J. reine angew. Math. 427 (1992), 137—156

Journal für die reine und angewandte Mathematik

A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number 2

By *B. M. M. de Weger*[1]) at Enschede

1. Introduction

In 1983 Antoniadis [An], studying the imaginary quadratic number fields with class number 2, showed that these fields, with only one exception, correspond to solutions of certain diophantine equations. In many cases he was able to show that these diophantine equations have no other solutions than those corresponding to the number fields, but he left some cases open, such as $X^6 + 4 = pY^2$ (which has been solved by Tzanakis [Tz] for $p = 17$, 41, 89 (the cases relevant for Antoniadis' results), and is still open for the other primes $p \equiv 1 \pmod 8$), and the diophantine system

$$\begin{cases} Y^3 - 1 = pX^2, & (1) \\ (5 + Y^3)^2 - 52 = 13Z^2, & (2) \end{cases}$$

where $p = 7, 31$ are the relevant cases for Antoniadis' work. For $p = 7$ Ljunggren [Lj] showed that equation (1) has only the solutions $(X, Y) = (\pm 1, 2), (\pm 3, 4), (\pm 39, 22)$, of which only the first pair leads to solutions of (2), namely with $Z = \pm 3$. For $p = 31$ the present author [dW1] showed that equation (1) has only the solutions $(X, Y) = (0, 1)$, $(\pm 2, 5)$, of which only the second pair leads to solutions of (2), namely with $Z = \pm 36$.

It is of interest to study equation (2) independent of (1), since it does not depend on p, so solving it would yield much more general results. The aim of this paper is to prove the following result, which was conjectured by Antoniadis ([An], Vermutung (2.5.9)).

Theorem 1. *The diophantine equation*

$$X^6 + 10X^3 - 27 = 13Y^2 \qquad (3)$$

[1]) The author is grateful to J. A. Antoniadis for drawing his attention to the problem, and to N. Tzanakis for discussions.

has only the solutions $(X, Y) = (2, \pm 3), (5, \pm 36)$.

In view of [An], Satz (1.6.1), this result yields a new proof of the fact that the only fields $\mathbb{Q}(\sqrt{-13p})$ with p not a multiple of 2 or 3 and having class number 2 are $\mathbb{Q}(\sqrt{-91})$ (with $p = 7$) and $\mathbb{Q}(\sqrt{-403})$ (with $p = 31$).

Our method of solving the hyperelliptic equation (3) is very similar to the method we used for solving the elliptic equation $Y^3 - 1 = 31X^2$ in [dW1]. So we first reduce the problem to a Thue equation, and then apply the method of [TW1], based on the theory of linear forms in logarithms, and computational diophantine approximation, to solve it.

To the author's best knowledge this is the first time that a sextic hyperelliptic equation has been solved completely by this method, although it has been known for some time that in principle it could be done (cf. [ShT], Chapter 6, giving also a survey of the history of super- and hyperelliptic equations). The Thue equation that we are led to is of degree 6, and the associated number field is totally real, which is a more complicated situation than in the cases that have been studied before. Namely, the number of variables in the unit equation that one is led to, equals the unit rank of the number field, thus 5 in this case.

However, very helpful facts here are that the mentioned sextic field has a quadratic and a cubic subfield, and is Galois. We will show that this implies that solving our sextic Thue equation with coefficients in $\mathbb{Z}$ is equivalent to solving a cubic Thue equation with coefficients in a quadratic number field (although we still restrict the variables to $\mathbb{Z}$). Such an equation has not yet been treated before, to the author's best knowledge. Moreover, the Galois group of the sextic field has a nice structure, imposed by the existence of subfields, that enables us to reduce the size of the problem: we will show that the number of variables in the unit equation can be reduced by one to 4. This implies a much better upper bound from the theory of linear forms in logarithms, and an easier computational problem of reducing this bound.

Moreover, this additional structure of the field is used to justify that the computations needed for the reduction of the bound are done for only one conjugate of the unit equation, whereas in general one has to do them for all six conjugates. Thus another reduction of the computation time by a factor 6 is established. Note that similar phenomena occur in [StTz], where the quartic equation $X^2 + 1 = 2Y^4$ is solved by a method that is essentially the same as ours.

2. Reduction to a cubic Thue equation with quadratic coefficients

In this section we reduce equation (3) to a Thue equation $F(x, y) = h$, where F is a cubic binary form with coefficients in the ring of integers of $\mathbb{Q}(\sqrt{13})$, x and y are the variables in $\mathbb{Z}$, and h is a unit of the ring of integers in $\mathbb{Q}(\sqrt{13})$.

Rewrite equation (3) as

$$Y^2 + 4 = 13\left(\frac{X^3 + 5}{13}\right)^2 \tag{4}$$

(note that $13 | X^3 + 5$). Factorizing over $\mathbb{Q}(i)$ yields:

$$(Y+2i)(Y-2i) = (3+2i)(3-2i)\left(\frac{X^3+5}{13}\right)^2 .$$

Note that $(Y+2i, Y-2i) | 4$, hence it is equal to a unit times $(1+i)^d$ for a $d \in \{0,1,2,3,4\}$. So

$$Y+2i = i^a(3+2i)^b(3-2i)^c(1+i)^d(u+vi)^2 ,$$

where now we may take $a, b, c, d \in \{0,1\}$ and $u, v \in \mathbb{Z}$. Taking norms we obtain

$$13\left(\frac{X^3+5}{13}\right)^2 = N(Y+2i) = 13^{b+c}2^d(u^2+v^2)^2 ,$$

so $a = 0$ or 1, $(b, c) = (0,1)$ or $(1,0)$, and $d = 0$. The cases $(b, c) = (0,1)$ and $(b, c) = (1,0)$ are equivalent (take conjugates). So assume $(b, c) = (0,1)$. Then equation (4) is equivalent to

$$\begin{cases} Y+2i = i^a(3-2i)(u+vi)^2 , \\ u^2+v^2 = (X^3+5)/13 . \end{cases}$$

The case $a = 1$, on equating imaginary parts, leads to $3u^2+4uv-3v^2 = 2$, which is impossible. Thus $a = 0$, and we derive, on equating real and imaginary parts,

$$\begin{cases} u^2-3uv-v^2 = -1 , & (5) \\ 18u^2-15uv+8v^2 = X^3 , & (6) \\ 3u^2+4uv-3v^2 = Y . & (7) \end{cases}$$

Equations (5) and (6) give valuable information on u and v, whereas equation (7) can only be used to find Y from u, v. Theorem 1 now follows easily from the following result.

Theorem 2. *The system of equations* (5) *and* (6) *has only the solutions*

$$(u, v, X) = (0, \pm 1, 2), (\pm 3, \pm 1, 5).$$

It is well known how to find the solutions of equation (5), since it is essentially a Pell equation. They are all given by $(u, v) = \pm(u_{2n}, u_{2n-1})$ for arbitrary $n \in \mathbb{Z}$, where

$$u_n = \frac{1}{\sqrt{13}}\alpha^n - \frac{1}{\sqrt{13}}\bar{\alpha}^n , \tag{8}$$

with $\alpha = \frac{3+\sqrt{13}}{2}$, $\bar{\alpha} = \frac{3-\sqrt{13}}{2}$. We will use this result later on.

