Complete solutions of quartic Thue and index form equations *†

Maurice Mignotte
Université Louis Pasteur
7 rue René Descartes
67084 Strasbourg Cedex
France

Attila Pethö ‡
Kossuth Lajos University
Department of Computer Science
H-4010 Debrecen, P.O.Box 12
Hungary

Ralf Roth
FB-14 Informatik
Universität des Saarlandes
D-6600 Saarbrücken
Germany

November 28, 2009

Abstract

*1980 Mathematics Subject Classification: Primery 11D25, 11D57, 11R16, 11Y50

†Key words and phrases: Thue equation, index form equation, linear forms in the logarithms of algebraic numbers, distributed computation

‡Research partly done while the author was a visiting professor at the Fachbereich 14 - Informatik, Universität des Saarlandes.

Continuing the work of [8] we prove that the diophantine equation

$$f_a(x,y) = x^4 - ax^3y - x^2y^2 + axy^3 + y^4 = 1$$

for $|a| \geq 3$ has exactly 12 solutions except when $|a| = 4$ where it has 16 solutions.
If $\alpha = \alpha(a)$ denotes one of the zeros of $p_a(x,1)$ then for $|a| \geq 4$ we establish also all those $\gamma \in \mathbb{Z}[\alpha]$ with $\mathbb{Z}[\gamma] = \mathbb{Z}[\alpha]$.

1 Introduction

Let $a \in \mathbb{Z}$ and

$$f_a(x,y) = x^4 - ax^3y - x^2y^2 + axy^3 + y^4 = x(x-y)(x+y)(x-ay) + y^4$$

In a recent paper Pethö [8] proved that for $3 \leq |a| \leq 100$ and $|a| \geq 9.9 \times 10^{27}$ the Thue equation

$$f_a(x,y) = 1 \tag{1}$$

only has the following trivial solutions $\pm(x,y) = (0,1),(1,0),(1,1),(1,-1),(a,1),(1,-a)$ except when $|a| = 4$, in which case it has the 4 further solutions

$$\pm(x,y) = \begin{cases} (8,7),(7,-8) & \text{, if } a = 4 \\ (8,-7),(7,8) & \text{, if } a = -4 \end{cases} \tag{2}$$

Combining this result with new ideas and an extensive computer search we prove in this paper

Theorem 1 *For $|a| \geq 3$, Equation (1) has only trivial solutions except for $|a| = 4$, when it has the four nontrivial solutions given by (2).*

Several similar parametrized families of Thue equations have been studied recently. Apart the result of Pethö [8] and the references he used, we mention the papers of Mignotte and Tzanakis [6], Lee [4] and Thomas [9]. We also refer the paper of Mignotte [5], where he proved that for $n \geq 4$, $n \in \mathbb{Z}$ the diophantine equation

$$x^3 - (n-1)x^2y - (n+2)xy^2 - y^3 = 1$$

only has the trivial solutions $(x,y) = (1,0),(0,-1),(-1,1)$. This is the first example where a parametrized Thue equation was completely solved.

We mention that the method of the proof of Theorem 1 is also applicable to other parameterized families of diophantine equations. For more details see the Remark in §4.

We are now giving two applications of Theorem 1. Let η and η' be the zeros of the polynomial $x^2 - ax + 1$ and let

$$R_n = \frac{\eta^n - \eta'^n}{\eta - \eta'}$$

for $n \in \mathbb{Z}$. Combining Theorem 1 with the proof of Thereom 4 of [8] we get

Theorem 2 *Assume that* $|a| \geq 3$ *and*

$$4u^2 + v^2 = z^2$$

with $(u, v) = (R_n, R_{n+1})$ *or* (R_{n+1}, R_n) *and* $z \in \mathbb{Z}$. *Then* $n = 0, 2$ *or* -3 *except when* $|a| = 4$, *in which case* $(n, u, v) = (4, 56, 15), (-5, -56, -15)$.

To formulate the next results we need to introduce some notation.

Let $a, b \in \mathbb{Z}, \quad a \geq 0$ and $f(x) = f_{a,b}(x) = x^4 - ax^3 - bx^2 + ax + 1$.

Denote $\alpha = \alpha(a, b)$ one of the zeros of $f_{a,b}(x)$ and put $\epsilon = \epsilon(a, b) = \alpha - \frac{1}{\alpha}$. Since α is a unit, ϵ is an algebraic integer. Let $\mathbb{K} = \mathbb{K}_{a,b} = Q(\alpha(a, b))$ and $O = O_{a,b} = \mathbb{Z}[\alpha(a, b)]$. Then O is an order in $\mathbb{K}$. By ([8], Lemma 2.1) the degree of $\mathbb{K}$ over $\mathbb{Q}$ is 4 if and only if ϵ is a quadratic algebraic number, i.e. $a^2 + 4b - 8$ is not a square of an integer. In the sequel we assume $[\mathbb{K} : \mathbb{Q}] = 4$.

