}}$	$\sqrt{2-2\sqrt{6}}$	$\sqrt{3+3\sqrt{6}}$	$-\sqrt{3-3\sqrt{6}}$

TABLE 2. Field generators

3. A proof by diophantine approximation methods

In this section we give a complete proof of the Theorem using the techniques exposed in [6] and [7]. However, details that may distract the reader's attention from the main line of reasoning are omitted. In those instances complete references are provided.

First proof of the Proposition. We set off by showing that the case $i=4$ is the spitting image of the case $i=3$, provided we allow for $X, Y \in (1/(\sqrt{3}))\mathbb{Z}$ and $a \in \frac{1}{2}\mathbb{Z}$ instead of $X, Y, a \in \mathbb{Z}$. Indeed, the associated number fields for the cases $i=3$ and $i=4$ coincide, and the relation

$$3-\psi=\sqrt{3}\varepsilon^{1/2}\eta^{-1}$$

in the octic number field $\mathbb{K}(\sqrt{3})$, is easily verified. Further, $g_3(X,Y)=9$ and $g_3(X/\sqrt{3}, Y/\sqrt{3})=1$ are equivalent. Hence, equation (11) with $i=4$, i.e.

$$X-Y\psi=\pm(3-\psi)\varepsilon^a\eta^b,$$

may be rewritten as

$$\frac{X}{\sqrt{3}} - \frac{Y}{\sqrt{3}}\psi = \pm\varepsilon^{a+1/2}\eta^{b-1}, \tag{13}$$

which is of the form (11) for $i=3$, where $(X/\sqrt{3}, Y/\sqrt{3}, a+\frac{1}{2}, b-1)$ replaces (X, Y, a, b). Note that relation (13) is invariant under the non-trivial $\mathbb{K}$-automorphism of $\mathbb{K}(\sqrt{3})$ which sends $\sqrt{3}$ to $-\sqrt{3}$ and $\varepsilon^{1/2}$ to $-\varepsilon^{1/2}$. It will become transparent soon that adjusting the domains for X, Y and a in this way is justified.

Recall that equation (11) has two real conjugates:

$$X - Y\psi_i = \pm\mu_i\varepsilon_i^a\eta_i^b, \quad i=1,2.$$

Because of symmetry—$\psi_2 = -\psi_1$ and the pairs (X, Y), $(X, -Y)$ are at the same time solutions or non-solutions—we may assume without loss of generality that

$$|X - Y\psi_1| \leqq |X - Y\psi_2|.$$

Following [6, Sections II.1 and II.2], we put

$$\beta := X - Y\psi. \tag{14}$$

Then $|\beta_1| \leqq |\beta_2|$ and hence the i_0 of [6, Lemma 1.1] has the value 1. Elimination of X and Y from the first, third and fourth conjugate equations of (14)—with the appropriate adjustment in case $i=4$—yields

$$(\psi_4-\psi_1)\beta_3 + (\psi_1-\psi_3)\beta_4 + (\psi_3-\psi_4)\beta_1 = 0.$$

By (11) this leads to

$$\frac{\psi_1-\psi_4}{\psi_1-\psi_3}\cdot\frac{\mu_3}{\mu_4}\left(\frac{\varepsilon_3}{\varepsilon_4}\right)^a\left(\frac{\eta_3}{\eta_4}\right)^b - 1 = -\frac{\psi_3-\psi_4}{\psi_3-\psi_1}\cdot\frac{\beta_1}{\beta_2}. \tag{15}$$

As it happens, ε is real so that $\varepsilon_4 = \bar{\varepsilon}_3 = \varepsilon_3$. Hence the variable a disappears from the left-hand-side of equation (15). Also X and Y are absent. As all information we need to make our argument work is implicitly given by equation (15), taking $X, Y \in (1/\sqrt{3})\mathbb{Z}$ and $a \in \frac{1}{2}\mathbb{Z}$ is justified.