Equation (6) leads to

$$(12u-5v)^2 + 39v^2 = (2X)^3 .$$

We factorize over $\mathbb{Q}(\sqrt{-39})$, which has class number 4. Let $\mathfrak{a}$ be a prime ideal not dividing 78, that divides both $(12u-(5+\sqrt{-39})v)$ and its conjugate ideal. Then $\mathfrak{a}|(2\sqrt{-39}v)$, hence $\mathfrak{a}|(v)$, and it follows that $\mathfrak{a}|(12u)$, hence $\mathfrak{a}|(u)$. This contradicts that u and v are relatively prime (by (5)). So $((12u-(5+\sqrt{-39})v), (12u-(5-\sqrt{-39})v))$ consists of prime ideals dividing 2, 3 and 13 only. Note that 2 and 5 split, whereas 3 and 13 ramify. Thus there are prime ideals $\mathfrak{b}$, $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{u}$ such that

$$(2)=\mathfrak{b}\bar{\mathfrak{b}},\quad (3)=\mathfrak{p}^2,\quad (5)=\mathfrak{u}\bar{\mathfrak{u}},\quad (13)=\mathfrak{q}^2.$$

Moreover, we have the relations

$$\mathfrak{b}^4=\left(\frac{5+\sqrt{-39}}{2}\right),\quad \mathfrak{bu}=\left(\frac{1+\sqrt{-39}}{2}\right).$$

There exists an ideal $\mathfrak{a}$ (not necessarily prime, not necessarily principal, but integral), such that

$$(12u-(5+\sqrt{-39})v)=\mathfrak{b}^a\bar{\mathfrak{b}}^b\mathfrak{p}^c\mathfrak{q}^d\mathfrak{a}^3, \tag{9}$$

where $a, b, c, d\in\{0,1,2\}$. Take norms, to obtain

$$(2X)^3=2^{a+b}3^c13^dN(\mathfrak{a})^3,$$

hence $c=d=0$ and $a+b=0$ or 3, thus $(a,b)=(0,0),(1,2)$ or $(2,1)$. Note that the solutions $(u,v)=(0,\pm1)$ lead to $(a,b)=(2,1)$ and $\mathfrak{a}=\mathfrak{b}$, and the solutions $(u,v)=\pm(3,1)$ lead to $(a,b)=(2,1)$ and $\mathfrak{a}=\bar{\mathfrak{u}}$.

First let $(a,b)=(0,0)$. Then

$$(12u-(5+\sqrt{-39})v)=\mathfrak{a}^3, \tag{10}$$

and $\mathfrak{a}$ is necessarily a principal ideal. Thus there are $e, f\in\mathbb{Z}$ with

$$\mathfrak{a}=\left(\frac{e+f\sqrt{-39}}{2}\right).$$

Substituting this into (10), and equating real and imaginary parts, we obtain

$$\begin{cases} 8(12u-5v)=e^3-117ef^2,\\ \quad -8v=3e^2f-39f^3,\end{cases}$$

hence $3|v$. Since (5), by (8), yields $v=\pm u_{2n-1}$, and $3\nmid u_n$ for odd n, we have a contradiction. Also the first equation of the above system leads to a contradiction by (5) and (8), by considering it modulo 13.

Next let $(a, b) = (1, 2)$. Then

$$(12u - (5 + \sqrt{-39})v) = \mathfrak{b}\bar{\mathfrak{b}}^2\mathfrak{a}^3,$$

and now $\mathfrak{a}$ is not a principal ideal. But note that

$$\left(6u - \frac{5+\sqrt{-39}}{2}v\right) = \bar{\mathfrak{b}}\mathfrak{a}^3 = \left(\frac{5-\sqrt{-39}}{2}\right)(\mathfrak{a}\bar{\mathfrak{b}}^{-1})^3, \tag{11}$$

so $\mathfrak{a}\bar{\mathfrak{b}}^{-1}$ is a principal ideal, however not necessarily integral, but $(2)\mathfrak{a}\bar{\mathfrak{b}}^{-1}$ is integral. Thus there are $e, f \in \mathbb{Z}$ with

$$\mathfrak{a} = \bar{\mathfrak{b}}\left(\frac{e+f\sqrt{-39}}{4}\right).$$

Substituting this expression for $\mathfrak{a}$ into (11), and equating real and imaginary parts, we obtain (neglecting without loss of generality signs)

$$\begin{cases} 5e^3 + 117e^2f - 585ef^2 - 1521f^3 = 64(12u - 5v), \\ -e^3 + 15e^2f + 117ef^2 - 195f^3 = -64v. \end{cases}$$

Adding 5 times the second equation to the first one, we get, after dividing by 64,

$$12u - 10v = 3e^2f - 39f^3,$$

implying $3 \mid v$. As in the case $(a, b) = (0, 0)$ we reach a contradiction.

It follows that $(a, b) = (2, 1)$. Then

$$(12u - (5 + \sqrt{-39})v) = \mathfrak{b}^2\bar{\mathfrak{b}}\mathfrak{a}^3,$$

and again $\mathfrak{a}$ is not a principal ideal. But note that

$$\left(6u - \frac{5+\sqrt{-39}}{2}v\right) = \mathfrak{b}\mathfrak{a}^3 = \left(\frac{5+\sqrt{-39}}{2}\right)(\mathfrak{a}\mathfrak{b}^{-1})^3, \tag{12}$$

so $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal ideal, however not necessarily integral, but $(2)\mathfrak{a}\mathfrak{b}^{-1}$ is integral. Thus there are $e, f \in \mathbb{Z}$ with

$$\mathfrak{a} = \mathfrak{b}\left(\frac{e+f\sqrt{-39}}{4}\right).$$

Substituting this expression for $\mathfrak{a}$ into (12), and equating real and imaginary parts, we obtain (neglecting without loss of generality signs)

$$\begin{cases} 5e^3 - 117e^2f - 585ef^2 + 1521f^3 = 64(12u - 5v), \\ e^3 + 15e^2f - 117ef^2 - 195f^3 = -64v, \end{cases}$$

hence, by (5) and (8), assuming without loss of generality that $(u, v) = -(u_{2n}, u_{2n-1})$, we find

$$\begin{cases} 5e^3 - 117e^2f - 585ef^2 + 1521f^3 = -768u_{2n} + 320u_{2n-1}, & (13) \\ e^3 + 15e^2f - 117ef^2 - 195f^3 = 64u_{2n-1}. & (14) \end{cases}$$

Clearly this system is equivalent to the at first sight somewhat simpler system

$$\begin{cases} (e^2 - 13f^2)f = 4u_{2n}, & (15) \\ e(e^2 - 117f^2) = -60u_{2n} + 64u_{2n-1}. & (16) \end{cases}$$

Equations (13)–(16) are examples of what one could call 'Thue-recurrence equations'. About such equations not much seems to be known in general, not even conditions for the finiteness of the number of solutions. Some numerical experiments (up to $\max\{|e|, |f|\} \leqq 1000$ only) led us to the following conjecture. Let

$$w_n = \alpha^n + \bar{\alpha}^n$$

for all $n \in \mathbb{Z}$.

Conjecture 1. (i) *Equation* (13) *has only the solutions* $(e,f,n) = (1, -1, 1), (4, 0, 0), (-29, 5, 0), (-443, -5, 6)$.

(ii) *Equation* (14) *has only the solutions* $(e,f,n) = (1, -1, 0), (1, -1, 1), (4, 0, 0), (4, 0, 1), (-5, 1, 2), (-5, 1, -1), (7, 1, 0), (7, 1, 1), (-32, 4, 4), (-32, 4, -3), (49, -1, 4), (49, -1, -3)$.