We shall prove in Lemma 3.1 that $1, \epsilon, \alpha, \alpha\epsilon$ is an integral basis of O. In order to state our results it is more convenient to consider this basis as the natural basis $1, \alpha, \alpha^2, \alpha^3$. We have

Theorem 3 *Let* $a, b, \in \mathbb{Z}$ *such that* $a^2 + 4b - 8$ *is not the square of an integer,* $2a^2 + 9b - 23, \quad a^2 + 5b - 16, \quad 2a^2 + 76 - 11, \quad a^2 + 3b - 4 \neq 0$ *and* $b = 6$ *or* $a^2 + 4b - 8 \not| b - 6$. *Let* $\gamma = x_1 + x_2\epsilon + x_3\alpha + x_4\alpha\epsilon$ *such that* $\mathbb{Z}[\gamma] = O$. *Then there exist integers* b_1, b_2 *with* $(b_1, b_2) = 1$, $b_1 b_2 = (2 - b)$ *and a solution* $(u, v) \in \mathbb{Z}^2$ *of the Thue equation*

$$b_2^2 v^4 - b_2 a v^3 u + (b - 2)u^2 v^2 + b_1 a v u^3 + b_1^2 u^4 = \pm 1 \tag{3}$$

such that $(x_2, x_3, x_4) = (b_1 u^2, b_2 v^2 - b_1 u^2 - auv, uv)$. *The convers is also true.*

The elements $\gamma, \delta \in O$ are called equivalent, denoted by $\gamma \sim \delta$, if $\gamma + \delta$ or $\gamma - \delta$ belongs to $\mathbb{Z}$. It is clear that if $\gamma \sim \delta$ then $|D_{K/Q}(\gamma)| = |D_{K/Q}(\delta)|$ and they have the same index corresponding to O.

From Theorems 1 and 3 we deduce

Theorem 4 *Let $b = 1$, $a \geq 4$. Then all the equivalence classes of O contain an element*
$\gamma = y_2\alpha + y_3\alpha^2 + y_4\alpha^3$ *with*

$$(y_2, y_3, y_4) \in \{(1,0,0), (1,a,-1), (a,a-1,-1), (a,-a-1,1), (1,0,-1), (1,-a(a^2+1),a^2)\}$$

except when $a = 4$ in which case

$$(y_2, y_3, y_4) \in \{(1,0,0), (1,4,-1), (4,3,-1), (4,-5,1), (1,0,-1), (1,-68,16), (209,140,-49), (209,-352,64)\}.$$

Remark *$O_{a,1}$ often is the maximal order of $\mathbb{K}_{a,1}$. In the range $4 \leq a \leq 1000$ we found 471 values for which this is true. For $a = 4, 5$ and 8 we compared the result of Theorem 4 with the table of Gaál, Pethö and Pohst [2], [3]. (For other values this is not possible because, either $O_{a,1}$ is not maximal or the discriminant of $\mathbb{K}_{a,1}$ is too large.) For $a = 4$ and 5 the results are the same although they computed only the small solutions of the corresponding index form equations. For $a = 8$ their method is not applicable because the class number of the quadratic subfield $(\mathbb{Q}(\sqrt{15}))$ of $\mathbb{K}_{8,1}$, is not 1.*

We want to thank Volker Müller from the Universität des Saarlandes for his assistance in using PARI in library mode.

2 Preparations to the proof of Theorem 1

In §§2-4 we will use the notation (v, a_1, a_2, a_3, δ_3) of Pethö [8]. We refer to the equations and statements of that paper by (P.n.m) and statement P.n.m respectively. Since Theorem 1 was proved for $a \leq 100$ in [8] we assume $a \geq 100$. Denote by α the largest and β the second largest real zeros of $p(x) = p_a(x, 1)$ and put $\epsilon = \alpha - \frac{1}{\alpha}$.

We first establish more exact estimates, than those which were proved in [8].

