JOURNAL OF NUMBER THEORY **60**, 373–392 (1996)
ARTICLE NO. 0129

Solving Thue Equations of High Degree

Yuri Bilu

Mathématiques Stochastiques, Université Bordeaux 2, F-33076 Bordeaux Cedex, France and Mathematisches Institut, SFB 170, Bunsenstrasse 3–5, 37073 Göttingen, Germany

and

Guillaume Hanrot[1]

Mathématiques Stochastiques, Université Bordeaux 2, F-33076 Bordeaux Cedex, France and Algorithmique Arithmétique Expérimentale (A2X), UMR CNRS 9936, Université Bordeaux 1, F-33405 Talence Cedex, France

We propose a general method for numerical solution of Thue equations, which allows one to solve in reasonable time Thue equations of high degree (provided necessary algebraic number theory data is available). We illustrate our method, solving completely concrete Thue equations of degrees 19 and 33. © 1996 Academic Press, Inc.

1. INTRODUCTION

One of the classical objects of number theory is the Diophantine equation of Thue,

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

where $f(x, y) \in \mathbf{Z}[x, y]$ is an irreducible form of degree $n \geqslant 3$ and a is a non-zero integer.

In 1909 A. Thue [Th09] proved that (1) has finitely many solutions in integers x, y. His proof was non-effective. The first effective upper bound for the solutions of Thue equation was obtained in 1968 by A. Baker [Ba68]. He combined an idea of A. O. Gelfond [Ge52] with a non-trivial lower bound for linear forms in the logarithms of algebraic numbers [Ba66].

[1] E-mail: hanrot@math.u-bordeaux.fr.

0022-314X/96 $18.00

Baker's results were improved and generalized by many authors; see [ShT86] and [Sp82] for further information and an extensive bibliography.

The result of Baker implies that all solutions of the Thue equation (1) can be found in finitely many steps, at least by direct enumeration. However, Baker's upper bound, even after numerous improvements, is so large that it is hopeless to try to solve a concrete Thue equation in this way. Nevertheless, starting from Baker and Davenport [BD69], various authors succeeded in solving completely certain Diophantine equations, combining Baker's method with some computational ideas. We refer to the papers [TW89] and [Pe90] for a description of the methods, a historical account, and further references.

To the best of our knowledge, so far only Thue equations of small degrees (3, 4, 5) have been solved. Recently P. M. Voutier [Vo95] succeeded in solving several totally real equations of higher degrees (6, 8, 9, 10, 11, 14), but he used in an essential way certain specific features of these concrete equations. See also [We92].

In this paper we show that the method of N. Tzanakis and B. M. M. de Weger [TW89], suitably modified, can solve general Thue equations of rather high degree in reasonable time. A preliminary version of our method (without numerical examples) appeared in [Bi94]. One of the ideas from [Bi94] was successfully applied in [MW94] to solve certain equations of degree 5.

Since the description of our method in [Bi94] was oriented to applications for the superelliptic Diophantine equations, we give in Section 2 an outline of the method for the (much simpler) case of Thue equations.

In Section 3, we illustrate our method by solving completely concrete Thue equations of degrees 19 and 33 (the latter seems to be the current "world record"). The choice of these equations was due to the fact that the required algebraic number theory data (fundamental units, etc.; see Section 2.1) was available. We claim that *no other special properties of these equations were used in solving them.*

2. THE DESCRIPTION OF THE METHOD

2.1. *Notation and Conventions*

We consider the equation (1) with

$$f(x, y) = f_0 y^n + f_1 y^{n-1} x + \cdots + f_n x^n = f_0 (y - \alpha^{(1)} x) \cdots (y - \alpha^{(n)} x).$$

We put $g(y) = f(1, y)$.

Let $\alpha = \alpha^{(1)}$ and

$$\sigma^{(i)}: \mathbf{K} = \mathbf{Q}(\alpha) \to \mathbf{Q}(\alpha^{(i)})$$
$$\alpha \to \alpha^{(i)}.$$

For $\beta \in \mathbf{K}$ we shall write $\beta^{(i)}$ instead of $\sigma^{(i)}(\beta)$.

We fix an ordering of the roots so that $\alpha^{(1)}, ..., \alpha^{(s)} \in \mathbf{R}$ and $\alpha^{(s+i+t)} = \alpha^{(s+i)}$ for $1 \leqslant i \leqslant t$. In the course of the paper we introduce constants $c_0, c_1, ...$, some of which will depend on the fixed ordering.