(iii) *Equation* (15) *has only the solutions* $(e,f,n) = (e, 0, 0), (w_{2n}, u_{2n}, n), (-w_{2n}, u_{2n}, n), (w_{2m-1} + 2, u_{2m-1}, 2m-1), (-w_{2m-1} - 2, u_{2m-1}, 2m-1), (w_{2m-1} - 2, -u_{2m-1}, 2m-1), (-w_{2m-1} + 2, -u_{2m-1}, 2m-1)$ *for* $e, n, m \in \mathbb{Z}$.

(iv) *Equation* (16) *has only the solutions* $(e,f,n) = (1, -1, 1), (1, 1, 1), (4, 0, 0)$.

We have no idea how to prove this conjecture. We even will not be surprised if the conjecture (especially parts (i) and (ii)) turns out to be false. However, for the proof of Theorem 2, our present aim, there is no need to study equations (13)–(16) independently from each other, since (e.g.) both equations (15) and (16) should hold for the same e, f, n. Therefore we now search for a linear combination of these two equations, that is equivalent to the system of (15) and (16), and has a simpler form. We find for a $\gamma \in \mathbb{Q}(\sqrt{13})$

$$\begin{aligned} e^3 - 117ef^2 - \gamma(-e^2f + 13f^3) &= 4(\gamma - 15)u_{2n} + 64u_{2n-1} \\ &= \frac{4}{\sqrt{13}}((\gamma - 15)\alpha + 16)\alpha^{2n-1} - \frac{4}{\sqrt{13}}((\gamma - 15)\bar{\alpha} + 16)\bar{\alpha}^{2n-1}. \end{aligned}$$

With $\gamma = 39 + 8\sqrt{13}$ the second term vanishes:

$$((39 + 8\sqrt{13}) - 15)\bar{\alpha} + 16 = 0,$$

and further

$$((39 + 8\sqrt{13}) - 15)\alpha + 16 = -16\sqrt{13} \cdot \alpha,$$

hence we have derived the equation

$$(17) \quad e^3 + (39 + 8\sqrt{13})e^2 f - 117ef^2 - (507 + 104\sqrt{13})f^3 = 64\left(\frac{3+\sqrt{13}}{2}\right)^{2n}.$$

This equation has a nice form, since the left hand side is a binary form with quadratic integers as coefficients, and the right hand side is a constant times a unit, so the binary recurrence has disappeared. Equation (17) could be called a Thue equation with coefficients in $\mathbb{Q}(\sqrt{13})$. Note that subtracting its conjugate from equation (17) returns equation (15). Hence (17) is equivalent to the system of (15) and (16), and no information has been lost by making the linear combination. Other combinations of equations (15) and (16) can be made (i.e. other choices for γ), but the one given above seems to be the only one that leads somewhere.

Considering (17) modulo 4 it is easy to see that $4 | e + f$. Now put

$$x = \frac{e+f}{4}, \quad y = f.$$

Then we see that (17) is equivalent to

$$(18) \quad x^3 + (9 + 2\sqrt{13})x^2 y - (12 + \sqrt{13})xy^2 - \frac{11 + 3\sqrt{13}}{2} y^3 = \left(\frac{3+\sqrt{13}}{2}\right)^{2n}.$$

This is the Thue equation announced in the introduction, with coefficients in the ring of integers of $\mathbb{Q}(\sqrt{13})$, and variables still in $\mathbb{Z}$. In the next section we will prove the following result.

Theorem 3. *Equation* (18) *has only the solutions* $(x, y, n) = (1, 0, 0), (0, -1, 1)$.

Note that Theorem 3 implies Theorem 2.

We conclude this section with some remarks. By adding equation (18) to its conjugate, we obtain the Thue-recurrence equation

$$(19) \quad 2x^3 + 18x^2 y - 24xy^2 - 11y^3 = w_{2n},$$

with w_n as defined just before Conjecture 1. From a small numerical experiment we arrived at the following conjecture.

Conjecture 2. *Equation* (19) *has only the solutions* $(x, y, n) = (1, 0, 0)$, $(0, -1, 1)$, $(0, -1, -1)$, $(3, 2, 0)$.

Of these solutions the last one does not essentially come from solutions of (18).

What one might also do is to take norms in (18). This gives the following sextic Thue equation:

$$x^6 + 18x^5y + 5x^4y^2 - 175x^3y^3 + 110x^2y^4 + 93xy^5 + y^6 = 1\,, \tag{20}$$

having exactly the solutions $(x, y) = (\pm 1, 0), (0, \pm 1)$ (this follows at once from Theorem 3). It is a 'common' Thue equation, i.e. its coefficients are in $\mathbb{Z}$. In solving (20), (18) still seems to be the best starting point.

3. Solving the Thue equation

3.1. The sextic field. Let ξ be a root of

$$t^3 + (9 + 2\sqrt{13})t^2 - (12 + \sqrt{13})t - \frac{11 + 3\sqrt{13}}{2} = 0\,, \tag{21}$$

(cf. (18)), hence of

$$t^6 + 18t^5 + 5t^4 - 175t^3 + 110t^2 + 93t + 1 = 0\,, \tag{22}$$

(cf. (20)). Put $K = \mathbb{Q}(\xi)$, then $[K: \mathbb{Q}] = 6$, and $\mathbb{Q}(\sqrt{13}) \subset K$. The conjugates of ξ in K are numbered as follows:

$$\xi^{(1)} = -17.0870386250\ldots, \quad \xi^{(2)} = -0.4731926214\ldots, \quad \xi^{(3)} = 1.3491286955\ldots$$

which are the roots of (21), and

$$\xi^{(4)} = -3.9228341276\ldots, \quad \xi^{(5)} = 2.1448322141\ldots, \quad \xi^{(6)} = -0.0108955356\ldots$$

which are the roots of the conjugate of (21) over $\mathbb{Q}(\sqrt{13})$. Thus K is a totally real sextic field. The discriminant of the cubic polynomial of (21) is $13^4\alpha^2$, and the discriminant of the sextic polynomial of (22) is 13^{17}. We need some more data on the field K. In the Tables in [PWZ] there is one totally real sextic field over $\mathbb{Q}$ having $\mathbb{Q}(\sqrt{13})$ as a subfield, namely $\mathbb{Q}(\theta)$ with θ a root of

$$t^6 + t^5 - 5t^4 - 4t^3 + 6t^2 + 3t - 1 = 0\,.$$

The discriminant of $\mathbb{Q}(\theta)$ is 13^5. After some numerical experimentation we found the relation

$$\xi = -2 + 8\theta + 3\theta^2 - 8\theta^3 - \theta^4 + 2\theta^5\,,$$

which can easily be verified exactly (not only numerically) once it is known. Thus in fact $K = \mathbb{Q}(\xi) = \mathbb{Q}(\theta)$, and from the Tables in [PWZ] we learn that a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_K$ of K is $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$, and a system of fundamental units of $\mathcal{O}_K$ is $\{\theta, \eta, \phi, \psi, \chi\}$, with

$$\eta = 1 - \theta, \quad \phi = 1 + \theta, \quad \psi = -1 - \theta + \theta^2, \quad \chi = 3 - \theta^2 .$$

Note that $\xi = -\theta^6 \eta^3 \phi^4 \psi^{-2} \chi^4$. The field K is Galois, and its Galois group is generated by ϱ, σ given by

$$\varrho(\theta) = 5\theta - 5\theta^3 + \theta^5, \quad \sigma(\theta) = -3\theta + \theta^3 ,$$

satisfying $\varrho^2 = \sigma^3 = \mathrm{id}$. The conjugates of θ are numbered, in accordance with the numbering of the conjugates of ξ, as follows:

$$\begin{aligned} \theta^{(1)} &= -1.9418836348\ldots, \\ \theta^{(2)} = \sigma(\theta^{(1)}) &= -1.4970214963\ldots, \\ \theta^{(3)} = \sigma^2(\theta^{(1)}) &= \ \ 1.1361294934\ldots, \end{aligned}$$

which are the roots of

$$t^3 + \frac{1+\sqrt{13}}{2} t^2 - t - \frac{3+\sqrt{13}}{2} = 0 , \tag{23}$$

and

$$\begin{aligned} \theta^{(4)} = \varrho(\theta^{(1)}) &= -0.7092097740\ldots, \\ \theta^{(5)} = \varrho(\theta^{(2)}) = \sigma(\theta^{(4)}) &= \ \ 1.7709120513\ldots, \\ \theta^{(6)} = \varrho(\theta^{(3)}) = \sigma^2(\theta^{(4)}) &= \ \ 0.2410733605\ldots, \end{aligned}$$

which are the roots of the conjugate of (23) over $\mathbb{Q}(\sqrt{13})$.