Considering $p(x)$ at the points $1 + \frac{1}{2a}$, $1 + \frac{1}{a}$, $a - \frac{2}{a}$, $a - \frac{1}{a}$ and a one gets

$$a - \frac{2}{a} < \epsilon < a - \frac{1}{a} < \alpha < a,$$

$$1+\frac{1}{2a}<\beta<1+\frac{1}{a}<1+\frac{1}{\epsilon}. \tag{4}$$

Using the estimates above and the inequality

$$\frac{\log 2}{x}<\log\left(1+\frac{1}{x}\right)<\frac{1}{x}$$

which is true for any $x>1$, it is easy to derive the following

$$\frac{\log 2}{2a}<\log\beta<\frac{1}{a},$$

$$\log a-\frac{\log 2}{a^2-1}<\log\alpha<\log a,$$

$$\log\epsilon<\log\alpha-\frac{\log 2}{\alpha^2-1},$$

$$\log\frac{\alpha+1}{\alpha-1}<\frac{2}{a-2},$$

$$\log 2a+\frac{\log 2}{2a}<\log\frac{\beta+1}{\beta-1}.$$

We also need an estimate for A, the regulator of $\mathbb{Z}[\alpha]$.

$$\begin{aligned} A &= \log\alpha\log\frac{\beta+1}{\beta-1}-\log\beta\log\frac{\alpha+1}{\alpha-1} \\ &> \log\epsilon\log\frac{\beta+1}{\beta-1}+\frac{(\log 2)\log 2a}{\alpha^2-1}-\frac{2}{a(a-2)} \\ &> \log\epsilon\log\frac{\beta+1}{\beta-1}. \end{aligned} \tag{5}$$

Put $K_1=a_3-a_1$ and $K_2=a_1+a_3+2a_2$. Then by (P.5.16), (4), (5) and by

$$\delta_3 < \frac{2}{A}\log\frac{a+1}{a-1}\log\beta$$

we get

$$\begin{aligned} K_1 &< 2\,\frac{\log\epsilon\log\beta}{A}v + \frac{2}{A}\log\frac{a+1}{a-1}\log\beta \\ &< \frac{2v}{a\log\frac{\beta+1}{\beta-1}}\left(1+\frac{2}{a-1}\frac{2}{\epsilon\log^2\epsilon}\right) \\ &< \frac{2v\left(1+\frac{1}{a^2}\right)}{a\log 2a+\frac{\log 2}{2}} < \frac{2v}{a\log 2a}. \end{aligned} \tag{6}$$

Since in Lemma P.5.4 we found all solutions of (1) with $a_1 = a_3$, we may assume $K_1 > 0$, hence

$$v > \frac{1}{2}a\log 2a, \tag{7}$$

which is stronger than (P.5.18). We will use this estimate to find all type I solutions.

For type II solutions we may assume by Lemma P.6.4 that $K_2 \geq 2$. Then by (P.6.12) and (5) we have

$$1 \leq K_2 - 1 \leq 2v\,\frac{\log\epsilon\log\frac{\alpha+1}{\alpha-1}}{A} < \frac{4v}{(a-2)\log 2a}. \tag{8}$$

Thus, in this case

$$v > \frac{(a-2)\log 2a}{4} \tag{9}$$

which is an improvement on (P.6.15).

To prove Theorem 1 we shall use lower bounds for the following linear forms in logarithms of algebraic numbers

$$|\Lambda_1| = \left|\log\frac{\alpha\beta+1}{\alpha-\beta} + (K_2-1)\log\beta + K_1\log\frac{\beta+1}{\beta-1}\right| < 3.1\;\epsilon^{-2v-1}, \tag{10}$$

$$(11) \quad |\Lambda_2| = \left|\log \frac{\alpha\beta+1}{\alpha-\beta} + (K_2-1)\log\alpha + K_1 \log\frac{\alpha+1}{\alpha-1}\right| < 1.1\ \epsilon^{-2v},$$

$$\Lambda_3 = \log\left[\frac{\alpha\beta+1}{\alpha-\beta}\left(\frac{\beta+1}{\beta-1}\right)^{K_1}\right] + (K_2-1)\log\beta$$

and

$$\Lambda_4 = \log\left[\frac{\alpha\beta+1}{\alpha-\beta}\alpha^{K_2-1}\right] + K_1\log\frac{\alpha+1}{\alpha-1}.$$

The upper bounds are exactly (P.5.17) and (P.6.14).