If $s = 0$ then

$$|f(x, y)| \geqslant c_0(\max(|x|, |y|))^n, \tag{2}$$

with $c_0 = f_0(|\operatorname{Im} \alpha^{(1)}| \cdots |\operatorname{Im} \alpha^{(n)}|)^{-1}$, and all integer solutions of (1) can be easily found. We suppose in the sequel that $s \geqslant 1$, in particular $\alpha \in \mathbf{R}$.

For practical implementation of the proposed method one should be able to perform the following operations in the number field $\mathbf{K}$:

(U) find a system of fundamental units;

(N) given a fractional ideal I of the field $\mathbf{K}$ and a non-zero $\lambda \in \mathbf{Q}$, find a complete system of non-associate solutions of the norm equation

$$N_{\mathbf{K}/\mathbf{Q}}(\beta) = \lambda, \qquad \beta \in I. \tag{3}$$

The units of $\mathbf{K}$ act on the solutions of (3) by multiplication. By *a complete system of non-associate solutions* of the equation (3) we mean any set of representatives of this action. It is well known that any complete system of non-associate solutions is finite, and that the problems (U) and (N) are effectively soluble [BS66, Ch. 2]. However, finding efficient algorithms for practical solution of these problems proved to be difficult, especially for fields of high degree. We do not discuss this problem further, referring instead to [Co93], [PZ89], and [Po93].

The purpose of the present paper is merely to show that the Thue equation (1) can be practically solved in reasonable time as soon as the problem (U) is solved and the problem (N) is solved for the equation

$$N_{\mathbf{K}/\mathbf{Q}}(\beta) = a/f_0, \qquad \beta \in I = (1, \alpha). \tag{4}$$

Thus, fix once and for all a system $\eta_1, ..., \eta_r$ of basic units of the field $\mathbf{K}$, where $r = s + t - 1$, and a complete system M of non-associate solutions of (4). In the important particular case $|f_0| = |a| = 1$ we have $\mathrm{M} = \{1\}$.

Since the field $\mathbf{K}$ has a real embedding, the only roots of unity in $\mathbf{K}$ are ± 1. Therefore for any solution $\beta \in I$ of the equation (4) there exists $\mu \in \pm \mathrm{M}$ and $b_1, ..., b_r \in \mathbf{Z}$ such that $\beta = \mu \eta_1^{b_1} \cdots \eta_r^{b_r}$. Here $\pm \mathrm{M} = \{\pm \mu : \mu \in \mathrm{M}\}$.

2.2. *Reduction to Linear Forms in the Logarithms*

A. O. Gelfond [Ge52] noticed that every large solution of a Thue equation corresponds to a very small value of a certain linear form in the logarithms of algebraic numbers. In this subsection we describe this correspondence explicitly. We follow [TW89] with some changes.

Fix a solution $(x, y) \in \mathbf{Z}^2$ of the equation (1). **The first observation** is: if x is large enough then the ratio y/x is very close to one of the real roots $\alpha^{(1)}, \ldots, \alpha^{(s)}$.

PROPOSITION 2.2.1. *Put*

$$X_0 = \begin{cases} \left(\dfrac{2^{n-1} \cdot |a|}{\min_{1 \leqslant i \leqslant t} |g'(\alpha^{(s+i)})| \cdot \min_{1 \leqslant i \leqslant t} |\operatorname{Im} \alpha^{(s+i)}|} \right)^{1/n} & \text{if} \quad t \geqslant 1, \\ 1 & \text{if} \quad t = 0, \end{cases}$$

$$c_1 = \frac{2^{n-1} \cdot |a|}{\min_{1 \leqslant i \leqslant s} |g'(\alpha^{(i)})|},$$

$$c_2 = \min_{1 \leqslant i < j \leqslant n} |\alpha^{(i)} - \alpha^{(j)}|,$$

$$X_1 = \max(X_0, ((n+1)\, c_1 c_2^{-1})^{1/n}).$$

Let (x, y) *be an integer solution of* (1).

