

## COMPLETE SOLUTIONS OF A FAMILY OF QUARTIC THUE AND INDEX FORM EQUATIONS

MAURICE MIGNOTTE, ATTILA PETHÖ, AND RALF ROTH

ABSTRACT. Continuing the recent work of the second author, 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  $|a| = 4$ , when it has 16 solutions. If  $\alpha = \alpha(a)$  denotes one of the zeros of  $f_a(x, 1)$ , then for  $|a| \geq 4$  we also find all  $\gamma \in \mathbb{Z}[\alpha]$  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

$$(1) \quad f_a(x, y) = 1$$

has only 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 four further solutions

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

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 from the result of Pethö [8] and the references therein, we mention the papers of Mignotte and Tzanakis [6], Lee [4] and Thomas [9]. We also refer to

---

Received by the editor March 3, 1992 and, in revised form, February 25, 1993, September 27, 1993, March 15, 1994, and June 2, 1994.

1991 *Mathematics Subject Classification.* Primary 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 second author was a visiting professor at the Fachbereich 14 - Informatik, Universität des Saarlandes.

the paper of Mignotte [5], where he proved that for  $n \geq 4$ ,  $n \in \mathbb{Z}$ , the diophantine equation

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

has only 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 proof of Theorem 1 is also applicable to other parametrized families of diophantine equations. For more details, see the Remark in §4.

We now give two applications of Theorem 1. Let  $\eta$  and  $\eta'$  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 Theorem 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  $a, b \in \mathbb{Z}$ ,  $a \geq 0$ , and  $f(x) = f_{a,b}(x) = x^4 - ax^3 - bx^2 + ax + 1$ . Denote by  $\alpha = \alpha(a, b)$  one of the zeros of  $f_{a,b}(x)$  and put  $\varepsilon = \varepsilon(a, b) = \alpha - \frac{1}{\alpha}$ . Since  $\alpha$  is a unit,  $\varepsilon$  is an algebraic integer. Let  $\mathbb{K} = \mathbb{K}_{a,b} = \mathbb{Q}(\alpha(a, b))$  and  $\mathcal{O} = \mathcal{O}_{a,b} = \mathbb{Z}[\alpha(a, b)]$ . Then  $\mathcal{O}$  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  $\varepsilon$  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 2 that  $1, \varepsilon, \alpha, \alpha\varepsilon$  is an integral basis of  $\mathcal{O}$ . In order to state our results, it is more convenient to consider this basis than 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,  $2a^2 + 9b - 23 \neq 0$ ,  $a^2 + 5b - 16 \neq 0$ ,  $2a^2 + 7b - 11 \neq 0$ ,  $a^2 + 3b - 4 \neq 0$  and  $b = 6$  or  $a^2 + 4b - 8 \nmid b - 6$ . Let  $\gamma = x_1 + x_2\varepsilon + x_3\alpha + x_4\alpha\varepsilon$  be such that  $\mathbb{Z}[\gamma] = \mathcal{O}$ . Then there exists a solution  $(u, v) \in \mathbb{Z}^2$  of the Thue equation*

$$(3) \quad v^4 - av^3u - bu^2v^2 + avu^3 + u^4 = \pm 1$$

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

The elements  $\gamma, \delta \in \mathcal{O}$  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  $|D_{\mathbb{K}/\mathbb{Q}}(\gamma)| = |D_{\mathbb{K}/\mathbb{Q}}(\delta)|$  and they have the same index corresponding to  $\mathcal{O}$ . From Theorems 1 and 3 we deduce

**Theorem 4.** *Let  $b = 1, a \geq 4$ . Then every element  $\gamma \in \mathcal{O}$  such that  $\mathbb{Z}[\gamma] = \mathcal{O}$  is equivalent to some 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.* The order  $\mathcal{O}_{a,1}$  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  $\mathcal{O}_{a,1}$  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.

2. PREPARATIONS TO THE PROOF OF THEOREM 1

In §§2-4 we shall use the notation  $(v, a_1, a_2, a_3, \delta_3)$  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  $a > 100$ . Denote by  $\alpha$  the largest and by  $\beta$  the second-largest real zeros of  $p(x) = p_a(x, 1)$ , and put  $\varepsilon = \alpha - \alpha^{-1}$ .