Now we estimate the absolute logarithmic height of the algebraic numbers occuring in Λ_i, $i = 1, .., 4$.

$$h(\alpha) = h(\beta) = \frac{1}{4}\log|\alpha\beta| < \frac{\log(a+1)}{4},$$

$$h\left(\frac{\alpha+1}{\alpha-1}\right) = h\left(\frac{\beta+1}{\beta-1}\right) < \frac{\log 5a}{4},$$

$$h\left(\frac{\alpha\beta+1}{\alpha-\beta}\right) < \frac{1}{4}\log(a^2-4) + \frac{1}{4}\log\frac{a+2}{a-1-\frac{2}{a}} < \frac{\log(a+3)}{2},$$

$$(12) \qquad h\left(\frac{\alpha\beta+1}{\alpha-\beta}\left(\frac{\beta+1}{\beta-1}\right)^{K_1}\right) < \frac{\log(a+3)}{2} + \frac{K_1\log 5a}{4},$$

$$(13) \qquad h\left(\frac{\alpha\beta+1}{\alpha-\beta}\alpha^{K_2-1}\right) < \frac{\log(a+3)}{2} + \frac{(K_2-1)\log(a+1)}{4}.$$

The third of this set of inequations follows from the fact that $\frac{\alpha\beta+1}{\alpha-\beta}$ is a zero of the irreducible polynomial

$$x^4 - \frac{2a^2+17}{a^2-4}x^2 + 1.$$

From (12), (6) and (7) as well as from (13), (8) and (9) we conclude

$$h\left(\frac{\alpha\beta+1}{\alpha-\beta}\left(\frac{\beta+1}{\beta-1}\right)^{K_1-1}\right) < \frac{1.55\ \log(a+3)}{a\log 2a} \tag{14}$$

and

$$h\left(\frac{\alpha\beta+1}{\alpha-\beta}\alpha^{K_2-1}\right) < \frac{3v\log(a+3)}{(a-2)\log 2a} \tag{15}$$

assuming $a > 10^7$.

Now we are able to apply Corollary 1.1 of Mignotte and Waldschmidt [7] to Λ_3 and Λ_4. By using (10) and (14) we get

$$(2v+1)\log\epsilon - \log 3.1 < 250\ 8^4 \frac{1.55v\log(a+3)}{a\log 2a}\frac{\log 5a}{4}(7.5+\log K_2)^2,$$

so that if $a > 10^7$ then

$$a < 250\ 8^3\ 1.71\ (7.5+\log K_2)^2. \tag{16}$$

By Theorem P.1, $K_2 < 10^{28}$, hence we get

$$a < 1.2\times 10^9 \tag{17}$$

for type I solutions.

Similarly using (11) and (15) we get for type II solutions

$$2v\log\epsilon - \log 1.1 < 250\ 8^4 \frac{3v\log(a+3)}{(a-2)\log 2a}\frac{\log 5a}{4}(7.5+\log K_1)^2 \quad ,$$

thus

$$a < 250\ 8^3\ 3.3\ (7.5+\log K_1)^2 \quad . \tag{18}$$

By Theorem P.1, $K_1 < 10^{28}$, hence by (17)

$$a < 2.2\times 10^9 \quad . \tag{19}$$

Assuming that $a > 10^2$ we improve the estimates (P.5.19) for v using Corollary 1.5 of Waldschmidt [10]. With his notation we set for both Λ_1 and Λ_2

$n = 3, \quad D = 8, \quad g = 1,$

$\log A_1 = \frac{\log(a+1)}{4}, \quad \log A_2 = \frac{\log 5a}{4}, \quad \log A_3 = \frac{\log(a+3)}{2},$

$A = A_3, \quad f = 1, \quad E = 6, \quad M = \frac{4v+6}{\log(a+1)},$

$Z_0 = 7 + 3\log 3, \quad G_0 = \log M$ and

$$\begin{aligned} U_0 &= \frac{8^5(7+3\log 3)}{\log^4 6}\frac{\log(a+1)}{4}\frac{\log 5a}{4}\frac{\log(a+3)}{2}\log M \\ &< 5.09\times 10^5 \log(a+1)\left(\log(4v+6) - 1.529\right). \end{aligned}$$

Remark that the correctness of M follows from (P.5.15), (P.5.16), (P.6.12) and (P.6.13), because $|K_1|, |K_2| \leq 2v+1$.

The cited result of Waldschmidt implies

$$|\Lambda_1|, \ |\Lambda_2| \geq exp(-2000\ 2^9\ 3^{14} U_0).$$

By comparing the last inequality with (10) and (11) we get

$$2v\log\epsilon - \log 1.1 < 2.49\times 10^{18}\log(a+1)(\log(4v+6) - 1.529) \quad ,$$

so that

$$2v < 2.5\times 10^8(\log(4+6v) - 1.529) + 0.03$$

and finally

$$|K_1|, \ |K_2| \leq 2v+1 \leq 2\times 10^{20} \tag{20}$$

follows immendiatelly for both type I and II solutions.