(i) *If* $|x| > X_0$ *then for some* $i_0 \in \{1, \ldots, s\}$ *we have*

$$\left| \frac{y}{x} - \alpha^{(i_0)} \right| \leqslant \frac{c_1}{|x|^n}. \tag{5}$$

(ii) *If* $|x| > X_1$ *then*

$$\frac{n+2}{n+1} |\alpha^{(i_0)} - \alpha^{(i)}| \geqslant \left| \frac{y}{x} - \alpha^{(i)} \right| \geqslant \frac{n}{n+1} |\alpha^{(i_0)} - \alpha^{(i)}| \quad (i \neq i_0). \tag{6}$$

Proof. For (i) see [TW89, Lemma 1.1]. To prove (ii) note that $|x|^n \geqslant (n+1)\, c_1 c_2^{-1}$, whence

$$\left| \frac{y}{x} - \alpha^{(i_0)} \right| \leqslant \frac{1}{n+1} c_2 \leqslant \frac{1}{n+1} |\alpha^{(i_0)} - \alpha^{(i)}|,$$

which implies (6).

It is worth mentioning that (6) is slightly sharper than the corresponding inequality in [TW89], which results in improving some of the constants, in particular c_6.

In concrete examples the constant X_1 is very small, and solutions satisfying $|x| \leqslant X_1$ can be easily enumerated. Suppose now that $|x| > X_1$, so that (5) holds for some i_0. We will assume $i_0 = 1$; other values of i_0 can be treated similarly.

We have

$$\left|\frac{y}{x} - \alpha\right| \leqslant \frac{c_1}{|x|^n}, \tag{7}$$

$$\frac{n+2}{n+1}\,|\alpha - \alpha^{(i)}| \geqslant \left|\frac{y}{x} - \alpha^{(i)}\right| \geqslant \frac{n}{n+1}\,|\alpha - \alpha^{(i)}| \qquad (i > 1). \tag{8}$$

Combining "Siegel's identity"

$$(\alpha - \alpha^{(3)})(y - \alpha^{(2)}x) - (\alpha - \alpha^{(2)})(y - \alpha^{(3)}x) = (\alpha^{(2)} - \alpha^{(3)})(y - \alpha x) \tag{9}$$

with (7) and (8), we obtain

$$\left|\frac{\alpha - \alpha^{(3)}}{\alpha - \alpha^{(2)}}\,\frac{y - \alpha^{(2)}x}{y - \alpha^{(3)}x} - 1\right| \leqslant \frac{c_3}{|x|^n}, \tag{10}$$

where

$$c_3 = \frac{n+1}{n}\,\frac{|\alpha^{(2)} - \alpha^{(3)}|}{|\alpha - \alpha^{(2)}|\;|\alpha - \alpha^{(3)}|}\,c_1.$$

The second observation is that Eq. (1) may be written as

$$N_{\mathbf{K}/\mathbf{Q}}(y - \alpha x) = a/f_0, \tag{11}$$

where $N_{\mathbf{K}/\mathbf{Q}}$ is the norm map. Therefore there exist $\mu \in \pm \mathrm{M}$ and $b_1, \ldots, b_r \in \mathbf{Z}$ such that

$$y - \alpha x = \mu \eta_1^{b_1} \cdots \eta_r^{b_r}. \tag{12}$$

Combining (10) and (12), we obtain

$$|\beta_0 \beta_1^{b_1} \cdots \beta_r^{b_r} - 1| \leqslant c_3\,|x|^{-n}, \tag{13}$$

where

$$\beta_0 = \frac{\alpha - \alpha^{(3)}}{\alpha - \alpha^{(2)}}\,\frac{\mu^{(2)}}{\mu^{(3)}}, \qquad \beta_j = \frac{\eta_j^{(2)}}{\eta_j^{(3)}} \quad (1 \leqslant j \leqslant r).$$

Denote by log the principal value of the logarithm, that is $-\pi < \operatorname{Im} \log z \leqslant \pi$. Then for any complex number z with $|z| \leqslant 1/2$ we have

$$|\log(1+z)| \leqslant 1.39\,|z| \tag{14}$$

(see [TW89, p. 106]). We obtain the following assertion.

PROPOSITION 2.2.2. *Put* $X_2 = \max(X_1, (2c_3)^{1/n})$ *and* $c_4 = 1.39c_3$. *Let* $|x| \geqslant X_2$. *Then in the previous notations we have*

$$|\log \beta_0 + b_1 \log \beta_1 + \cdots + b_r \log \beta_r + b_{r+1}\pi i| \leqslant c_4\,|x|^{-n}, \tag{15}$$

for some $b_{r+1} \in \mathbf{Z}$.

Comparing the imaginary parts, we obtain

$$\begin{aligned} |b_{r+1}| &\leqslant 1 + |b_1| + \cdots + |b_r| + \pi^{-1}c_4\,|x|^{-n} \\ &\leqslant 1.23 + |b_1| + \cdots + |b_r|, \end{aligned} \tag{16}$$

because by the definition of c_4 and X_2 we have $\pi^{-1}c_4\,|x|^{-n} \leqslant 1.39(2\pi)^{-1} < 0.23$.