Put $\beta = \theta \eta^{-1} \phi^{-1} \psi$. Note that $\beta^{(1)} = \alpha$, and $\beta = \theta \sigma(\theta) \sigma^2(\theta)$, hence

$$\beta^{(1)} = \beta^{(2)} = \beta^{(3)} = \alpha, \quad \beta^{(4)} = \beta^{(5)} = \beta^{(6)} = \bar{\alpha} .$$

Further note that $\theta \varrho(\theta) = \phi^{-1} \chi^{-1}$ is a root of $t^3 + t^2 - 4t + 1 = 0$, inducing the cubic subfield of K (also given in the Tables of [PWZ]).[2])

3.2. The unit equation and the linear form in logarithms. In this section we will derive from (18) a unit equation, study it, and relate it to a linear form in logarithms.

Let (x, y, n) be any solution of (18), i.e. of

$$(x - y\xi)(x - y\sigma(\xi))(x - y\sigma^2(\xi)) = \beta^{2n} .$$

[2]) After this paper was finished, L. Washington pointed out to me that the field K is generated over $\mathbb{Q}$ by the cyclotomic unit $e^{\frac{2}{13}\pi i} + e^{-\frac{2}{13}\pi i}$. Using this might lead to some improvements in the sequel.

We may assume that $y \neq 0$. It follows at once that $x - y\xi$ is a unit of $\mathcal{O}_K$, say ε. Note that $\varepsilon^{(1)}\varepsilon^{(2)}\varepsilon^{(3)} = \alpha^{2n}$. From

$$x - y\xi = \varepsilon, \quad x - y\sigma(\xi) = \sigma(\varepsilon), \quad x - y\sigma^2(\xi) = \sigma^2(\varepsilon)$$

we eliminate x and y, and so obtain the 'unit equation'

$$(\sigma(\xi) - \sigma^2(\xi))\varepsilon + (\sigma^2(\xi) - \xi)\sigma(\varepsilon) + (\xi - \sigma(\xi))\sigma^2(\varepsilon) = 0\,. \tag{24}$$

Here the unknown is ε. By Dirichlet's Unit Theorem we may write

$$\varepsilon = \pm\theta^{a_1}\eta^{a_2}\phi^{a_3}\psi^{a_4}\chi^{a_5}$$

for unknowns $a_1, \ldots, a_5 \in \mathbb{Z}$.

We will now show that one solution ε of (24) gives rise to infinitely many others. Namely, multiplying (24) by β^m for some $m \in \mathbb{Z}$, we find that whenever

$$\varepsilon = \varepsilon_0 = \pm\theta^{a_1}\eta^{a_2}\phi^{a_3}\psi^{a_4}\chi^{a_5}$$

satisfies (24), so does

$$\varepsilon = \beta^m\varepsilon_0 = \pm\theta^{a_1+m}\eta^{a_2-m}\phi^{a_3-m}\psi^{a_4+m}\chi^{a_5}\,.$$

We now choose m such that one of the terms vanishes, say the term with the ψ. In other words, we always take $m = -a_4$. Thus we may assume that $a_4 = 0$, and $\varepsilon = \pm\theta^{a_1}\eta^{a_2}\phi^{a_3}\chi^{a_5}$.

In this way we have established a reduction of the number of variables in the unit equation from 5 to 4. In general a Thue equation leads to a unit equation such as (24) in which the number of variables (exponents) equals the unit rank of the associated number field. The above argument shows that when the number field has additional structure, this number of variables might be reduced. It is probable that something like this often can be done when the number field is Galois and has a proper subfield of degree at least 3. Such a reduction is important, because the (computational) complexity of solving the unit equation is a quickly increasing function of this number of variables.

Given a solution $\varepsilon = \pm\theta^{a_1}\eta^{a_2}\phi^{a_3}\chi^{a_5}$ of (24), we must be able to decide whether it comes from a solution (x, y, n) of (18). This can easily be done as follows. Note that if $x - y\xi = \beta^m\varepsilon$, then

$$\begin{cases} x - y\xi^{(1)} = \alpha^m\varepsilon^{(1)}, \\ x - y\xi^{(2)} = \alpha^m\varepsilon^{(2)}, \end{cases}$$

whence

$$x = \alpha^m\frac{\xi^{(2)}\varepsilon^{(1)} - \xi^{(1)}\varepsilon^{(2)}}{\xi^{(2)} - \xi^{(1)}}, \quad y = \alpha^m\frac{\varepsilon^{(1)} - \varepsilon^{(2)}}{\xi^{(2)} - \xi^{(1)}}\,. \tag{25}$$

Further, $x - y\xi^{(4)} = \bar{\alpha}^m \varepsilon^{(4)} = (-\alpha)^{-m}\varepsilon^{(4)}$, thus on substituting (25) we obtain

$$(-\alpha^2)^m = \frac{\varepsilon^{(4)}(\xi^{(2)} - \xi^{(1)})}{\varepsilon^{(1)}(\xi^{(2)} - \xi^{(4)}) - \varepsilon^{(2)}(\xi^{(1)} - \xi^{(4)})}. \tag{26}$$

In this formula m is the only unknown, so it can be computed and checked for being integral. Then (25) shows how to find x and y.

We now relate (24) to a linear form in logarithms. Note that (24) is equivalent to

$$\frac{\xi - \sigma^2(\xi)}{\xi - \sigma(\xi)} \cdot \frac{\sigma(\varepsilon)}{\sigma^2(\varepsilon)} - 1 = -\frac{\sigma(\xi) - \sigma^2(\xi)}{\sigma(\xi) - \xi} \cdot \frac{\varepsilon}{\sigma^2(\varepsilon)}. \tag{27}$$