We insert the new upper estimate (20) into (16) and (18) and get the final upper bound

$$a < 6.441\times 10^8 \tag{21}$$

for type I solutions and

$$a < 1.125\times 10^9 \tag{22}$$

for type II solutions.

To exclude non-trivial solutions from the remaining range we used computer search, which is described in the next two sections.

3 Diophantine approximation properties of non-trivial solutions

The following lemmas are basic for the final computer search for non-trivial solutions. By $\|x\|$ we denote the distance of the real number x to the nearest integer.

Lemma 1 *Let* $10^2 \le a \le 6.441 \times 10^8 \qquad (1.25 \times 10^9)$,

$$\delta_1 = \log \frac{\alpha\beta+1}{\alpha-\beta} / \log \beta \qquad \left(\log \frac{\alpha\beta+1}{\alpha-\beta} / \log \frac{\alpha+1}{\alpha-1} \right) \quad \textit{and}$$

$$\delta_2 = \log \frac{\beta+1}{\beta-1} / \log \beta \qquad \left(\log \alpha / \log \frac{\alpha+1}{\alpha-1} \right).$$

If there exists a convergent $\frac{p}{q}$ *in the continued fraction expansion of* δ_2 *such that*

$$q \le 10^{50} \tag{23}$$

and

$$q\|q\delta_1\| > \frac{2.1 \times 10^{20}}{a \log 2a} \qquad \left(\frac{4.1 \times 10^{20}}{a \log 2a} \right) \tag{24}$$

then (10) ((11)) cannot hold for K_1, $K_2 \in \mathbb{Z}$ *with* $|K_1|$, $|K_2| \le 2v+1$ *and* $K_1 \neq 0 \qquad (K_2 \neq 1)$.

Proof: Assume to the contrary that there exist K_1, $K_2 \in \mathbb{Z}$ with $|K_1|$, $|K_2| < 2v+1$ wich satisfy (10) and let $\frac{p}{q}$ be the convergent of δ_2 with (23) and (24). Then by (7), $v > \frac{1}{2} a \log 2a > 260$, thus by (10)

$$|\delta_1 + K_1\delta_2 + (K_2 - 1)| < 10^{-1000} \quad .$$

Multiplying this inequality by q we get

$$|q\delta_1 + K_1(\delta_2 q - p) + K_1 p + (K_2 - 1)q| < 10^{-950}, \tag{25}$$

thus

$$\|q\delta_1\| \le 10^{-950} + |K_1||q\delta_2 - p| < \frac{|K_1|}{q} + 10^{-950}.$$

Hence by (6) and (20)

$$q\|q\delta_1\| \le \frac{2\ 10^{20}}{a\log 2a} + 10^{-900} < \frac{2.1\ 10^{20}}{a\log 2a}.$$

This contradiction proves the lemma. □

Since on a computer we cannot work with δ_1 and δ_2 but only with their approximate values, we have to know how close this approximation has to be.

Lemma 2 *Let* $a < 6.441 \times 10^8 \qquad (1.25 \times 10^9)$ *and* δ_1, δ_2 *as in Lemma 2. Let* $\tilde{\delta}_1$, $\tilde{\delta}_2 \in \mathbb{Q}$ *such that*

$$|\delta_1 - \tilde{\delta}_1|,\ |\delta_2 - \tilde{\delta}_2| < 10^{-50} \tag{26}$$

and let $\frac{p}{q}$ *be a convergent of* $\tilde{\delta}_2$ *with*

$$q < 10^{28} \quad \textit{and} \quad q\|q\tilde{\delta}_1\| > \frac{3\times 10^{20}}{a\log 2a} \qquad \left(\frac{5\times 10^{20}}{a\log 2a}\right). \tag{27}$$

Then (10) ((11)) cannot hold for K_1, $K_2 \in \mathbb{Z}$ *with* $|K_1|$, $|K_2| \le 2v+1$ *and* $K_1 \ne 0 \qquad (K_2 \ne 1)$.

Proof: We start as in the proof of Lemma 1 up to equation (25) except that now $\frac{p}{q}$ denotes a convergent of $\tilde{\delta}_2$.