The third observation is that

$$B = \max(|b_1|, \ldots, |b_r|) \leqslant c_5 \log |x| + c_6. \tag{17}$$

Indeed, we have

$$\begin{aligned} \log|y - \alpha^{(i+1)}x| = \log|\mu^{(i+1)}| + b_1 \log|\eta_1^{(i+1)}| + \cdots \\ + b_r \log|\eta_r^{(i+1)}| \qquad (1 \leqslant i \leqslant r). \end{aligned} \tag{18}$$

Let $A = [a_{ij}]_{1 \leqslant i,j \leqslant r}$ be the inverse of the matrix

$$[\log|\eta_j^{(i+1)}|]_{1 \leqslant i,j \leqslant r} \tag{19}$$

(The matrix (19) is non-degenerate, because its determinant is $\pm 2^{-t}$ times the regulator of the field $\mathbf{K}$.) Then for $1 \leqslant i \leqslant r$ we have

$$\begin{aligned} b_i &= \left(\sum_{j=1}^{r} a_{ij}\right) \log|x| + \sum_{j=1}^{r} a_{ij} \log\left|\frac{y/x - \alpha^{(j+1)}}{\mu^{(j+1)}}\right| \\ &= \left(\sum_{j=1}^{r} a_{ij}\right) \log|x| + \sum_{j=1}^{r} a_{ij} \log\left|\frac{\alpha - \alpha^{(j+1)}}{\mu^{(j+1)}}\right| \\ &\quad + \sum_{j=1}^{r} a_{ij} \log\left|\frac{y/x - \alpha^{(j+1)}}{\alpha - \alpha^{(j+1)}}\right|. \end{aligned} \tag{20}$$

We derive from (8) that

$$\left|\sum_{j=1}^{r} a_{ij} \log \left|\frac{y/x-\alpha^{(j+1)}}{\alpha-\alpha^{(j+1)}}\right|\right| \leqslant \sum_{j=1}^{r} |a_{ij}| \log \frac{n+2}{n+1} \leqslant \frac{1}{n} \sum_{j=1}^{r} |a_{ij}|.$$

This proves (17) with

$$\begin{aligned} c_5 &= \max_{1 \leqslant i \leqslant r} \left|\sum_{j=1}^{r} a_{ij}\right|, \\ c_6 &= \max_{1 \leqslant i \leqslant r} \left(\frac{1}{n} \sum_{j=1}^{r} |a_{ij}| + \left|\sum_{j=1}^{r} a_{ij} \log \left|\frac{\alpha-\alpha^{(j+1)}}{\mu^{(j+1)}}\right|\right|\right). \end{aligned} \tag{21}$$

Actually, B and $\log |x|$ have the same order of magnitude; i.e., in addition to (17) we have also $\log |x| \ll B$. We do not need this fact here.

Remark 2.2.3. It is worth mentioning that formula (20), though innocent looking, will play a crucial role in this paper. First, in Subsection 2.4 it would allow us to use continued fractions instead of the LLL-reduction algorithm. Second, when we compute the very important constant c_5, we take into account probable fluctuations of signs of a_{ij}. Third, our approach to the final enumeration in Subsection 2.5 is also based on (20).

From (16) we obtain the inequality

$$B' = \max(|b_1|, ..., |b_{r+1}|) \leqslant (1.23 + rB) \leqslant c_7 \log |x| + c_8 \tag{22}$$

with $c_7 = rc_5$ and $c_8 = 1.23 + rc_6$.

Taking together (15) and (22), we get

$$|\log \beta_0 + b_1 \log \beta_1 + \cdots + b_r \log \beta_r + b_{r+1} \pi i| \leqslant c_9 \exp(-c_{10} B') \tag{23}$$

with $c_9 = c_4 \exp(nc_8/c_7)$ and $c_{10} = n/c_7$.

2.3. *A Large Upper Bound for B*

Now we apply Baker's result on linear forms in the logarithms. Baker's original bound [Ba66] was improved by many authors. We apply a recent result of Baker and Wüstholz [BW93], formulating it in a form convenient for the present paper.