We first establish more precise estimates than those proved in [8]. Using Taylor's formula at the point  $a$ , we get

$$(4) \quad a - \frac{2}{a^3} < \alpha \leq a - \frac{1}{a^3}.$$

Since  $\varepsilon = \frac{1}{2}(a + \sqrt{a^2 - 4})$  [note that  $\varepsilon$  is the largest root of the polynomial  $X^2 - aX + 1$ ], using the development of  $(1 + u)^{1/2}$ , we see that

$$(5) \quad a - \frac{1}{a} - \frac{2}{a^3} < \varepsilon < a - \frac{1}{a} - \frac{1}{a^3}.$$

If  $\varepsilon' = \frac{1}{2}(a - \sqrt{a^2 - 4})$  is the conjugate of  $\varepsilon$ , then  $\varepsilon' = \beta - \beta^{-1}$ . Hence,  $\beta = \frac{\varepsilon'}{2} + \sqrt{1 + \varepsilon'^2/4}$ . This formula, the relation  $\varepsilon' = a - \varepsilon$  and (5) lead to the inequalities

$$(6) \quad 1 + \frac{1}{2a} + \frac{1}{5a^2} < \beta < 1 + \frac{1}{2a} + \frac{1}{3a^2}.$$

Using the estimates above and the inequalities  $\frac{1}{x} - \frac{2}{x^2} < \log(1 + \frac{1}{x}) < \frac{1}{x}$ , which are true for  $x > 1$ , we get

$$\begin{aligned} \frac{1}{2a} < \log \beta < \frac{1}{2a} + \frac{1}{3a^2}, \\ \log a - \frac{3}{a^4} < \log \alpha < \log a, \\ \log \varepsilon &\leq \log a - \frac{1}{a^2} \quad [\text{since } \log(1 - x) < -x \text{ for } 0 < x < 1], \\ \log \frac{\alpha + 1}{\alpha - 1} &< \frac{2}{a} + \frac{2}{a^3} \quad \left[ \text{since } \frac{1}{2} \log \frac{1+x}{1-x} = x + \frac{x^3}{3} + \frac{x^5}{5} + \dots \text{ for } 0 < x < 1 \right], \\ \frac{\beta + 1}{\beta - 1} &= 1 + \frac{2}{\beta - 1} > 1 + \frac{2}{\frac{1}{2a} + \frac{1}{3a^2}} = 1 + \frac{4a}{1 + \frac{2}{3a}} > 4a - \frac{5}{3} + \frac{8}{5a}, \\ \log \frac{\beta + 1}{\beta - 1} &> \log 4a - \frac{5}{11a}. \end{aligned}$$

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

$$\begin{aligned}
 (7) \quad A &= \log \alpha \log \frac{\beta+1}{\beta-1} - \log \beta \log \frac{\alpha+1}{\alpha-1} \\
 &> \left( \log a - \frac{3}{a^4} \right) \left( \log 4a - \frac{5}{11a} \right) - \left( \frac{1}{2a} + \frac{1}{3a^2} \right) \left( \frac{2}{a} + \frac{2}{a^3} \right) \\
 &> \log a \times \left( \log 4a - \frac{1}{2a} \right),
 \end{aligned}$$

and also

$$A > \log \varepsilon \times \log \frac{\beta+1}{\beta-1}.$$

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 (in case I)

$$\begin{aligned}
 (8) \quad K_1 &< 2 \frac{\log \varepsilon \log \beta}{A} v + \frac{2}{A} \log \frac{a+1}{a-1} \log \beta \\
 &< 2 \frac{\log \varepsilon \log \beta}{A} \left( v + \frac{2.001}{a \log \varepsilon} \right) \\
 &< \frac{(1 + \frac{1}{a})(v + \frac{1}{a})}{a \log 4a} < \frac{1.02v}{a \log 4a}.
 \end{aligned}$$

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

$$(9) \quad \left( 1 + \frac{1}{a} \right) \left( v + \frac{1}{a} \right) > a \log 4a \quad [\text{and } a > 100 \text{ implies } v > 600],$$

which is stronger than (P.5.18). By (P.5.15), we also have

$$-K_2 = |K_2| < \left[ 2v \frac{\log \varepsilon \log \frac{\beta+1}{\beta-1}}{A} + 1.26 \right] \leq 2v + 1.$$

We shall use these estimates 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 (7) we have

$$(10) \quad 1 \leq K_2 - 1 \leq 2v \frac{\log \varepsilon \log \frac{\alpha+1}{\alpha-1}}{A} < 2v \frac{\log \varepsilon \log \frac{\alpha+1}{\alpha-1}}{\log(4a) + \frac{1}{6a}} < \frac{4v(1 + \frac{1}{a})}{a \log 4a}.$$