From (25) we get

$$\|q\tilde{\delta}_1\| \le 10^{-950} + |K_1||q\tilde{\delta}_2 - p| + q|\delta_1 - \tilde{\delta}_1| + q|\delta_2 - \tilde{\delta}_2|,$$

hence

$$q\|q\tilde{\delta}_1\| \le \frac{2.1\times 10^{20}}{a\log 2a} + 2\times 10^6 < \frac{2.2\times 10^{20}}{a\log 2a}$$

and the lemma is proved. □

4 The computer search

For the evaluating of about 10^8, (2×10^8) equations we decided to use distributed computation. We wrote a program which for $a = 101$ to $10^8 \quad (2\times 10^8)$ executed the following steps

1. compute δ_1 and δ_2 with sufficient precision (50 digits were enough if (24) holds for q $< 10^{28}$)
2. compute the continued fraction expansion of δ_2
3. compute the sequence $\{q_n\}_{n\geq 0}$ of the denominators of the convergents of δ_2
4. **if** $10^{17} < q_n < 10^{28}$ and (24) holds then continue with the next value for a
   else remember a and try again later with higher precision

The necessary computer programs are implemented in C. They use the library of the computer algebra-system PARI for the higher precision computations. Our experiments showed that PARI in this case is 10 times faster than MAPLE V. Furthermore we used the LiPS system [1] to distribute the computations over a local network of SUN-Workstations (Sparc Stations).

First we did our search for $a \in [100, 10^5]$ with 100 digits precision.

The remaining interval $[10^5, 10^8] \quad ([10^5, 2\ 10^8])$ was divided into blocks of length 10^5. These intervals were distributed by LiPS over 40 machines of the local Ethernet of the Universität des Saarlandes. The programs on each workstation did the search and collected the questionable cases.

Altogether the computations took

- 2748 h 21 min $\approx$ 144 days for type I
- 10185 h 55 min $\approx$ 424 days for type II (4×10^8)

The given time is the summerized CPU-time over all workstations. The real time was about 3 weeks.

For every $100 \leq a \leq 10^8 \quad (2 \times 10^8)$ we found a q with (27). This completes the proof of Theorem 1.

Remark As we mentioned in the introduction, the method descibed in §§2-4 is also applicable for the complete resolution of other parametrized

families of diophantine equations. Of course, suppose that it is possible for a parametrized family of diophantine equations to derive fintely many inequalities of the form

$$0 < |\log \delta_0(a) + K_1 \log \delta_1(a) + K_2 \log \delta_2(a)| < c_1 \exp(-c_2 K),$$

where $K = \max\{|K_1|, |K_2|\}$. If we also can prove $K > c_3 a \log a$, then we get an upper bound B_0 for K as described in [8]. This implies $|a| < B_1$ with a suitable B_1. If moreover $|K_1|$ must be less than $|K_2|$ then using a convenient theorem on linear forms in two logarithms in algebraic numbers we can , like in §2, derive a much better bound B_2 for $|a|$.

All the examples treated in [4], [6] and [8] fullfil the conditions above.

Obviously the Lemmas 1 and 2 do not depend on the special choice of δ_1 and δ_2. Finally if B_2 is reasonable then one can perform the computer search from this section.

5 The general index form equation of $O_{a,b}$

Let $\alpha, \epsilon, \mathbb{K}$ and O be the same as in §1. Then

Lemma 3 *$1, \epsilon, \alpha, \alpha\epsilon$ is an integral basis of O.*

Proof: We have

$$\epsilon = \alpha - \frac{1}{\alpha} = a + (1-b)\alpha - a\alpha^2 + \alpha^3$$

and

$$\alpha\epsilon = -1 + \alpha^2,$$

hence

$$(1, \alpha, \alpha\epsilon, \epsilon)^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ a & 1-b & -a & 1 \end{pmatrix} (1, \alpha, \alpha^2, \alpha^3)$$

which proves the assertion. □

Assume that $[\mathbb{K} : \mathbb{Q}] = 4$. Then $f(\alpha) = 0$ implies that $-\frac{1}{\alpha}$ is a zero of $f(x)$, cf Lemma P.2.1. Let β denote one of the zeros of $f(x)$ which is different from α and $\frac{-1}{\alpha}$. In the sequel we order the conjugates $\mathbb{K}^{(i)}, i = 1, 2, 3, 4$ of $\mathbb{K}$ such that $\alpha^{(1)} = \alpha$, $\alpha^{(2)} = -\frac{1}{\alpha}$, $\alpha^{(3)} = \beta, \alpha^{(4)} = -\frac{1}{\beta}$. This implies $\epsilon^{(1)} = \epsilon^{(2)} = \epsilon$ and $\epsilon^{(3)} = \epsilon^{(4)} = \epsilon'$ where ϵ' denotes the conjugate of ϵ with respect to the extension $\mathbb{Q}(\epsilon)/\mathbb{Q}$.

We denote by D_o the discriminant of the order O and by $D(\gamma) = D_{\mathbb{K}/\mathbb{Q}}(\gamma)$ the discriminant of the element $\gamma \in \mathbb{K}$.