Put

$$\delta := \frac{\psi_1-\psi_4}{\psi_1-\psi_3}\cdot\frac{\mu_3}{\mu_4}.$$

Since $\alpha_4 = \bar{\alpha}_3$ for all $\alpha \in \mathbb{K}$, it follows that δ and η_3/η_4 are on the unit circle. Now put

$$\delta =: e^{i\zeta}, \quad \frac{\eta_3}{\eta_4} =: e^{i\gamma}, \quad \text{for } \zeta, \gamma \in (-\pi, \pi].$$

Then (15) implies that $|e^{i(\zeta + b\gamma)} - 1|$ is small for large b, so that a rational integer k exists such that

$$\Lambda := \zeta + b\gamma + k \cdot 2\pi \tag{16}$$

is close to 0. In fact, with $A = \max(|a|, |b|)$, we have by [6, Lemma 2.2]: if $|Y| \geqq 6$ then

$$|\Lambda| \leqq C_6 \exp\left(\frac{-4}{C_5} \cdot A\right). \tag{17}$$

Omitting the details, we merely provide the final constants that may be used in each of our four cases:

$$\begin{aligned} C_5 &\leqq 1.0323, \\ C_6 &\leqq 1.1533 \times 10^6. \end{aligned} \tag{18}$$

Note that all solutions (X, Y) with $|Y| \leqq 5$ can be found by direct search.

Next we apply the theory of linear forms in logarithms. The sharp bound of [1] yields in all cases—again we omit the details:

$$|\Lambda| > \exp(-4.7057 \times 10^{16} \log \max(|b|, |k|)).$$

Observe that by (16), provided $A \geqq 4$,

$$|k| < \frac{1}{2\pi} \cdot 1.1533 \times 10^6 \exp\left(\frac{-4 \times 3}{1.0323}\right) + \tfrac{1}{2} + \tfrac{1}{2}|b| < A. \tag{19}$$

Hence we obtain

$$|\Lambda| > (\exp -4.7057 \times 10^{16} \log A). \tag{20}$$

Combining (17) with (18) and (20) yields

$$A \leqq 4.9480 \times 10^{17}.$$

The next step is to reduce this huge bound on A by computational diophantine approximation techniques.

Consider the lattice $\Gamma \subset \mathbb{Z}^2$ generated by the column vectors of the matrix

$$\mathscr{A} = \begin{pmatrix} 1 & 0 \\ [10^{40}\gamma] & [10^{40} \cdot 2\pi] \end{pmatrix},$$

where $[\cdot]$ means rounding towards 0. Further consider the vector $\mathbf{y} \in \mathbb{Z}^2$ given by

$$\mathbf{y} = \begin{pmatrix} 0 \\ -[10^{40}\zeta] \end{pmatrix}.$$

In fact we have a different pair $(\Gamma, \mathbf{y})$ for each of the four cases corresponding to $i = 1, 2, 3(4), 5$.

Using an adaptation of the Euclidean Algorithm we computed a reduced basis for Γ. From that reduced basis it is easy to calculate

$$\ell(\Gamma, \mathbf{y}) := \min_{\mathbf{x} \in \Gamma} |\mathbf{x} - \mathbf{y}|.$$

See [7, Chapter 3] for details. We found that

$$\ell(\Gamma, \mathbf{y}) \geqq 3.6795 \times 10^{18}$$

in all five cases. Now put

$$\mathscr{A}\begin{pmatrix} b \\ k \end{pmatrix} - \mathbf{y} =: \begin{pmatrix} b \\ \lambda \end{pmatrix}.$$

Then clearly $\lambda \in \mathbb{Z}$. We have

$$(3.6795 \times 10^{18})^2 \leqq \ell(\Gamma, \mathbf{y})^2 \leqq \left\| \begin{pmatrix} b \\ \lambda \end{pmatrix} \right\|^2 = b^2 + \lambda^2 \leqq A^2 + \lambda^2 \leqq (4.9480 \times 10^{17})^2 + \lambda^2,$$

and hence

$$|\lambda| \geqq 3.6460 \times 10^{18}.$$

Further, $\lambda = [10^{40}\zeta] + b[10^{40}\gamma] + k[10^{40} \cdot 2\pi]$, which implies—see (16) and (19)—that

$$|\lambda - 10^{40}\Lambda| \leqq 1 + |b| + |k| \leqq 1 + 2A \leqq 9.8961 \times 10^{17},$$

provided that $A \geqq 4$. It follows that

$$|\Lambda| \geqq 10^{-40}(|\lambda| - 9.8961 \times 10^{17}) \geqq 2.6563 \times 10^{-22}.$$