Let $i_0 \in \{1, \ldots, 6\}$ be such that $|\varepsilon^{(i_0)}| = \min_{1 \leq i \leq 6} |\varepsilon^{(i)}|$. Later on we will show that for this i_0th conjugate the right hand side of (27) is extremely close to zero. Therefore it is sensible to study

$$\Lambda_i = \log \left| \frac{\xi^{(i)} - \sigma^2(\xi^{(i)})}{\xi^{(i)} - \sigma(\xi^{(i)})} \cdot \frac{\sigma(\varepsilon^{(i)})}{\sigma^2(\varepsilon^{(i)})} \right|$$

for $i = i_0$, since it is a linear form in logarithms of algebraic numbers (as we'll see in a moment), which is also extremely close to zero. First, we'll derive a useful expression for Λ_i. Note that

$$\frac{\xi - \sigma^2(\xi)}{\xi - \sigma(\xi)} = 1 - 6\theta - 4\theta^2 + 9\theta^3 + \theta^4 - 2\theta^5 = \theta^{-2}\eta^{-1}\phi^{-3}\psi\chi^{-3}$$

is a unit of $\mathcal{O}_K$. Further, we have

$\cdot$	$\sigma(\cdot)$	$\sigma^2(\cdot)$	$\varrho(\cdot)$
θ	$-\theta \quad \chi$	$-\theta^{-1}\eta^{-1}\phi^{-1}\psi \quad \chi^{-1}$	$\theta^{-1} \quad \phi^{-1} \quad \chi^{-1}$
η	$-\theta^2 \quad \eta^2 \quad \phi^4 \quad \psi^{-1}\chi^3$	$\theta^{-2}\eta^{-3}\phi^{-4}\psi \quad \chi^{-3}$	$\theta^2 \quad \eta \quad \phi \quad \psi^{-1}\chi$
ϕ	$\eta^{-1}\phi^{-2} \quad \chi^{-1}$	$\eta \quad \phi \quad \chi$	$-\theta^{-2}\eta^{-2}\phi^{-3}\psi \quad \chi^{-2}$
ψ	$\theta^2 \quad \phi \quad \chi$	$-\eta^{-2}\phi^{-3}\psi \quad \chi^{-1}$	ψ^{-1}
χ	$-\theta^{-2}\eta^{-1}\phi^{-1}\psi \quad \chi^{-2}$	$\theta^2 \quad \eta \quad \phi \quad \psi^{-1}\chi$	$-\theta^2 \quad \eta^2 \quad \phi^4 \quad \psi^{-1}\chi^3$

Put

$$\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_5 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 5 & -2 & -2 \\ 1 & 8 & -3 & -2 \\ -1 & -2 & 0 & 2 \\ 2 & 6 & -2 & -3 \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} -1 \\ -3 \\ 1 \\ -3 \end{pmatrix}.$$

With $\varepsilon = \pm\theta^{a_1}\eta^{a_2}\phi^{a_3}\chi^{a_5}$ we now obtain from the above table

$$\Lambda_i = b_2 \log|\eta^{(i)}| + b_3 \log|\phi^{(i)}| + b_4 \log|\theta^{(i)-2}\psi^{(i)}| + b_5 \log|\chi^{(i)}|,$$

where $\mathbf{b} = \mathbf{c} + T\mathbf{a}$. Note that T is invertible, and

$$T^{-1} = \begin{pmatrix} -2 & 0 & 1 & 2 \\ -1 & \frac{2}{3} & -\frac{1}{3} & 0 \\ -2 & 1 & -1 & 0 \\ -2 & \frac{2}{3} & \frac{2}{3} & 1 \end{pmatrix},$$

so that $\mathbf{a} = -T^{-1}\mathbf{c} + T^{-1}\mathbf{b}$ with $-T^{-1}\mathbf{c} = \left(3, \frac{4}{3}, 2, \frac{7}{3}\right)^t$.

Thus Λ_i is a homogeneous linear form in logarithms of algebraic numbers with 4 terms, and thus 4 unknowns b_2, b_3, b_4, b_5. Note that $\Lambda_i = 0$ if and only if $\mathbf{b} = \mathbf{0}$, which is impossible since then $\mathbf{a}$ is not integral.

Note that the solution $x = 1$, $y = 0$ of (18) yields $\varepsilon = 1$, $\mathbf{a} = \mathbf{0}$, $\mathbf{b} = \mathbf{c}$, so for this case (27) reads

$$\theta^{-2}\eta^{-1}\phi^{-3}\psi\chi^{-3} - 1 = -\theta^{-4}\eta^{-4}\phi^{-6}\psi^2\chi^{-5}.$$

And the solution $x = 0$, $y = -1$ of (18) yields $\varepsilon = \xi$, with a priori $a_1 = 6$, $a_2 = 3$, $a_3 = 4$, $a_4 = -2$, $a_5 = 4$. Thus the unit equation (24) has to be multiplied by β^2 in order to obtain $a_4 = 0$. Then ε becomes $\beta^2\xi$, with $\mathbf{a} = (8, 1, 2, 4)^t$, hence $\mathbf{b} = (0, -1, -1, 3)^t$, and (27) now reads

$$-\theta^2\phi^{-1}\psi^{-1}\chi^3 - 1 = -\theta^6\eta^2\phi^2\psi^{-3}\chi^4.$$

We return to the general case. Equation (27) can be written as

$$\eta^{b_2}\phi^{b_3}(\theta^{-2}\psi)^{b_4}\chi^{b_5} - 1 = \pm\eta^{d_2}\phi^{d_3}(\theta^{-2}\psi)^{d_4}\chi^{d_5} \tag{28}$$

(where the d_i can in some easy way be determined from the a_i). Applying σ or ϱ to this equation we see that one solution $\mathbf{b}$ leads to other ones. More specifically, put

$$\Sigma = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 4 & -2 & 1 & -1 \\ -1 & 0 & 0 & 1 \\ 3 & -1 & -1 & -2 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & -2 & 0 & 2 \\ 1 & -3 & 2 & 4 \\ -1 & 1 & -1 & -1 \\ 1 & -2 & 2 & 3 \end{pmatrix}.$$

Then Σ is associated with σ as follows:

$$\begin{pmatrix} y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix} = \Sigma \begin{pmatrix} x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

if and only if

$$\eta^{y_2}\phi^{y_3}(\theta^{-2}\psi)^{y_4}\chi^{y_5} = \sigma\left(\eta^{x_2}\phi^{x_3}(\theta^{-2}\psi)^{x_4}\chi^{x_5}\right),$$

and P is associated with ϱ in the analogous way. Note that $\Sigma^3 = P^2 = \mathrm{Id}$. Hence any solution $\mathbf{b} = (b_2, b_3, b_4, b_5)^t$ of (28) belongs to a class of six solutions:

$$\mathscr{B} = \{\mathbf{b}, \Sigma\mathbf{b}, \Sigma^2\mathbf{b}, P\mathbf{b}, \Sigma P\mathbf{b}, \Sigma^2 P\mathbf{b}\}.$$

When for a solution $\mathbf{b}$ we consider the linear form Λ_{i_0}, we have already chosen a specific conjugate, the i_0th. Note that then $\Sigma\mathbf{b}$ corresponds to $\Lambda_{i_0-1 \pmod 3}$, and $P\mathbf{b}$ to $\Lambda_{i_0-1 \pmod 6}$. Hence the above set $\mathscr{B}$ corresponds exactly to $\{\Lambda_1, \ldots, \Lambda_6\}$. In other words, without loss of generality we may take $i_0 = 1$, find all the solutions of (27) for which $|\varepsilon^{(1)}|$ is minimal among the $|\varepsilon^{(i)}|$, and recover all other solutions by applying all possible combinations of σ and ϱ. Thus, due to the additional structure of the sextic field, the amount of computational work to be done is reduced considerably again, since only one value for i_0 has to be dealt with, in stead of six.

3.3. An upper bound. We now study Λ_1, in order to obtain an upper bound for its absolute value, depending on the variables. Put $B = \max\{|b_2|, |b_3|, |b_4|, |b_5|\}$. We start with relating $|y|$ and B. As in [TW1] we derive sharp upper and lower bounds for $|\varepsilon^{(i)}|$ for $i = 1, \ldots, 6$. We follow the arguments of the proofs of Lemmas 1.1, 1.2 and 2.1 of [TW1]. We do not apply these lemmas directly, since they are based on an a priori unknown i_0, whereas we now know $i_0 = 1$, which enables us to improve the bounds considerably.