THEOREM 2.3.1 [BW93, p. 20]. *Let $\beta_0, ..., \beta_r$ be complex algebraic numbers distinct from* 0 *and* 1, *and $b_1, ..., b_{r+1}$ rational integers. Also, let*

$$d \geqslant [\mathbf{Q}(\beta_0, ..., \beta_r): \mathbf{Q}], \tag{24}$$

$$h_i \geqslant \max(h(\beta_i), d^{-1} |\log \beta_i|, d^{-1}) \qquad (0 \leqslant i \leqslant r), \tag{25}$$

where $h(\ldots)$ is the absolute logarithmic height. Then either

$$\Lambda = \log \beta_0 + b_1 \log \beta_1 + \cdots + b_r \log \beta_r + b_{r+1} \pi i = 0, \tag{26}$$

or

$$|\Lambda| \geqslant \exp(-c_{11} \log B''). \tag{27}$$

Here $B'' = \max(B', e)$, B' being from (22), and

$$c_{11} = 18\pi \cdot 32^{r+4}(r+3)!\,(r+2)^{r+3}\, d^{r+3} \log(2d(r+2))\, h_0 \cdots h_r.$$

Remark 2.3.2. The parameters n, $h'(\alpha_1)$, ..., $h'(\alpha_n)$, $h'(L)$ of the original theorem in [BW93] correspond in Theorem 2.3.1 to $r+2$, h_0, ..., h_r, π/d, $\log B''$, respectively.

We have slightly modified the statement in [BW93], to allow inequalities in (24) and (25). It is often much easier (and quicker) to find an upper bound for the degree of a number field or for the height of an algebraic number, than to compute them exactly.

The following lemma is the case $h = 1$ of Lemma 2.2 from [PW87].

LEMMA 2.3.3. *Let z and C_1 be positive real numbers and C_2 an arbitrary real number. Suppose that*

$$z \leqslant C_1 \log z + C_2. \tag{28}$$

Then

$$z \leqslant 2(C_1 \log C_1 + C_2).$$

Applying Theorem 2.3.1 in our case, we see that either

$$\frac{\alpha - \alpha^{(3)}}{\alpha - \alpha^{(2)}} \frac{y - \alpha^{(2)} x}{y - \alpha^{(3)} x} = 1, \tag{29}$$

or $B'' = e$, or $c_9 e^{-c_{10} B''} \geqslant e^{-c_{11} \log B''}$, as follows from (23) and (27). The latter inequality can be rewritten as

$$B'' \leqslant c_{10}^{-1} c_{11} \log B'' + c_{10}^{-1} \log c_9,$$

which, in view of Lemma 2.3.3, implies that

$$B'' \leqslant 2 c_{10}^{-1} c_{11} \log(c_{10}^{-1} c_{11} c_9^{1/c_{11}}).$$

The relation (29) yields that $y = \alpha x$, which is impossible. Therefore

$$B \leqslant B' \leqslant B'' \leqslant B_0, \tag{30}$$

where $B_0 = \max(e, 2c_{10}^{-1} c_{11} \log (c_{10}^{-1} c_{11} c_9^{1/c_{11}}))$.

2.4. *Reduction of Baker's Bound*

2.4.1. *Preliminaries.* In practice, the value of B_0 is too large for directly enumerating all possible $\mathbf{b} = (b_1, ..., b_r)$. However, B_0 may be significantly reduced by applying an appropriate version of the LLL-reduction algorithm, as described in [TW89]. The following improved version of LLL-TW reduction was proposed in [Bi94].

As above, let $A = [a_{ij}]_{1 \leqslant i, j \leqslant r}$ be the inverse of the matrix (19). For $1 \leqslant i \leqslant r$ put

$$\delta_i = \sum_{j=1}^{r} a_{ij},$$

$$\lambda_i = \sum_{j=1}^{r} a_{ij} \log \left| \frac{\alpha - \alpha^{(j+1)}}{\mu^{(j+1)}} \right|.$$

Fix distinct i_1 and i_2 such that $|\delta_{i_2}| \leqslant |\delta_{i_1}|$ and put

$$\delta = \delta_{i_1}^{-1} \delta_{i_2},$$

$$\lambda = \delta_{i_1}^{-1} (\delta_{i_2} \lambda_{i_1} - \delta_{i_1} \lambda_{i_2}).$$

By the choice of i_1 and i_2 we have $|\delta| \leqslant 1$.

PROPOSITION 2.4.1. *Let* $c_{12} = 2.78 c_1 c_2^{-1} \max_{1 \leqslant i \leqslant r} \sum_{j=1}^{r} |a_{ij}|$. *Then*

$$|b_{i_2} - \delta b_{i_1} + \lambda| \leqslant c_{12} |x|^{-n} \tag{31}$$

(*provided* $|x| > X_2$).