Combining this and (17) with (18) yields a reduced upper bound for A,

$$A \leqq 16.$$

For all $b \in \mathbb{Z}$ with $|b| \leqq 16$, we computed a from

$$\delta\left(\frac{\eta_3}{\eta_4}\right)^b - 1 = -\frac{\psi_3-\psi_4}{\psi_3-\psi_1}\cdot\frac{\mu_1}{\mu_4}\left(\frac{\varepsilon_1}{\varepsilon_4}\right)^a\left(\frac{\eta_1}{\eta_4}\right)^b,$$

(cf. (15)), and checked for $a\in\frac{1}{2}\mathbb{Z}$. The solutions we found can be read off from the following diagram; X and Y were computed from (11).

i	a	b	X	Y
1	-2	-1	13	7
1	0	0	1	1
2	0	0	2	1
3	$\frac{1}{2}$	± 1	$\sqrt{3}$	$\pm\frac{1}{3}\sqrt{3}$
3	0	0	1	0
5	-1	-1	-3	1
5	0	0	3	1

This completes the first proof of the Proposition. □

4. An algebraic proof

It could be argued that one of the drawbacks of the method presented in the previous section lies in the fact that only limited use is made of the specific structure of the associated number fields. In this section we don't use estimation techniques but instead we try to express the solutions of (11) in terms of characteristic elements of the quartic number fields involved. Like before, we have to consider five separate cases. As the process is very similar in each case, we shall sometimes omit the details so as not to try the reader's patience too much. A description of this algebraic approach may also be found in [3].

Second proof of the Proposition. We proceed by considering (11) once more. Or rather, we exchange η for ξ as the second fundamental unit—it is clear from Table 1 that this is permitted—so that (11) becomes

$$\frac{X-Y\psi}{\mu} = \sigma\varepsilon^a\xi^b, \quad \text{with } \sigma = \pm 1, \tag{21}$$

where μ is given by (12) for $i=1,2,3,4,5$.

We know that $\psi_2=-\psi_1$, $\varepsilon_2=\varepsilon_1$ and $\xi_2=\xi_1^{-1}$. For convenience we shall drop the index 1 and write ψ instead of ψ_1 etc.

Define the sequences $(s_n)_{n\in\mathbb{Z}}$ and $(t_n)_{n\in\mathbb{Z}}$ as follows:

$$s_n := \frac{\xi^n-\xi^{-n}}{\xi-\xi^{-1}}, \quad \text{and} \quad t_n := \xi^n+\xi^{-n}, \quad \text{for } n\in\mathbb{Z}.$$

It is easily verified that s_n and t_n are algebraic integers of $\mathbb{L}$ for all n. Indeed, on putting $\rho := \xi + \xi^{-1} \in \mathbb{Z}[\sqrt{6}]$, this follows immediately from the binary recurrences

$$s_{n+1} = \rho s_n - s_{n-1}, \quad t_{n+1} = \rho t_n - t_{n-1}, \tag{22}$$

with initial values $s_0 = 0$, $s_1 = 1$ and $t_0 = 2$, $t_1 = \rho$. Moreover,

$$t_n = s_{n+1} - s_{n-1} \quad \text{for all } n. \tag{23}$$

Immediate consequences of the definitions are the doubling formulas

$$s_{2n} = s_n t_n, \quad t_{2n} = t_n^2 - 2 \quad \text{for all } n. \tag{24}$$

We return to (21). Adding this equation to its (real) conjugate on the one hand, and subtracting (21) from its conjugate on the other hand, we arrive at the two expressions:

$$\begin{aligned} \frac{\mu_1(X + Y\psi) + \mu_2(X - Y\psi)}{\mu_1\mu_2} &= \sigma\varepsilon^a t_b, \\ \frac{-\mu_1(X + Y\psi) + \mu_2(X - Y\psi)}{\mu_1\mu_2(\xi - \xi^{-1})} &= \sigma\varepsilon^a s_b. \end{aligned} \tag{25}$$