Thus, in this case

$$(11) \quad \left( 1 + \frac{1}{a} \right) v > \frac{a \log 4a}{4} \quad [\text{and } a > 100 \text{ implies } v > 150],$$

which is an improvement of (P.6.15). By (P.6.13), we have

$$|K_1| < 2v \frac{\log \varepsilon \log \frac{\alpha+1}{\alpha-1}}{A} + 1.$$

In [8], it is proved that

$$(12) \quad \Lambda_1 = \log \frac{\alpha\beta+1}{\alpha-\beta} + (K_2 - 1) \log \beta + K_1 \log \frac{\beta+1}{\beta-1}$$

satisfies  $|\Lambda_1| < \varepsilon^{-2v}$  in case I, and that

$$(13) \quad \Lambda_2 = \log \frac{\alpha\beta + 1}{\alpha - \beta} + (K_2 - 1) \log \alpha + K_1 \log \frac{\alpha + 1}{\alpha - 1}$$

satisfies  $|\Lambda_2| < 1.1\varepsilon^{-2v}$  in case II. To prove Theorem 1, we shall use lower bounds for these linear forms in logarithms of algebraic numbers. We write also

$$\Lambda'_1 = \Lambda_1 = \log \left\{ \frac{\alpha\beta + 1}{\alpha - \beta} \left( \frac{\beta + 1}{\beta - 1} \right)^{K_1} \right\} + (K_2 - 1) \log \beta$$

and

$$\Lambda'_2 = \Lambda_2 = \log \left\{ \frac{\alpha\beta + 1}{\alpha - \beta} \alpha^{K_2 - 1} \right\} + K_1 \log \frac{\alpha + 1}{\alpha - 1}.$$

Now we estimate the absolute logarithmic height of the algebraic numbers occurring in  $\Lambda_i$ , for  $i = 1$  and  $2$ . We have

$$\begin{aligned} h(\alpha) = h(\beta) &= \frac{1}{4} \log |\alpha\beta| < \frac{\log(a + 1)}{4}, \\ h(\alpha + 1) = h(\beta + 1) &= \frac{1}{4} \log |(\alpha + 1)(\beta + 1)| < \frac{\log(2a + 4)}{4}, \\ h(\alpha - 1) = h(\beta - 1) &= \frac{1}{4} \log |(\alpha - 1)(-\alpha^{-1} - 1)(\beta^{-1} - 1)| < \frac{\log(2a + 4)}{4}, \\ h\left(\frac{\alpha + 1}{\alpha - 1}\right) &= h\left(\frac{\beta + 1}{\beta - 1}\right) < \frac{\log(4a + 8)}{4}, \\ h\left(\frac{\alpha\beta + 1}{\alpha - \beta}\right) &< \frac{1}{4} \log(a^2 - 4) + \frac{1}{4} \log \frac{a + 2}{a - 1 - \frac{2}{a}} < \frac{\log(a + 3)}{2}. \end{aligned}$$

Thus,

$$(14) \quad \begin{aligned} h \left\{ \frac{\alpha\beta + 1}{\alpha - \beta} \left( \frac{\beta + 1}{\beta - 1} \right)^{K_1} \right\} &< \frac{\log(a + 3)}{2} + \frac{K_1 \log(4a + 8)}{4} \\ &< (K_1 + 2) \frac{\log(4a + 8)}{4} \end{aligned}$$

and

$$(15) \quad \begin{aligned} h \left\{ \frac{\alpha\beta + 1}{\alpha - \beta} \alpha^{K_2 - 1} \right\} &< \frac{\log(a + 3)}{2} + \frac{(K_2 - 1) \log(a + 1)}{4} \\ &< (K_2 + 1) \frac{\log(a + 3)}{4}. \end{aligned}$$

In a first version of the present paper, we applied the main theorem of [7] to  $\Lambda'_1$  and  $\Lambda'_2$  to find an upper bound of  $a$  in terms of  $v$ . Since that time, a new result was proved by Michel Laurent (see [11]). After a second version of this paper, this result was improved by Laurent, Mignotte and Nesterenko (see [12]). This second result is the following.

**Proposition 1.** *Let  $\alpha_1$  and  $\alpha_2$  be two real algebraic numbers multiplicatively independent. Consider the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where  $b_1$  and  $b_2$  are positive rational integers. Put  $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ , and let  $A_1, A_2$  be two real numbers  $\geq e$  such that

$$h(\alpha_i) \leq \log A_i, \quad i = 1, 2,$$

and let  $B$  be a real number such that  $B \geq 1 + \log b'$ , where

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

Then, if  $DB \geq 21$ , we have

$$\log |\Lambda| \geq -25D^4 B^2 \log A_1 \log A_2.$$

Now we want to bound  $a$ , and we assume  $a > 10^6$ . Here, with the notations of Proposition 1, we can choose

$$\log A_1 = \left( \frac{(1 + \frac{1}{a})(v + \frac{1}{a})}{a \log 4a} + 2 \right) \frac{\log(4a + 8)}{4}, \quad \log A_2 = \frac{\log(a + 1)}{4},$$

with  $K = |K_1|$  in case I, and

$$\log A_1 = \left( 4 \frac{(1 + \frac{1}{a})v}{a \log 4a} + 2 \right) \frac{\log(a + 3)}{4}, \quad \log A_2 = \frac{\log(4a + 8)}{4},$$

with  $K = |K_2|$  in case II. In case I,

$$8b' \leq \frac{|K_2|}{\log A_1} + \frac{1}{\log A_2} \leq \frac{4(2v + 1)}{(\frac{v}{a \log 4a} + 2) \log(4a + 8)} + 1 \leq 8a + 1,$$

thus (taking  $B = 1 + \log(a + 1)$ , so that  $DB \geq 21$  since  $D = 8$ )

$$2v \log \varepsilon < 25 \times D^4 \times \log A_1 \times \log A_2 \times (1 + \log(a + 1))^2.$$