Proof. By (7) and (14) we obtain

$$\left| \log \left| \frac{y/x - \alpha^{(j+1)}}{\alpha - \alpha^{(j+1)}} \right| \right| \leqslant \left| \log \left(1 + \frac{y/x - \alpha}{\alpha - \alpha^{(j+1)}} \right) \right|$$

$$\leqslant 1.39 c_2^{-1} \left| \frac{y}{x} - \alpha \right|$$

$$\leqslant 1.39 c_1 c_2^{-1} |x|^{-n} \qquad (1 \leqslant j \leqslant r). \tag{32}$$

Combining this with (20), we get

$$|\delta_i \log |x| - b_i + \lambda_i| \leqslant c_{13} |x|^{-n} \qquad (1 \leqslant i \leqslant r), \tag{33}$$

where $c_{13} = 1.39 c_1 c_2^{-1} \max_{1 \leqslant i \leqslant r} \sum_{j=1}^{r} |a_{ij}|$. Therefore

$$\begin{aligned} |b_{i_2} - \delta b_{i_1} + \lambda| &= |\delta_{i_2} \log |x| - b_{i_2} + \lambda_{i_2} - \delta(\delta_{i_1} \log |x| - b_{i_1} + \lambda_{i_1})| \\ &\leqslant |\delta_{i_2} \log |x| - b_{i_2} + \lambda_{i_2}| + |\delta| \, |\delta_{i_1} \log |x| - b_{i_1} + \lambda_{i_1}| \\ &\leqslant (1 + |\delta|) \, c_{13} |x|^{-n}. \end{aligned}$$

This proves (31) because $(1 + |\delta|) \, c_{13} \leqslant 2c_{13} = c_{12}$.

In view of (17), we have

$$|b_{i_2} - \delta b_{i_1} + \lambda| \leqslant c_{14} \exp(-c_{15} B) \tag{34}$$

with $c_{14} = c_{12} \exp(nc_6/c_5)$ and $c_{15} = n/c_5$. Now, instead of applying the LLL-reduction to the linear inequality (23) in r variables $b_1, ..., b_r$, as in [TW89], we apply it to the inequality (34) in 2 variables, which turns out to be more efficient.

In practice, it is better to define i_1 by the condition

$$|\delta_{i_1}| = \max_{1 \leqslant i \leqslant r} |\delta_i| = c_5, \tag{35}$$

and then choose an arbitrary $i_2 \neq i_1$. Clearly, $\delta_{i_1} \neq 0$, because the matrix A is non-degenerate.

2.4.2. *The Reduction*

Tzanakis and de Weger [TW89] reduced the upper bound for B using the LLL-reduction algorithm. Since we have only two variables b_{i_1} and b_{i_2}, we may replace the LLL by the simple procedure described in [BD69].

Let $\kappa > 2$ be a not very large number (a few paragraphs below we discuss the practical choice of κ). By the theorem of Dirichlet, there exists a positive integer $q \leqslant \kappa B_0$ such that

$$\|q\delta\| \leqslant (\kappa B_0)^{-1}, \tag{36}$$

where $\| \cdots \|$ is the distance to the nearest integer. In practice q can be quickly found from the continuous fraction expansion of δ. Multiplying (34) by q, we obtain

$$\| \pm b_{i_1} \| q\delta\| + q\lambda\| \leqslant c_{14} \kappa B_0 \exp(-c_{15} B), \tag{37}$$

where "$\pm$" should be "$+$" if $q\delta$ is smaller than the nearest integer and "$-$" otherwise.

It follows from (36) that $|b_{i_1}| \cdot \|q\delta\| \leqslant \kappa^{-1}$. Therefore (37) implies that

$$\|q\lambda\| - \kappa^{-1} \leqslant c_{14}\kappa B_0 \exp(-c_{15}B). \tag{38}$$

If $\|q\lambda\| > \kappa^{-1}$, which is heuristically plausible when κ is large enough, then we have a new estimate for B:

$$B \leqslant c_{15}^{-1}\left(\log B_0 + \log \frac{c_{14}\kappa}{\|q\lambda\| - \kappa^{-1}}\right). \tag{39}$$

In particular, when $\|q\lambda\| \geqslant 2\kappa^{-1}$, we have an estimate

$$B \leqslant c_{15}^{-1}(\log B_0 + \log (c_{14}\kappa^2)) \tag{40}$$

(compare this with the lemma from [BD69, Section 3]).