Assuming that $|\varepsilon^{(1)}| \leqq |\varepsilon^{(i)}|$ for $i = 2, \ldots, 6$, we will prove the following results:

$$|\varepsilon^{(1)}| \leqq 2.42 \cdot 10^{-5} \frac{1}{|y|^5}, \tag{29}$$

$$|\varepsilon^{(1)}| \geqq 7.55 \cdot 10^{-7} \frac{1}{|y|^5}, \tag{30}$$

$$|\varepsilon^{(i)}| \leqq \left(|\xi^{(1)} - \xi^{(i)}| + 2.42 \cdot 10^{-5}\right)|y| \quad \text{for } i \neq 1, \tag{31}$$

$$|\varepsilon^{(i)}| \geqq \frac{1}{2}|\xi^{(1)} - \xi^{(i)}||y| \quad \text{for } i \neq 1. \tag{32}$$

Namely, for $i \neq 1$ we have

$$|y||\xi^{(1)} - \xi^{(i)}| = |\varepsilon^{(i)} - \varepsilon^{(1)}| \leqq |\varepsilon^{(i)}| + |\varepsilon^{(1)}| \leqq 2|\varepsilon^{(i)}|,$$

which proves (32); by (32) we obtain

$$|\varepsilon^{(1)}| = \prod_{i=2}^{6} \frac{1}{|\varepsilon^{(i)}|} \leqq \frac{2^5}{\prod_{i=2}^{6} |\xi^{(1)} - \xi^{(i)}|} \cdot \frac{1}{|y|^5} \leqq 2.42 \cdot 10^{-5} \frac{1}{|y|^5},$$

which proves (29); by (29) and $|y| \geqq 1$ we find

$$|\varepsilon^{(i)}| = |x - y\xi^{(i)}| \leqq |x - y\xi^{(1)}| + |y||\xi^{(1)} - \xi^{(i)}|$$
$$\leqq 2.42 \cdot 10^{-5} \frac{1}{|y|^5} + |y||\xi^{(1)} - \xi^{(i)}| \leqq (|\xi^{(1)} - \xi^{(i)}| + 2.42 \cdot 10^{-5})|y|,$$

which proves (31), and finally (31) implies

$$|\varepsilon^{(1)}| = \prod_{i=2}^{6} \frac{1}{|\varepsilon^{(i)}|} \geqq \frac{1}{\prod_{i=2}^{6} (|\xi^{(1)} - \xi^{(i)}| + 2.42 \cdot 10^{-5})} \cdot \frac{1}{|y|^5} \geqq 7.55 \cdot 10^{-7} \frac{1}{|y|^5},$$

which proves (30). Now we estimate $|\Lambda_1|$. By (27), (29) and (32) we have

$$\left| \frac{\xi^{(1)} - \sigma^2(\xi^{(1)})}{\xi^{(1)} - \sigma(\xi^{(1)})} \cdot \frac{\sigma(\varepsilon^{(1)})}{\sigma^2(\varepsilon^{(1)})} - 1 \right| = \left| \frac{\xi^{(2)} - \xi^{(3)}}{\xi^{(2)} - \xi^{(1)}} \right| \left| \frac{\varepsilon^{(1)}}{\varepsilon^{(3)}} \right| \leqq \left| \frac{\xi^{(2)} - \xi^{(3)}}{\xi^{(2)} - \xi^{(1)}} \right| \frac{2.42 \cdot 10^{-5}}{\frac{1}{2}|\xi^{(1)} - \xi^{(3)}|} \cdot \frac{1}{|y|^6}$$
$$< 2.88 \cdot 10^{-7} \frac{1}{|y|^6}.$$

By $|y| \geqq 1$ we find that $\dfrac{\xi^{(1)} - \sigma^2(\xi^{(1)})}{\xi^{(1)} - \sigma(\xi^{(1)})} \cdot \dfrac{\sigma(\varepsilon^{(1)})}{\sigma^2(\varepsilon^{(1)})}$ is positive, hence it equals e^{Λ_1}. It follows that

$$|\Lambda_1| < 1.001 |e^{\Lambda_1} - 1| < 2.89 \cdot 10^{-7} \frac{1}{|y|^6}. \tag{33}$$

Next we derive an upper bound for B in terms of $|y|$. Let $I = \{i_1, \ldots, i_4\} \subset \{1, \ldots, 6\}$, and consider the matrix

$$U_I = \begin{pmatrix} \log|\eta^{(i_1)}| & \log|\phi^{(i_1)}| & \log|\theta^{(i_1)^{-2}}\psi^{(i_1)}| & \log|\chi^{(i_1)}| \\ \vdots & \vdots & \vdots & \vdots \\ \log|\eta^{(i_4)}| & \log|\phi^{(i_4)}| & \log|\theta^{(i_4)^{-2}}\psi^{(i_4)}| & \log|\chi^{(i_4)}| \end{pmatrix}.$$

We now have, by the definitions of $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and T,

$$U_I \mathbf{b} = \begin{pmatrix} \log|\Lambda_{i_1}| \\ \vdots \\ \log|\Lambda_{i_4}| \end{pmatrix} = U_I \mathbf{c} + \begin{pmatrix} \log\left|\dfrac{\sigma(\varepsilon^{(i_1)})}{\sigma^2(\varepsilon^{(i_1)})}\right| \\ \vdots \\ \log\left|\dfrac{\sigma(\varepsilon^{(i_4)})}{\sigma^2(\varepsilon^{(i_4)})}\right| \end{pmatrix}.$$

By inspection it can be shown that U_I is invertible if and only if

$$\#(I\cap\{1,2,3\}) = \#(I\cap\{4,5,6\}) = 2\,.$$

In these cases,

$$\mathbf{b} = \mathbf{c} + U_I^{-1}\begin{pmatrix} \log\left|\dfrac{\sigma(\varepsilon^{(i_1)})}{\sigma^2(\varepsilon^{(i_1)})}\right| \\ \vdots \\ \log\left|\dfrac{\sigma(\varepsilon^{(i_4)})}{\sigma^2(\varepsilon^{(i_4)})}\right| \end{pmatrix}.$$

We take $I=\{1,2,4,5\}$, since this I appeared to give the best bounds. Now, (29)–(32) imply

$$\left\|\log\left|\frac{\sigma(\varepsilon^{(1)})}{\sigma^2(\varepsilon^{(1)})}\right\| = \left\|\log\left|\frac{\varepsilon^{(2)}}{\varepsilon^{(3)}}\right\| < 0.7973\,,$$

$$\left\|\log\left|\frac{\sigma(\varepsilon^{(2)})}{\sigma^2(\varepsilon^{(2)})}\right\| = \left\|\log\left|\frac{\varepsilon^{(3)}}{\varepsilon^{(1)}}\right\| < 17.0107 + 6\log|y|\,,$$

$$\left\|\log\left|\frac{\sigma(\varepsilon^{(4)})}{\sigma^2(\varepsilon^{(4)})}\right\| = \left\|\log\left|\frac{\varepsilon^{(5)}}{\varepsilon^{(6)}}\right\| < 0.8121\,,$$

$$\left\|\log\left|\frac{\sigma(\varepsilon^{(5)})}{\sigma^2(\varepsilon^{(5)})}\right\| = \left\|\log\left|\frac{\varepsilon^{(6)}}{\varepsilon^{(4)}}\right\| < 0.9534\,.$$

Note that

$$U_I^{-1} = \begin{pmatrix} 1.22206\ldots & -0.46909\ldots & 0.20641\ldots & 0.00016\ldots \\ 1.24142\ldots & -1.43198\ldots & -0.04741\ldots & 0.01435\ldots \\ -0.23980\ldots & 0.48845\ldots & -0.47443\ldots & -0.25399\ldots \\ 0.73360\ldots & -1.19735\ldots & 0.46041\ldots & -0.22027\ldots \end{pmatrix},$$

and we thus find

$$B \leqq 25.4012 + 8.5920\log|y|\,.$$

Together with (33) this implies

$$|\Lambda_1| < 14.606\,e^{-0.69832B}\,. \tag{34}$$

Note that $|\Lambda_1| < 0.5$ if $B \geqq 5$.