Using (5) and dividing by  $\log(a + 1)$ , we get

$$(16) \quad 1.999v \leq 6400 \times \log(4a + 8) \times \left( \frac{1.02v}{a \log 4a} + 2 \right) \times (1 + \log(a + 1))^2.$$

Using (9) and multiplying each side of (16) by  $a/v$ , we get

$$a < 9715 \times (1 + \log a)^2,$$

which implies

$$a < 2.4 \times 10^6.$$

Moreover, it is easy to verify that relation (16) leads to the following implications:

$$a > a^* := 10^6 \Rightarrow 0.59v < 12800 \times \log(4a + 8) \times (1 + \log(a + 1))^2 \Rightarrow v < 10^8.$$

In case II,

$$8b' = \frac{|K_1|}{\log A_1} + \frac{1}{\log A_2} \leq \frac{4(2v + 1)}{(\frac{4v}{a \log 4a} + 2) \log(4a + 8)} + 1 \leq 2a + 1,$$

thus

$$2v \log \varepsilon - 0.1 < 25 \times D^4 \times \log A_1 \times \log A_2 + (1 + \log(0.25a + 1))^2.$$

Proceeding as before, we have

$$(17) \quad 1.999v \leq 6400 \log(4a + 8) \left( \frac{4.001v}{a \log 4a} + 2 \right) (1 + \log(0.25a + 1))^2.$$

Now, using (11), we get

$$a < 38800 \times (1 + \log(a/4))^2,$$

which implies

$$a < 9.6 \times 10^6.$$

Moreover, relation (17) leads to the following implications:

$$a > a^{**} := 4 \times 10^6 \Rightarrow 0.59v < 12800 \log(4a + 8)(1 + \log(0.25a + 1))^2 \Rightarrow v < 10^8.$$

Now we come back to the hypothesis  $a > 100$  and we use a result of Waldschmidt [10] to find an upper bound for  $v$  for the remaining values of  $a$ . Thus, we assume  $a \leq a^*$  in case I, respectively  $a \leq a^{**}$  in case II. For the convenience of the reader, we recall Waldschmidt's result.

**Proposition 2.** *Let  $\alpha_1, \dots, \alpha_n$  be nonzero algebraic numbers; for  $i = 1, \dots, n$ , let  $\log \alpha_i$  be a determination of the logarithm of  $\alpha_i$ . Suppose that the numbers  $\log \alpha_1, \dots, \log \alpha_n$  are  $\mathbb{Q}$ -linearly independent. Put*

$$D = [\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}] \quad \text{and} \quad g = [\mathbb{R}(\log \alpha_1, \dots, \log \alpha_n) : \mathbb{R}].$$

Let  $A_1, \dots, A_n, A, E$  and  $f$  be positive real numbers such that

$$\log A_i \geq h(\alpha_i) \quad (1 \leq i \leq n), \quad A = \max\{A_1, \dots, A_n\}$$

and

$$e \leq E \leq \min \left\{ A_1^D, \dots, A_n^D, \frac{nD}{f} \left( \sum_{i=1}^n \frac{|\log \alpha_i|}{\log A_i} \right)^{-1} \right\}.$$

Let  $b_1, \dots, b_n$  be rational integers with  $b_n \neq 0$ . Put

$$M = \max_{1 \leq j < n} \left\{ \frac{|b_n|}{\log A_j} + \frac{|b_j|}{\log A_n} \right\},$$

$$Z_0 = \max \left\{ 7 + 3 \log n, \frac{g}{D} \log E, \log \left( \frac{D}{\log E} \right) \right\}, \quad G_0 = \max\{4nZ_0, \log M\}$$

and

$$U_0 = \max\{D^2 \log A, D^{n+2} G_0 Z_0 \log A_1 \cdots \log A_n (\log E)^{-n-1}\}.$$

Then the linear form

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$$

satisfies

$$|\Lambda| \geq \exp \left\{ -1500g^{-n-2} 2^{2n} n^{3n+5} \left( 1 + \frac{g}{f} \right)^n U_0 \right\}.$$