The left-hand-side of each of these equations is an integer of $\mathbb{L}$. Because of (23), equations (25) give rise to explicit expressions of the form $A(X, Y) + B(X, Y)\sqrt{6}$ for every element of the sequence (s_n) once $i \in \{1, 2, 3, 4, 5\}$ is specified. Here A and B are linear forms with coefficients in $\mathbb{Q}$. Of expressions like (25) we calculate the values by the additive valuation functions of the prime above 2. As 2 ramifies in $\mathbb{L}$, a rational integer must be exactly divisible by an even number of the prime above 2, unless it vanishes. We shall use this fact repeatedly.

We'll be more specific now and deal with each one of the cases corresponding to $i \in \{1, 2, 3, 4, 5\}$ separately. Writing equations (25) in the form

$$\begin{aligned} T_1(X, Y) + T_2(X, Y)\sqrt{6} &= \sigma\varepsilon^a t_b, \\ S_1(X, Y) + S_2(X, Y)\sqrt{6} &= \sigma\varepsilon^a s_b, \end{aligned}$$

i	T_1	T_2	S_1	S_2
1	$2Y$	$\frac{1}{3}(-X+Y)$	$\frac{5}{6}(-X+Y)$	$\frac{1}{3}(X-Y)$
2	$2(X-Y)$	$\frac{2}{3}(X-2Y)$	$\frac{7}{30}(-X+2Y)$	$\frac{1}{10}(X-2Y)$
3	$2X$	0	$-3Y$	Y
4	$2(5X-14Y)$	$4(X-3Y)$	$X-3Y$	$\frac{1}{3}(X-3Y)$
5	$2(-X+4Y)$	$-X+3Y$	$\frac{1}{6}(-X+3Y)$	0

TABLE 3. $\mathbb{L}$-expressions for s_b and t_b

we obtain the following explicit expressions, gathered in Table 3.

For $i=1$, applying (22) and (23), we deduce from the relevant entries of Table 3 the relations

$$\frac{-7X+13Y}{6}=\sigma\varepsilon^a s_{b+1},$$
$$\frac{-X+Y}{6}=\sigma\varepsilon^{a+1}s_b. \tag{26}$$

This shows that

$$\varepsilon^a s_{b+1}\in\mathbb{Z} \quad \text{and} \quad \varepsilon^{a+1}s_b\in\mathbb{Z}.$$

Indeed, for each of the equations (26), the left-hand-side is a rational number and the right-hand-side is an algebraic integer of $\mathbb{L}$.

It is not difficult to see that for odd integers n, we have

$$s_n\equiv 1 \pmod 2 \quad \text{and} \quad t_n\equiv 2(1+\sqrt{6}) \pmod 4,$$

and hence

$$s_{2n}=2(1+\sqrt{6}) \pmod 4.$$

By repeated index doubling with (24)—see also [3, Lemma 1]—and mathematical induction, it follows from

$$\varepsilon^m\equiv 1 \pmod 2$$

and the observations above that for any $m,n\in\mathbb{Z}$ with $n\neq 0$, an integer $e\geqq 1$ exists such that

$$\varepsilon^m s_{2n}=2^e(1+\sqrt{6}) \pmod{2^{e+1}}.$$

This implies that $\varepsilon^m s_{2n} \notin \mathbb{Z}$, unless $n=0$. Consequently, from (26) we deduce that $b=0$ or $b=-1$, whence the only solutions in this case are $(X, Y)=(\sigma,\sigma),(13\sigma,7\sigma)$.

In the next case $i=2$ we deduce from Table 3 that

$$\frac{X-2Y}{30}(-7+3\sqrt{6})=\sigma\varepsilon^a s_b,$$
$$\frac{19X-2Y}{3}=\sigma\varepsilon^a(s_{b+1}-11s_{b-1}). \tag{27}$$

The first equation of (27) implies that b is even. Indeed, in $\mathbb{L}$ the prime $1+\sqrt{6}$ divides s_b only for even b, as can be seen from (22) and the fact that ρ is divisible by $1+\sqrt{6}$ too.