We took as a starting value $\kappa = 10$, and tried the first reduction. If $\|q\lambda\| < 2\kappa^{-1}$, then we changed κ by 10κ and repeated the process. In all cases we obtained successful reduction in two or three iterations at most.

The reduced bound for B can be reduced again, using the same procedure, etc. In practical examples we obtained $B \leqslant 60$ after the first reduction step, and $B \leqslant 6$ after the second reduction. We did not have enough numerical practice to make a definite conclusion why the reduction was so efficient. We guess that the success was achieved, in particular, due to accurate computation of the constant c_5, see Remark 2.2.3. Since in our examples n is large, this gives a rather large value for $c_{15} = n/c_5$, which improves the quality of estimate (40).

2.4.3. *Computational Remarks*

In practice, we deal with an approximate value of δ, which we denote by $\tilde{\delta}$. Instead of (36) we have $\|q\tilde{\delta}\| \leqslant (\kappa B_0)^{-1}$, and (38) turns to

$$\|q\lambda\| - \kappa^{-1} - \kappa B_0^2 |\delta - \tilde{\delta}| \leqslant c_{14}\kappa B_0 \exp(-c_{15}B).$$

The term $\kappa B_0^2 |\delta - \tilde{\delta}|$ can be "ignored" only when the error $|\delta - \tilde{\delta}|$ is very small. We found the approximation $\tilde{\delta}$ with accuracy $|\delta - \tilde{\delta}| \leqslant 0.1(\kappa B_0)^{-2}$. In this case we have (40) assuming $\|q\lambda\| \geqslant 2.1\kappa^{-1}$.

To compute δ with error $0.1(\kappa B_0)^{-2}$, one needs even higher precision for the entries of the matrix A. This, in turn, requires very high accuracy in computing the entries of the matrix (19), and very accurate inverting of the latter. Inverting the high-dimensional matrix (19) with entries having many (in practice, several hundreds) decimal digits is the most time-consuming operation of our method.

Since matrix inversion is not stable, we had to make special effort for estimating the accuracy of this operation. We used the following lemma.

(Given a matrix R with real entries, we denote by $|R|_\infty$ the maximum of the absolute values of its entries.)

LEMMA 2.4.2. *Let R, $\tilde{R}$, A, $\tilde{A}$ be $r \times r$-matrices with real entries and ε_1, ε_2 positive real numbers, satisfying the following conditions*:

$$AR = I, \tag{41}$$

$$|R - \tilde{R}|_\infty \leqslant \varepsilon_1, \tag{42}$$

$$|\tilde{A}\tilde{R} - I|_\infty \leqslant \varepsilon_2, \tag{43}$$

$$r\,|\tilde{A}|_\infty\,\varepsilon_1 + \varepsilon_2 \leqslant \frac{1}{2r}, \tag{44}$$

where I is the $r \times r$ identity matrix. Then

$$|A - \tilde{A}|_\infty \leqslant \varepsilon_3, \tag{45}$$

where $\varepsilon_3 = 2r^2\,|\tilde{A}|_\infty (r\,|\tilde{A}|_\infty\,\varepsilon_1 + \varepsilon_2)$.

Proof. Combining (42) and (43), we obtain

$$|\tilde{A}R - I|_\infty \leqslant \varepsilon_4, \tag{46}$$

where ε_4 is the left-hand side of (44). Write $\tilde{A}R = I + E$ with $|E|_\infty \leqslant \varepsilon_4$. By induction one easily proves that $|E^v|_\infty \leqslant r^{v-1}\varepsilon_4^v$, where $v = 1, 2, \ldots$. Therefore

$$\begin{aligned} |(I+E)^{-1}|_\infty &\leqslant 1 + \sum_{v=1}^{\infty} |E^v|_\infty \\ &\leqslant 1 + \frac{\varepsilon_4}{1 - r\varepsilon_4} \leqslant 1 + 2\varepsilon_4 \leqslant 2. \end{aligned}$$

Using this, we obtain

$$|A|_\infty = |(I+E)^{-1}\,\tilde{A}|_\infty \leqslant r\,|(I+E)^{-1}|_\infty\,|\tilde{A}|_\infty \leqslant 2r\,|\tilde{A}|_\infty.$$

Finally, we have

$$|A - \tilde{A}|_\infty = |EA|_\infty \leqslant r\,|E|_\infty\,|A|_\infty \leqslant 2r^2\,|\tilde{A}|_\infty\,\varepsilon_4 = \varepsilon_3,$$

and the proof is complete.