Recall that  $100 < a < a^*$  (respectively,  $100 < a < a^{**}$ ). With the notations of Proposition 2, we can set for both linear forms  $\Lambda_1$  and  $\Lambda_2$

$$\begin{aligned}
 n &= 3, \quad D = 8, \quad g = 1, \\
 \alpha_1 &= \frac{\alpha\beta + 1}{\alpha - \beta}, \quad \alpha_2 = \begin{cases} \beta & \text{in case I,} \\ \alpha & \text{in case II,} \end{cases} \quad \alpha_3 = \begin{cases} (\beta + 1)/(\beta - 1) & \text{in case I,} \\ (\alpha + 1)/(\alpha - 1) & \text{in case II,} \end{cases} \\
 \log A_1 &= \frac{\log(a + 3)}{2}, \quad \log A_2 = \frac{\log(4a + 8)}{4}, \quad \log A_3 = \frac{\log(a + 1)}{4}, \\
 f &= 0.656, \quad \Sigma := \sum \frac{|\log \alpha_i|}{\log A_i} < 4.02, \quad E = 24/(f\Sigma) > 9.1, \\
 M &= \frac{4|K_1|}{\log(4a + 8)} + \frac{4|K_2 - 1|}{\log(a + 1)} \leq \begin{cases} 8.04v/\log(a + 1) & \text{in case I,} \\ 8.04v/\log(4a + 8) & \text{in case II,} \end{cases}
 \end{aligned}$$

and get

$$\log |\Lambda_i| \geq -3.275 \times 10^{15} \times G_0 \times (\log(a + 2))^2 \times \log(4a + 8) \quad \text{for } i = 1, 2,$$

where

$$G_0 = \max\{123.55, \log M\}.$$

Comparing this last inequality with (12) and (13), we get

$$2v \log \varepsilon < 3.2755 \times 10^{15} \times G_0 \times (\log(a + 2))^2 \times \log(4a + 8),$$

since  $\log \varepsilon > \log a - 1.001a^{-2} > 0.9956 \log(a + 2)$ . This implies

$$v < 1.646 \times 10^{15} \times G_0 \times \log(a + 2) \times \log(4a + 8).$$

In case I, this gives the estimate

$$v < 4.81 \times 10^{19},$$

whereas in case II, we obtain

$$v < 5.71 \times 10^{19}.$$

### 3. DIOPHANTINE APPROXIMATION PROPERTIES OF NONTRIVIAL SOLUTIONS

The following lemma is basic for the final computer search for nontrivial solutions. We denote by  $\|x\|$  the distance of the real number  $x$  to the nearest integer.

**Lemma 1.** *Suppose that  $100 < a \leq 10^7$ . Put*

$$\delta_1 = \frac{\log \frac{\alpha\beta+1}{\alpha-\beta}}{\log \beta}, \quad \text{respectively} \quad \delta_1 = \frac{\log \frac{\alpha\beta+1}{\alpha-\beta}}{\log \frac{\alpha+1}{\alpha-1}},$$

and

$$\delta_2 = \frac{\log \frac{\beta+1}{\beta-1}}{\log \beta}, \quad \text{respectively} \quad \delta_2 = \frac{\log \alpha}{\log \frac{\alpha+1}{\alpha-1}}.$$

Assume that  $\tilde{\delta}_1$  and  $\tilde{\delta}_2$  are rational numbers such that

$$(18) \quad |\delta_1 - \tilde{\delta}_1| < 10^{-50}, \quad |\delta_2 - \tilde{\delta}_2| < \varepsilon_2 = \begin{cases} 10^{-57} & \text{for } a \leq a^*, \text{ resp. } a \leq a^{**}, \\ 10^{-50} & \text{for } a > a^*, \text{ resp. } a > a^{**}, \end{cases}$$



and assume that there exists a convergent  $p/q$  in the continued fraction expansion of  $\tilde{\delta}_1$  (respectively, of  $\tilde{\delta}_2$ ) such that

$$(19) \quad q \leq 10^{28}$$

and

$$(20) \quad q\|q\tilde{\delta}_1\| > \frac{5.4 \times 10^{19}}{a \log 4a}, \quad \text{respectively} \quad q\|q\tilde{\delta}_2\| > \frac{2.6 \times 10^{20}}{a \log 4a}.$$

Then (12), respectively (13), cannot hold for  $K_1, K_2 \in \mathbb{Z}$ .