The next step is to derive a lower bound for $|\Lambda_1|$ from the theory of linear forms in logarithms. We applied a sharp result due to Blass, Glass, Manski, Meronk and Steiner [BGMMS], Corollary 2, as restated in [TW2], Appendix A3. We have the following data: $m=4$, $D=6$,

i	1	2	3	4
α_i	ϕ	η	χ	$\theta^{-2}\psi$
$h(\alpha_i)$	0.3323...	0.4216...	0.4216...	0.5727...
V_i	0.3324	0.4217	0.4217	0.5728
V_i^+	1	1	1	1
$\bar{V}_i$	1	1	1.2651	2.2912
a_i	1.9566	2.3448	2.3448	1.1404
$\bar{a}_i$	1.9566	2.1332	2.1993	1.7850

$a = 1.7851$, $\bar{a} = 2.0052$, $E = 42.8407$, $\bar{E} = 8.0210$, $\log \bar{M} = 51.5566$. The theorem in [TW2], Appendix A3, now says

$$\text{(35)} \qquad \text{if } B \geqq 1.0202 \cdot 10^{13} \text{ then } |\Lambda_1| > e^{-2.1583 \cdot 10^{18}(\log B + 242.8982)}.$$

Combining (34) and (35) we derive

$$B < 1.0202 \cdot 10^{13} \quad \text{or} \quad B < 7.5071 \cdot 10^{20} + 3.0908 \cdot 10^{18} \log B,$$

which implies

$$\text{(36)} \qquad B < 8.9984 \cdot 10^{20}.$$

3.4. Reducing the upper bound. The upper bound (36) guarantees that now in principle only finitely many possibilities have to be checked. Since this bound is very large, this is impossible in practice. Therefore we use the method of [TW1], Section 2.3, to establish a reduced upper bound for B that is small enough to admit enumeration of all possibilities.

Our starting point is (34) in connection with an upper bound B_0 for B, which in view of (36) has initially the value $8.9984 \cdot 10^{20}$. Let C be a large number, and consider the lattice $\Gamma \subset \mathbb{Z}^4$ spanned by

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ [C \log|\eta^{(1)}|] \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ [C \log|\phi^{(1)}|] \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ [C \log|\theta^{-2^{(1)}}\psi^{(1)}|] \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ [C \log|\chi^{(1)}|] \end{pmatrix}$$

(where $[\cdot]$ denotes rounding towards zero). A reduced basis $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4$ of this lattice can be computed by the L^3-algorithm, see e.g. [dW2], Section 3.5. In view of (34) Proposition 3.1 of [TW1] now reads as follows:

$$\text{(37)} \quad \text{if } |\mathbf{b}_1| > \sqrt{152}\, B_0 \text{ then } B \leqq B_1 = \left\lfloor \frac{1}{0.69832} \log \frac{14.606\, C}{\sqrt{|\mathbf{b}_1|^2/8 - 3B_0^2} - 4B_0} \right\rfloor.$$

We applied four subsequent reduction steps, with data as follows. We have computed the terms of the linear form in logarithms up to over 100 decimal places, and found, based on

$$\theta^{(1)} = -1.94188\,36348\,52104\,05431\,39645\,52587\,57845\,44997\,30211\,47800$$
$$71771\,75289\,05295\,40834\,17520\,01335\,38651\,49212\,81676\,85321\,0886\ldots$$

the following data:

$$\log|\eta^{(1)}| = 1.07905\,00683\,21578\,75789\,97850\,09123\,11979\,41827\,42930\,69090$$
$$31787\,08430\,46420\,06268\,43292\,00751\,74129\,51208\,60575\,76784\ldots,$$

$$\log|\phi^{(1)}| = -0.05987\,35419\,17211\,71424\,94787\,73425\,17306\,09252\,72751\,91040$$
$$71800\,46793\,78738\,31539\,56438\,52614\,79366\,95807\,63225\,45647\ldots,$$

$$\log|\theta^{(1)-2}\psi^{(1)}| = 0.22296\,44002\,54545\,84314\,40962\,88227\,63137\,86938\,86299\,65508$$
$$42227\,76876\,33535\,27870\,38692\,44571\,11228\,91907\,04379\,33520\ldots,$$

$$\log|\chi^{(1)}| = -0.26018\,09828\,63887\,61025\,77719\,25320\,02659\,38400\,35790\,06499$$
$$82612\,23473\,73969\,92233\,95023\,69149\,43282\,94565\,73471\,77954\ldots.$$

This is the required information for the inputs of the L^3-algorithm. The outputs of the L^3-algorithm, the reduced bases $\{\mathbf{b}_1, \ldots, \mathbf{b}_4\}$ of the lattices Γ, were as follows:

$C = 10^{96}$:

$$\mathbf{b}_1 = \begin{pmatrix} -1025\,93034\,88728\,79514\,16085 \\ 945\,24109\,95325\,69948\,12986 \\ -3054\,67021\,01992\,45624\,19358 \\ -3871\,44011\,21442\,92994\,10659 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 910\,18603\,32810\,72440\,76787 \\ -412\,88458\,02266\,19321\,54481 \\ -6025\,36470\,72115\,50281\,04930 \\ 3820\,10753\,47435\,35301\,01746 \end{pmatrix},$$

$$\mathbf{b}_3 = \begin{pmatrix} 3728\,54052\,33992\,73804\,66472 \\ -6959\,81252\,94012\,20114\,73872 \\ -1953\,53239\,20097\,73753\,55506 \\ 1694\,87791\,56181\,91343\,96487 \end{pmatrix}, \quad \mathbf{b}_4 = \begin{pmatrix} -9390\,68552\,47858\,70138\,81271 \\ -3348\,62713\,55297\,15659\,99167 \\ -753\,21451\,56779\,49588\,97779 \\ -89\,08168\,41903\,44455\,62162 \end{pmatrix};$$

$C = 10^{17}$:

$$\mathbf{b}_1 = \begin{pmatrix} -4617 \\ 5307 \\ 1864 \\ -1921 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} -2037 \\ 2478 \\ 2221 \\ 10429 \end{pmatrix}, \quad \mathbf{b}_3 = \begin{pmatrix} 7875 \\ 1405 \\ 13952 \\ -6760 \end{pmatrix}, \quad \mathbf{b}_4 = \begin{pmatrix} 7376 \\ 15421 \\ -8824 \\ 1889 \end{pmatrix};$$

$C = 10^{13}$:

$$\mathbf{b}_1 = \begin{pmatrix} -194 \\ -318 \\ 941 \\ -288 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 159 \\ -836 \\ -288 \\ -419 \end{pmatrix}, \quad \mathbf{b}_3 = \begin{pmatrix} -1125 \\ -603 \\ 245 \\ 804 \end{pmatrix}, \quad \mathbf{b}_4 = \begin{pmatrix} 1172 \\ -606 \\ 525 \\ 959 \end{pmatrix};$$