Then

$$D_o = (\epsilon - \epsilon')^4(\alpha + \frac{1}{\alpha})^2(\beta + \frac{1}{\beta})^2 = [a^2 + 4(b-2)]^2((b+2)^2 + 4a^2). \tag{28}$$

For $\gamma \in O$ let I_γ denote the index of γ in O. Then we have the well-known identity

$$D(\gamma) = I_\gamma^2 D_o. \tag{29}$$

In the next theorem we transform the index form equation corresponding to O to a system of quadratic equations.

Theorem 5 *Let $\gamma = x_1 + x_2\epsilon + x_3\alpha + x_4\alpha\epsilon \in O$ with index I_γ. Then there exist integers I_1, I_2, V with the following properties*

$$I_1 I_2 = I_\gamma \tag{30}$$

$$x_3^2 + ax_3x_4 + (2-b)x_4^2 = I_1 \tag{31}$$

$$x_2^2 + x_2x_3 + ax_2x_4 + (b-2)x_4^2 = V \tag{32}$$

and

$$(a^2 + 4b - 8)V^2 + (b-6)I_1V - I_1^2 = I_2. \tag{33}$$

Proof: Put $\gamma_{i,j} = \gamma^{(i)} - \gamma^{(j)}$ for $1 \le i, j \le 4$. Then we can rewrite (29) as

$$D^{1/2}(\gamma) = \prod_{1 \le i < j \le 4} \gamma_{i,j} = I_\gamma D_o^{1/2}. \tag{34}$$

Let $\mathbb{L} = \mathbb{Q}(\frac{\alpha}{\beta} + \frac{\beta}{\alpha})$, then since $\frac{\alpha}{\beta} + \frac{\beta}{\alpha}$ is a zero of the quadratic polynomial $x^2 - (b-2)x - (a^2 + 2b)$, we have $[\mathbb{L} : \mathbb{Q}] = 1$ or 2. Moreover, and this is the important fact, $\gamma_{1,4}\gamma_{2,3}$ is the conjugate of $\gamma_{1,3}\gamma_{2,4}$ with respect to $\mathbb{L}$. Using this observation a straightforward computation shows that

$$D^{1/2}(\gamma) = (\alpha + \frac{1}{\alpha})(\beta + \frac{1}{\beta})U[(\epsilon - \epsilon')^2 V - (2 - \frac{\alpha}{\beta} - \frac{\beta}{\alpha})U] \times$$

$$[(\epsilon - \epsilon')^2 V - (2 + \alpha\beta + \frac{1}{\alpha\beta}U)],$$

where

$$U = x_3^2 + ax_3x_4 + (2-b)x_4^2$$

$$V = x_2^2 + x_2x_3 + ax_2x_4 + (b-2)x_4^2.$$

We can simplify further the form of $D^{1/2}(\gamma)$ and finally get

$$D^{1/2}(\gamma) = (\epsilon - \epsilon')^2(\alpha + \frac{1}{\alpha})(\beta + \frac{1}{\beta})U[(\epsilon - \epsilon')^2 V^2 + (b-6)UV - U^2].$$

Inserting this equality and (28) into (34) we get the identity

$$I_\gamma = U[(a^2 + 4b - 8)V^2 + (b-6)UV - U^2].$$

As both factors on the right hand side are integers, setting $U = I_1$ and $(a^2 + 4b - 8)V^2 + (b-6)UV - U^2 = I_2$ we prove equation (30) - (33). $\square$

6 Proof of the theorems 3 and 4

Proof of Theorem 3: Since $a^2 + 4b - 8$ is not a square, $[\mathbb{K} : \mathbb{Q}] = 4$. It is well known that for $\gamma \in O$ the powers $1, \gamma, \gamma^2, \gamma^3$ form a basis of O if and only if $|I_\gamma| = 1$, thus we can use Theorem 5. Then $|I_1| = |I_2| = 1$ by (30).

Assume that (33) holds with $V \in \mathbb{Z}$, $I_1, I_2, \in \{1, -1\}$. We may assume that $I_1 = 1$, because if $V \in \mathbb{Z}$ is a solution of (33) for $I_1 = -1$, then $-V \in \mathbb{Z}$ is also a solution for $I_1 = 1$.

Let $I_2 = 1$, then $V|2$, hence $V \in \{-2, -1, 1, 2\}$, but all values of a, b which would satisfy (33) for $V \in \{-2, -1, 1, 2\}$ are excluded in the assumptions of the theorem.

Let $I_2 = -1$. Then either $V = 0$ or $(a^2 + 4b - 8)V + (b - 6)I_1 = 0$.

The second alternative is excluded in the assumptions too, therefore $V = 0$.