*Proof.* First consider case I. Assume that there exist  $K_1, K_2 \in \mathbb{Z}$  which satisfy (12). By (9), we have  $v > 600$ , hence

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

Let  $p/q$  be a convergent of  $\tilde{\delta}_2$  which satisfies (19) and (20). Multiplying the previous inequality by  $q$  and inserting  $\delta_1$  and  $\delta_2$ , we get

$$(21) \quad |q\tilde{\delta}_1 + q(\delta_1 - \tilde{\delta}_1) + K_1(\tilde{\delta}_2q - p) + K_1q(\delta_2 - \tilde{\delta}_2) + K_1p + (K_2 - 1)q| < 10^{-950},$$

thus

$$\|q\tilde{\delta}_1\| < 10^{-950} + q10^{-50} + q|K_1|\varepsilon_2 + |K_1| |\tilde{\delta}_2q - p|$$

and

$$(22) \quad \begin{aligned} q\|q\tilde{\delta}_1\| &< 10^{-900} + q^210^{-50} + q^2|K_1|\varepsilon_2 + |K_1| \times q|\tilde{\delta}_2q - p| \\ &< 10^6 + (1 + 10^{56}\varepsilon_2)|K_1|. \end{aligned}$$

If  $a \geq a^*$ , we know that  $v < 10^8$  and we assume  $\varepsilon_2 = 10^{-50}$ ; if  $100 < a < a^*$ , we assume  $\varepsilon_2 = 10^{-57}$  and we use the upper bound  $v < 4.81 \times 10^{19}$ . Then, using (8), we see that

$$q\|q\tilde{\delta}_1\| < \frac{5.4 \times 10^{19}}{a \log 4a},$$

which contradicts (20). This contradiction proves the lemma in the first case.

The proof is similar in the second case. We only give a few details. Assume first that there exist  $K_1, K_2 \in \mathbb{Z}$  which satisfy (13). By (12), we have  $v > 150$ , hence now

$$|\delta_1 + (K_2 - 1)\delta_2 + K_1| < 10^{-200}.$$

Let  $p/q$  be a convergent of  $\tilde{\delta}_2$  which satisfies (19) and (20); then

$$(23) \quad \begin{aligned} |q\tilde{\delta}_1 + q(\delta_1 - \tilde{\delta}_1) + (K_2 - 1)(\tilde{\delta}_2q - p) \\ + (K_2 - 1)q(\delta_2 - \tilde{\delta}_2) + K_1q + (K_2 - 1)p| < 10^{-150}, \end{aligned}$$

thus

$$(24) \quad \begin{aligned} q\|q\tilde{\delta}_1\| &< 10^{-100} + q^210^{-50} + q^2|K_2 - 1|\varepsilon_2 + |K_2 - 1| \times q|\tilde{\delta}_2q - p| \\ &< 10^6 + (1 + 10^{56}\varepsilon_2)|K_2 - 1|. \end{aligned}$$

If  $a \geq a^{**}$ , we know that  $v < 10^8$  and we assume  $\varepsilon_2 = 10^{-50}$ ; if  $100 < a < a^{**}$ , we assume  $\varepsilon_2 = 10^{-57}$  and we use the upper bound  $v < 5.71 \times 10^{19}$ . Then, using (10), we see that

$$q\|q\tilde{\delta}_1\| < \frac{2.6 \times 10^{20}}{a \log 4a},$$

which contradicts (20). This contradiction proves the lemma in the second case.  $\square$

*Remark.* We are extremely grateful to the referee who noticed a mistake in the statement of this lemma in the first version of this paper.

#### 4. THE COMPUTER SEARCH

First, we notice that in §2 we tried to use the present theory of linear forms as much as we could. This choice leads to some complications (namely the introduction of the values  $a^*$  and  $a^{**}$ ), but it has the advantage of reducing the computer work. Reducing the computer work saves some computer time (which is very large here), and, more importantly, the reliability of our result seems to be better.

For safety's sake, in case I we considered the range  $100 < a < 10^8$ , and in case II the range  $100 < a < 4 \times 10^8$ .

For evaluating approximately  $10^8$  (resp.  $4 \times 10^8$ ) equations, we decided to use distributed computation. We wrote a program which for  $a = 101$  to  $10^8$  (resp. to  $4 \times 10^8$ ) executed the following steps:

(1) Compute  $\delta_1$  and  $\delta_2$  with sufficient precision: 100 digits for  $100 \leq a \leq 10^5$ , 60 digits for  $10^5 < a \leq a^*$  (resp.  $10^5 < a \leq a^{**}$ ), and 50 digits in the range  $a > a^*$  (resp.  $a > a^{**}$ ).

(2) Compute the continued fraction expansion of  $\delta_2$ .

(3) Compute the sequence  $\{q_n\}_{n \geq 0}$  of the denominators of the convergents of  $\tilde{\delta}_2$ .

(4) **if** (20) holds for some  $q_n < 10^{28}$ , 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-digit precision. Then we considered the range  $10^5 < a \leq a^*$  (resp.  $10^5 < a \leq a^{**}$ ), with a precision of 60 digits. The remaining interval  $[a^*, 10^8]$  (resp.  $[a^{**}, 4 \times 10^8]$ ) 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 undecided cases.