We intend to prove that $b=0$ by showing inductively that b is divisible by all positive powers of 2. To this end we set

$$u_n := s_{n+1}-11s_{n-1}, \quad n\in\mathbb{Z}$$

and we use the following congruence relations

$$s_{2^i(2n+1)}\equiv(-1)^{n+1}2^i(1+\sqrt{6}) \pmod{2^{i+2}}, \quad i=1,2,\ldots \tag{28}$$

$$u_{2^i(2n+1)}\equiv 12+(-1)^n 2^{i+1}(1+2\sqrt{6}) \pmod{2^{i+3}}, \quad i=1,2,\ldots \tag{29}$$

These relations may be obtained from (22), (24) and the following facts

$$\begin{aligned} &u_{2n}=-12+u_n t_n, \\ &t_{2^i n}\equiv 2 \pmod{2^{i+2}} \quad i=1,2,\ldots \end{aligned} \quad \text{for all } n\in\mathbb{Z}, \tag{30}$$

which may be verified without great difficulty.

We proceed by assuming that $b\equiv 2^i \pmod{2^{i+1}}$ for some $i\geqq 1$. Using (28) and the first equation of (27), and dividing through by 2^i results in

$$\varepsilon^{a-1}\equiv j_i \pmod 4$$

for some rational integer j_1. Clearly, this is only possible for odd a.

Next, by (29) and the second equation of (27), we have

$$\varepsilon^a(12\pm 2^{i+1}+2^{i+2}\sqrt{6})\equiv j_2 \pmod{2^{i+3}}$$

for a rational integer j_2. However, this gives an impossible congruence modulo 16 as a is odd. Consequently, b must be divisible by all positive powers of 2, and hence $b=0$.

Then (27) implies that $X-2Y=0$ and $19X-2Y=36\sigma\varepsilon^a$, from which we deduce that $a=0$ and $(X, Y)=(2\sigma, \sigma)$.

For $i=3$ we obtain from Table 3 the following relations:

$$\begin{aligned} Y(-3+\sqrt{6}) &= \sigma\varepsilon^a s_b, \\ X-3Y &= \sigma\varepsilon^a s_{b+1}, \\ -X-3Y &= \sigma\varepsilon^a s_{b-1}. \end{aligned} \tag{31}$$

Again, the first equation of (31) is only possible for even b, as the prime above 3 in $\mathbb{L}$ divides s_n only for even n. Also, for odd n, the following characterizations may be obtained:

$$\begin{aligned} s_{2^i n} &= 2^i(c+d\sqrt{6}), \quad \text{with } c, d \text{ odd and } c+d\equiv 0 \pmod 4, \\ t_{2^i n} &= 2+2^{2i+1}(c'+d'\sqrt{6}), \quad \text{with } c', d' \text{ odd}, \end{aligned} \qquad i=1,2,\ldots, \tag{32}$$

which may be checked by using (24).

As before, let $b\equiv 2^i \pmod{2^{i+1}}$ for some $i\geqq 1$. We'll show again that this is impossible. We use the fact that the second and third equation of (31) imply that

$$s_{b+1}\overline{s_{b-1}} = 9Y^2 - X^2 \in \mathbb{Z}, \tag{33}$$

where the bar denotes conjugation in $\mathbb{L}$.

Now, substitution of the expressions (32)—see also (22)—into the relations

$$s_{b+1}+s_{b-1}=2(3+\sqrt{6})s_b, \quad s_{b+1}-s_{b-1}=t_b,$$

and adding and subtracting the results, yields expressions for s_{b+1} and s_{b-1} which may be used to show that

$$s_{b+1}\overline{s_{b-1}} - \overline{s_{b+1}}s_{b-1} \equiv 2^{i+2}(c+3d)\sqrt{6} \equiv 2^{i+3}\sqrt{6} \pmod{2^{i+4}},$$

as $c+3d\equiv 2 \pmod 4$. This clearly implies that $s_{b+1}\overline{s_{b-1}} \notin \mathbb{Z}$. Hence $b=0$, and from (31) we deduce that $(X, Y)=(\sigma, 0)$.