$C = 10^{12}$:

$$\mathbf{b}_1 = \begin{pmatrix} -82 \\ 55 \\ -117 \\ -536 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} -598 \\ 221 \\ 294 \\ -162 \end{pmatrix}, \quad \mathbf{b}_3 = \begin{pmatrix} -439 \\ -615 \\ 6 \\ 222 \end{pmatrix}, \quad \mathbf{b}_4 = \begin{pmatrix} -404 \\ 539 \\ -647 \\ 217 \end{pmatrix}.$$

Thus, the four applications of (37) yield:

step	B_0	condition of (37): $\lvert\mathbf{b}_1\rvert >$	C	$\lvert\mathbf{b}_1\rvert =$	B_1
first	$8.9984 \cdot 10^{20}$	$1.1094 \cdot 10^{22}$	10^{96}	$5.1249 \cdot 10^{23}$	243
second	243	2995.91	10^{17}	7526.33	49
third	49	604.12	10^{13}	1052.22	39
fourth	39	480.82	10^{12}	557.43	38

It is clear from these results that further reduction is not useful. The total computation time of the four applications of the L^3-algorithm was about 7 minutes on a VAX-3100 workstation.

The conclusion is $B \leqq 38$, which is much better than (36). For $5 \leqq B \leqq 40$ we checked all possible $\mathbf{b}$ for being a solution of (34). The solutions of it, as well as all possible $\mathbf{b}$ with $B \leqq 4$, were checked for (28) for all six conjugates. (For these computations, which required only a few minutes of computation time on a personal computer, 16 digit precision was amply sufficient.) For every solution $\mathbf{b}$, also the set $\mathscr{B}$ of 'conjugate' solutions was computed, and thus we found that (28) has exactly the 27 solutions presented in the table below. There are five sets $\mathscr{B}$ (one of which has only three distinct elements instead of six), which are presented as blocks in the table below. Here, the one but last column indicates the automorphism that relates the solution on that line to the first one of the block.

For these 27 solutions we computed m from (26), and found it to be an integer in only four cases, marked with * in the above Table:

$\mathbf{a} = (2, 3, 2, 2)^t$, with $m = -1$, leading (by (25)) to non-integral x, y;

$\mathbf{a} = (8, 1, 2, 4)^t$, with $m = -2$, leading (by (25)) to the solution $x = 0$, $y = -1$;

$\mathbf{a} = (0, 0, 0, 0)^t$, with $m = 0$, leading (by (25)) to the solution $x = 1$, $y = 0$;

$\mathbf{a} = (1, 1, 2, 1)^t$, with $m = 0$, leading (by (25)) to non-integral x, y.

This completes the proof of Theorem 3.

The solutions of (28):

a_1	a_2	a_3	a_5	b_2	b_3	b_4	b_5	d_2	d_3	d_4	d_5		
−4	−3	−5	−3	−4	−10	5	−10	−12	−19	6	−13	id	
−1	4	3	0	12	19	−6	13	8	9	−1	3	σ	
14	3	8	10	−8	−9	1	−3	4	10	−5	10	σ^2	
2	3	7	3	−4	−4	−1	−4	0	5	0	−1	ϱ	
5	−2	−3	0	0	−5	0	1	−4	−9	−1	−3	$\sigma\varrho$	
2	3	2	4	4	9	1	3	4	4	1	4	$\sigma^2\varrho$	
−4	−1	−1	−3	−2	−6	1	−6	−8	−11	4	−11	id, ϱ	
5	2	1	2	8	11	−4	11	6	5	−3	5	σ, $\sigma\varrho$	
8	3	6	8	−6	−5	3	−5	2	6	−1	6	σ^2,$\sigma^2\varrho$	
−1	−2	−3	−2	−2	−7	2	−5	−8	−13	3	−9	id	
2	3	2	2	8	13	−3	9	6	6	−1	4	σ	*
8	3	7	7	−6	−6	1	−4	2	7	−2	5	σ^2	
−1	2	3	0	2	3	−2	1	0	1	1	−3	ϱ	
8	1	2	4	0	−1	−1	3	2	2	−3	4	$\sigma\varrho$	*
2	1	1	3	−2	−2	3	−4	−2	−3	2	−1	$\sigma^2\varrho$	
0	0	0	0	−1	−3	1	−3	−4	−6	2	−5	id	*
3	2	2	2	4	6	−2	5	3	3	−1	2	σ	
6	2	4	5	−3	−3	1	−2	1	3	−1	3	σ^2	
1	1	2	1	−1	−2	0	−2	−2	−2	1	−3	ϱ	*
4	1	1	2	2	2	−1	3	1	0	−1	1	$\sigma\varrho$	
4	2	3	4	−1	0	1	−1	1	2	0	2	$\sigma^2\varrho$	
2	0	0	1	−1	−3	1	−2	−3	−5	1	−3	id	
2	2	2	2	3	5	−1	3	2	2	0	1	σ	
5	2	4	4	−2	−2	0	−1	1	3	−1	2	σ^2	
2	2	3	2	1	2	−1	1	1	0	0	0	ϱ	
5	1	2	3	−1	−2	0	0	0	0	−1	1	$\sigma\varrho$	
2	1	1	2	0	0	1	−1	−1	−2	1	−1	$\sigma^2\varrho$	

References

[An] *Jannis A. Antoniadis*, Über die Kennzeichnung zweiklassiger imaginär-quadratischer Zahlkörper durch Lösungen diophantischer Gleichungen, J. reine angew. Math. **339** (1983), 27–81.

[BGMMS] *J. Blass, A.M.W. Glass, D.K. Manski, D.B. Meronk* and *R.P. Steiner*, Constants for lower bounds for linear forms in logarithms of algebraic numbers II, The homogeneous rational case, Acta Arith. **55** (1990), 15–22.

[Lj] *W. Ljunggren*, Einige Sätze über bestimmte Gleichungen von der Form $AX^4 + BX^2 + C = DY^2$, Skrifter Ut. Norske Videnskaps-Akademii, Oslo, I. Mat.-Natur. Klasse, 1942, **9** Oslo 1943.

[PWZ] *M. Pohst, P. Weiler* and *H. Zassenhaus*, On effective computation of fundamental units II, Math. Comp. **38** (1982), 293–329.

[ShT] *T.N. Shorey* and *R. Tijdeman*, Exponential diophantine equations, Cambridge 1986.

[StTz] *R. Steiner* and *N. Tzanakis*, Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$, J. Number Th. **37** (1991), 123–132.

[Tz] *N. Tzanakis*, On the diophantine equation $2x^3 + 1 = py^2$, Manuscr. Math. **54** (1985), 145–164.

[TW1] *N. Tzanakis* and *B. M. M. de Weger*, On the practical solution of the Thue equation, J. Number Th. **31** (1989), 99–132.

[TW2] *N. Tzanakis* and *B. M. M. de Weger*, How to explicitly solve a Thue-Mahler equation, Comp. Math., to appear.

[dW1] *B. M. M. de Weger*, A diophantine equation of Antoniadis, in: Number Theory and Applications, NATO ASI (C) **265** (1989), 575–589.

[dW2] *B. M. M. de Weger*, Algorithms for diophantine equations, CWI-Tract No. 65, Centre for Math. and Comput. Sci., Amsterdam 1989.

Faculty of Applied Mathematics, University of Twente, 7500 AE Enschede, The Netherlands

Eingegangen 27. Juni 1991