Altogether the computations took

- about 1800 MIPS-days for type I,
- about 5300 MIPS-days for type II.

The real time was about 3 weeks. For every  $100 \leq a \leq 10^8$  (resp.  $\leq 4 \times 10^8$ ) we found a  $q$  with (20). This completes the proof of Theorem 1.

*Remark.* As we mentioned in the introduction, the method described in §§2–4 is also applicable for the complete resolution of other parametrized families of diophantine equations. Indeed, suppose that it is possible for a parametrized family of diophantine equations to derive finitely 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, 8] fulfill the conditions above. Obviously, Lemma 1 does not depend on the special choice of  $\delta_1$  and  $\delta_2$ . Finally, if  $B_2$  is reasonable, then one can perform the computer search described in this section.

5. THE GENERAL INDEX FORM EQUATION OF  $\mathcal{O}_{a,b}$

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

**Lemma 2.** *The elements  $1, \varepsilon, \alpha, \alpha\varepsilon$  form an integral basis of  $\mathcal{O}$ .*

*Proof.* We have

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

and

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

hence

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

which proves the assertion. □

Assume that  $[\mathbb{K} : \mathbb{Q}] = 4$ . Then  $f(\alpha) = 0$  implies that  $-\alpha^{-1}$  is a zero of  $f(x)$ . Let  $\beta$  denote one of the zeros of  $f(x)$  which is different from  $\alpha$  and  $-\alpha^{-1}$ . In the sequel we order the conjugates  $\mathbb{K}^{(i)}, i = 1, 2, 3, 4$ , of  $\mathbb{K}$  such that  $\alpha^{(1)} = \alpha, \alpha^{(2)} = -\alpha^{-1}, \alpha^{(3)} = \beta, \alpha^{(4)} = -\beta^{-1}$ . This implies  $\varepsilon^{(1)} = \varepsilon^{(2)} = \varepsilon$  and  $\varepsilon^{(3)} = \varepsilon^{(4)} = \varepsilon'$ , where  $\varepsilon'$  denotes the conjugate of  $\varepsilon$  with respect to the extension  $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ . We denote by  $D_o$  the discriminant of the order  $\mathcal{O}$  and by  $D(\gamma) = D_{\mathbb{K}/\mathbb{Q}}(\gamma)$  the discriminant of the element  $\gamma \in \mathbb{K}$ . Then

$$(25) \quad D_o = (\varepsilon - \varepsilon')^4 \left(\alpha + \frac{1}{\alpha}\right)^2 \left(\beta + \frac{1}{\beta}\right)^2 = [a^2 + 4(b - 2)]^2 ((b + 2)^2 + 4a^2).$$

For  $\gamma \in \mathcal{O}$ , let  $I_\gamma$  denote the index of  $\gamma$  in  $\mathcal{O}$ . Then we have the well-known identity

$$(26) \quad D(\gamma) = I_\gamma^2 D_o.$$

In the next lemma we transform the index form equation corresponding to  $\mathcal{O}$  to a system of quadratic equations.

**Lemma 3.** *Let  $\gamma = x_1 + x_2\varepsilon + x_3\alpha + x_4\alpha\varepsilon \in \mathcal{O}$  with index  $I_\gamma$ . Then there exist integers  $I_1, I_2, V$  with the following properties:*

$$(27) \quad I_1 I_2 = I_\gamma,$$

$$(28) \quad x_3^2 + ax_3x_4 + (2 - b)x_4^2 = I_1,$$

$$(29) \quad x_2^2 + x_2x_3 + ax_2x_4 + (b - 2)x_4^2 = V$$

and

$$(30) \quad (a^2 + 4b - 8)V^2 + (b - 6)I_1V - I_1^2 = I_2.$$

*Proof.* Put  $\gamma_{i,j} = \gamma^{(i)} - \gamma^{(j)}$  for  $1 \leq i, j \leq 4$ . Then we can rewrite (26) as

$$(31) \quad D^{1/2}(\gamma) = \prod_{1 \leq i < j \leq 4} \gamma_{i,j} = I_\gamma D_o^{1/2}.$$

Let  $\mathbb{L} = \mathbb{Q}(\frac{\alpha}{3} + \frac{\beta}{\alpha})$ ; then, since  $\frac{\alpha}{3} + \frac{\beta}{\alpha}$  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, we can show by a straightforward computation that

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

where

$$U = x_3^2 + ax_3x_4 + (2-b)x_4^2, \quad V = x_2^2 + x_2x_3 + ax_2x_4 + (b-2)x_4^2.$$

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

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

Inserting this equality and (25) into (31), 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

$$U = I_1 \quad \text{and} \quad (a^2 + 4b - 8)V^2 + (b - 6)UV - U^2 = I_2$$

proves equations (27) to (30). □

### 6. PROOF OF 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  $\gamma \in \mathcal{O}$  the powers  $1, \gamma, \gamma^2, \gamma^3$  form a basis of  $\mathcal{O}$  if and only if  $|I_\gamma| = 1$ ; thus we can use Lemma 3. Then  $|I_1| = |I_2| = 1$  by (27).