Since $V = 0$ we can rewrite (32) as

$$x_2(x_2 + (x_3 + ax_4)) = (2 - b)x_4^2. \tag{35}$$

On the other hand (31) implies that $(x_3 + ax_4, (2 - b)x_4^2) = 1$, thus $(x_2, x_2 + (x_3 + ax_4)) = 1$ holds too. Therefore there exist integers b_1, b_2, u, v such that

$$(b_1, b_2) = (u, v) = 1,$$
$$b_1 b_2 = 2 - b$$
$$uv = x_4$$
$$x_2 = b_1 u^2$$
$$x_2 + x_3 + ax_4 = b_2 v^2.$$

The last equation implies that

$$x_3 = b_2 v^2 - b_1 u^2 - auv.$$

Inserting the formulas for x_3 and x_4 into (31) we get (3). Obviously the convers holds. □

Remark *Let $b_1, b_2, \in \mathbb{Z}$ with $(b_1, b_2) = 1$ and $b_1 b_2 = 2 - b$. Futhermore let δ be a zero of the polynomial*

$$b_2^2 v^4 - b_2 a v^3 - b_1 b_2 v^2 + b_1 a v + b_1^2.$$

Then one can see easily that $\mathbb{Q}(\delta)$ is an extension of $\mathbb{Q}(\epsilon)$. If $\mathbb{Q}(\epsilon)$ is an imaginary quadratic field, i.e. $a^2 + 4(b-2) < 0$ then (3) is very easy to solve, since it can be transformed to an equation of form (31).

We now turn to the proof of Theorem 4.

Proof of Theorem 4: For $b = 1$ we have $2a^2 + 9b - 23, a^2 + 5b - 16$, $2a^2 + 7b - 11$ and $a^2 + 3b - 4 \neq 0$ for any $a \geq 0$. Furthermore $a^2 - 4$ divides

5 only if $a = 3$. Finally, for $a \geq 4$, $\quad a^2 - 4$ is not a square. Therefore all the assumptions hold in this case.

We have $b_1 = b_2 = \pm 1$, hence we get two equations of form (3), namely

$$v^4 - av^3u - u^2v^2 + avu^3 + u^4 = \pm 1 \tag{36}$$

and

$$v^4 + av^3u - u^2v^2 - avu^3 + u^4 = \pm 1 \quad . \tag{37}$$

The pair (v, u) is a solution of (37) if and only if $(-v, u)$ is a solution of (36), hence it is sufficient to solve (36).

By Theorem 1 all the solutions of (36) are

$$(v, u) = (0, \pm 1), (\pm 1, 0), (\pm 1, \pm 1), (\mp 1, \pm 1), (\pm a, \pm 1), (\pm 1, \mp a)$$

except when $a = 4$ in which case we have four more solutions, namely $(\pm 8, \pm 7), (\pm 7, \mp 8)$. For given b_1, b_2 the solution $(v, u) \in \mathbb{Z}^2$ of (3) gives the same triple $(x_2, x_3, x_4) \in \mathbb{Z}^3$ as $(-v, -u)$. Furthermore, the triple corresponding to $-b_1, -b_2$ and $(-v, u)$ is $-(x_2, x_3, x_4)$, hence for $a \geq 5$ and $a = 4$ we have 6 and 8 essentially different solutions. A straightforward computation shows that these are the triples given in the theorem. $\square$

References

[1] J. Buchmann, M. Diehl and R. Roth, *LiPS A system for distributed applications,* subm. to Third IEEE Symposium on Parallel and Distributed Processing, Dallas, Texas.

[2] I. Gaál, A. Pethö and M. Pohst, *On the resolution of index form equations in biquadratic number fields I and II,* J. Number Theory, **38** (1991), 18-34 and 35-51.

[3] I. Gaál, A. Pethö and M. Pohst, *On the resolution of index form equations*, in Proc. ISSAC '91 ed.: S.M. Watt, ACM Press 1991, 185-186.

[4] M. Lee, *D. Phil. Thesis*, Cambridge University, 1991

[5] M. Mignotte, *Verification of a conjecture of E. Thomas*, J. Number Theory, to appear.

[6] M. Mignotte and N. Tzanakis, *On a family of cubics*, J. Number Theory, to appear.

[7] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Scheiders' Method IV*, to appear.

[8] A. Pethö, *Complete solutions to families of quartic Thue equations,* Math. Comp., to appear.

[9] E. Thomas, *Solutions to certain families of Thue equations*, J. Number Theory, to appear.

[10] M. Waldschmidt, *Minoration de combinaisons linéaires de logarithmes de nombres algébriques*