For $i=4$ we have the same sequences (s_n) and (t_n) as in case $i=3$. From Table 3 we get

$$\begin{aligned} \frac{X-3Y}{3}(3+\sqrt{6}) &= \sigma\varepsilon^a s_b, \\ \frac{-X-3Y}{3}(3+\sqrt{6}) &= \sigma\varepsilon^a s_{b-2}, \\ -Y &= \sigma\varepsilon^a s_{b-1}. \end{aligned} \tag{34}$$

As in the previous case, it follows from the first equation of (34) that b is even. The third equation of (34) now implies that $a \equiv 0 \pmod 4$, as

$$s_{2n+1} \equiv \pm 1, \pm 3 \pmod 8.$$

The first relation of (32) can be extended inasmuch as c and d can be shown to satisfy

$$c+d \equiv 0 \pmod 8, \quad \text{provided } i \geqq 2.$$

Now either b or $b-2$ is divisible by 4. Suppose $b'=b$ or $b-2$ and $b' \equiv 2^i \pmod{2^{i+1}}$ for some $i \geqq 2$. Then

$$\varepsilon^a s_{b'}(-3+\sqrt{6}) \in \mathbb{Z} \tag{35}$$

according to the first or the second equation of (34). Further, by the first relation of (32),

$$\varepsilon^a s_{b'}(-3+\sqrt{6}) \equiv 2^i(-3c+6d+(c-3d)\sqrt{6}) \pmod{2^{i+3}}$$

with c,d odd and $c+d \equiv 0 \pmod 8$. But $c-3d \not\equiv 0 \pmod 8$ and this contradicts (35). Consequently, $b'=0$ so that $b=0$ or $b=2$, and this gives $(X, Y)=(3\sigma, \sigma), (-3\sigma, -\sigma)$ by (34).

The final case $i=5$ can be treated exactly like the first one. From Table 3 we read

$$\begin{aligned} \frac{-X+3Y}{6} &= \sigma\varepsilon^a s_b, \\ \frac{-X-3Y}{6} &= \sigma\varepsilon^a s_{b-1}. \end{aligned} \tag{36}$$

This implies that

$$\varepsilon^a s_b \in \mathbb{Z} \quad \text{and} \quad \varepsilon^a s_{b-1} \in \mathbb{Z},$$

and we proceed like we did in case $i=1$. We conclude that $b=0$ or $b=1$, which gives the solutions $(X, Y)=(3\sigma, \sigma), (-3\sigma, \sigma)$.

It is easy to check that the solutions found correspond to those given in the statement of the Proposition. The correspondences between (X, Y) and (u, v) of the Proposition are given by (10) and (11).

This completes the second proof. □

REFERENCES

1. A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

2. PERSI DIACONIS and R. L. GRAHAM, The Radon transform on $\mathbb{Z}_2^k$, *Pacific J. Math.* **118** (2) (1985), 323–345.

3. R. J. STROEKER, On quartic Thue equations with trivial solutions, *Math. Comp.* **52** (185) (1989), 175–187.

4. R. J. STROEKER and N. TZANAKIS, On the application of Skolem's p-adic method to the solution of Thue equations, *J. Number Theory* **29** (2) (1988), 166–195.

5. R. J. STROEKER and N. TZANAKIS, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms, *Acta. Arith.* **67** (2) (1994), 177–196.

6. N. TZANAKIS and B. M. M. DE WEGER, On the practical solution of the Thue equation, *J. Number Theory* **31** (2) (1989), 99–132.

7. B. M. M. DE WEGER, *Algorithms for Diophantine Equations* (PhD thesis, University of Leiden, 1987). Also appeared as CWI Tract **65**, Centre for Mathematics and Computer Science, Amsterdam 1989.

ECONOMETRIC INSTITUTE
ERASMUS UNIVERSITY
P.O. BOX 1738
3000 DR ROTTERDAM
THE NETHERLANDS

E-mail address: stroeker@wis.few.eur.nl, dweger@wis.few.eur.nl