Assume that (30) 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 (30) 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 (30) 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 (29) as

$$(32) \quad x_2(x_2 + (x_3 + ax_4)) = (2 - b)x_4^2.$$

On the other hand, (28) 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

$$\begin{aligned}(u, v) &= 1, \\ b_1 b_2 &= 1, \\ uv &= x_4, \\ x_2 &= b_1 u^2, \\ x_2 + x_3 + ax_4 &= b_2 v^2.\end{aligned}$$

The second equation implies  $b_1 = b_2 = 1$ . Using this and the last three equations, we express  $x_1, x_2, x_3$  and  $x_4$  in terms of  $u$  and  $v$ . Then, inserting this expression in (28), we get (3).  $\square$

*Proof of Theorem 4.* Let  $\gamma \in \mathcal{O}$  such that  $\mathbb{Z} = \mathcal{O}$ . Up to equivalence, and in view of Lemma 2, we may suppose that  $\gamma = x_2\varepsilon + x_3\alpha + x_4\alpha\varepsilon$  with  $x_2 \geq 0$ . It is easily checked that all the conditions of Theorem 3 (with  $b = 1$ ) hold; therefore,  $(x_2, x_3, x_4) = (u^2, v^2 - u^2 - auv, uv)$ , where  $(x, y) = (v, u)$  is a solution of (1). (Note that, by Theorem 1 of [8],  $f_a(x, y) = -1$  is impossible). Theorem 1 gives explicitly all possible values for  $(v, u)$ , which are inserted to the expression for  $x_2, x_3, x_4$  above. Then, on writing  $x_2\varepsilon + x_3\alpha + x_4\alpha\varepsilon = y_1 + y_2\alpha + y_3\alpha^2 + y_4\alpha^3$ , we see that, up to equivalence, the only possibilities for  $(y_2, y_3, y_4)$  are those announced in Theorem 4.  $\square$

#### ACKNOWLEDGMENT

We are very grateful to the referee who read our manuscript with great care and who corrected some computational errors in §2 and made many helpful comments. We want to thank Volker Müller from the Universität des Saarlandes for his assistance in using PARI in library mode.

#### REFERENCES

1. R. Roth, *LiPS—Ein System für verteilte Anwendungen*, Master Thesis, Dept. of Computer Science, Universität des Saarlandes, Germany, Jan. 1992.
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. MR **92g**:11031
3. ———, *On the resolution of index form equations*, Proc. ISSAC '91 (S. M. Watt, ed.), ACM Press, 1991 pp. 185–186.
4. E. Lee, *Studies on Diophantine equations*, Ph.D. Thesis, Cambridge University, 1992.
5. M. Mignotte, *Verification of a conjecture of E. Thomas*, *J. Number Theory* **44** (1993), 172–177. MR **94m**:11035
6. M. Mignotte and N. Tzanakis, *On a family of cubics*, *J. Number Theory* **39** (1991), 41–49. MR **92h**:11021
7. M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method III*, *Ann. Fac. Sci. Toulouse Math.* (5) **97** (1989), 43–75.
8. A. Pethö, *Complete solutions to families of quartic Thue equations*, *Math. Comp.* **57** (1991), 777–798. MR **92e**:11023
9. E. Thomas, *Solutions to certain families of Thue equations*, *J. Number Theory* **43** (1993), 319–369. MR **94b**:11028
10. M. Waldschmidt, *Minoration de combinaisons linéaires de logarithmes de nombres algébriques*, *Canad. J. Math.* **45** (1993), 176–224. MR **94f**:11065
11. ———, *Linear independence of logarithms of algebraic numbers*, The Institute of Mathematical Sciences, IMSc. Report no. 116, Madras, 1992.

12. M. Laurent, M. Mignotte, and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory, to appear.

UNIVERSITÉ LOUIS PASTEUR, 7 RUE RENÉ DESCARTES, 67084 STRASBOURG CEDEX, FRANCE  
*E-mail address:* `mignotte@math.u-strasbourg.fr`

DEPARTMENT OF COMPUTER SCIENCE, KOSSUTH LAJOS UNIVERSITY, P.O. BOX 12, H-4010  
DEBRECEN, HUNGARY  
*E-mail address:* `pethoe@peugeot.dote.hu`

FB-14 INFORMATIK, UNIVERSITÄT DES SAARLANDES, POSTFACH 151150, D-66041 SAAR-  
BRÜCKEN, GERMANY  
*E-mail address:* `roth@cs.uni-sb.de`