We apply this lemma with R the matrix (19), $\tilde{R}$ the approximation we compute, and $\tilde{A}$ the approximate inverse matrix. Since matrix multiplication is stable, one can easily find ε_2 and then compute ε_3. If ε_3 is not small

enough (which never happened in our computations), one has to find the entries of the matrix (19) with higher precision (that is, reduce ε_1) and recompute the inverse matrix.

In Subsections 3.2 and 3.3 we give a detailed information about the accuracy of our computations.

When $s \geqslant 2$, the computational time can be reduced using the following observation. Let $A^{(i_0)}$ be the inverse of the matrix, obtained by removing the i_0 th row from the matrix

$$[\log |\eta_j^{(i)}|]_{1 \leqslant i \leqslant r+1,\ 1 \leqslant j \leqslant r}. \tag{47}$$

Then $A^{(1)} = A$ and the matrix $A^{(i_0)}$ plays the same role for the arbitrary i_0 as A for $i_0 = 1$.

Multiplying the rows $s+1, ..., r+1$ of the matrix (47) by 2, we obtain a matrix with the sum of rows equal to zero. This implies a simple relation between the matrices $A^{(i_0)}$ and $A^{(i_0')}$ for different i_0 and i_0'. For example, suppose that $2 \leqslant i_0 \leqslant s$. Then

$$A^{(i_0)} = A^{(i_0-1)} T^{(i_0)}, \tag{48}$$

where the matrix $T^{(i_0)} = [t_{ij}]$ is defined by

$$t_{ij} = \begin{cases} -1, & i = i_0 - 1, \quad j \leqslant s-1, \\ -2, & i = i_0 - 1, \quad j \geqslant s, \\ 1, & i = j \neq i_0 - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Thus, having computed $A = A^{(1)}$ by inverting (19), we can quickly compute $A^{(2)}, ..., A^{(s)}$ from (48). Of course, this requires additional precision for the entries of A (approximately $(s-1)[\log_{10} n + 1]$ additional decimal digits), to compensate the rounding errors that occur in the iterative use of the relation (48).

2.4.4. *The Approach of Mignotte and de Weger*

As in (13), we have the inequalities

$$|\beta_0(j)\, \beta_1(j)^{b_1} \cdots \beta_r(j)^{b_r} - 1| \leqslant c_{16}\, |x|^{-n} \qquad (3 \leqslant j \leqslant s+t), \tag{49}$$

where

$$\beta_0(j) = \frac{\alpha - \alpha^{(j)}}{\alpha - \alpha^{(2)}} \frac{\mu^{(2)}}{\mu^{(j)}}, \qquad \beta_k(j) = \frac{\eta_k^{(2)}}{\eta_k^{(j)}} \qquad (1 \leqslant k \leqslant r),$$

$$c_{16} = \frac{n+1}{n} \max_{3 \leqslant j \leqslant s+t} \frac{|\alpha^{(2)} - \alpha^{(j)}|}{|\alpha - \alpha^{(2)}|\ |\alpha - \alpha^{(j)}|}.$$

Putting

$$L_j(\mathbf{b}) = \log|\beta_0(j)| + b_1 \log|\beta_1(j)| + \cdots + b_r \log|\beta_r(j)|, \tag{50}$$

we obtain $r-1 = s+t-2$ simultaneous linear inequalities

$$|L_j(\mathbf{b})| \leqslant c_{17} \exp(-c_{15} B) \qquad (3 \leqslant j \leqslant s+t) \tag{51}$$

with $c_{17} = 1.39 c_{16} \exp(nc_6/c_5)$. It is easy to see that inequality (34) can be obtained (with another value of c_{14}) by linear elimination of all variables except b_{i_1} and b_{i_2} from the simulateneous inequalities (51). This is exactly what was done in [Bi94].

Mignotte and de Weger [MW94] modified this idea, suggesting to apply the LLL-reduction directly to the system of linear inequalities (51). This approach has the following advantages:

- inverting a large matrix with high accuracy can be avoided;
- constants should be computed with precision about $B_0^{-(r/r-1)}$ instead of B_0^{-2}, as in our approach;
- the inequality (40) can be improved, because $\log B_0$ can be replaced there by $\log B_0/(r-1)$.

However, one has to apply the LLL-algorithm to an r-dimensional lattice, which is very slow when r is large.

Of course, one can try an intermediate approach, eliminating from (51) all but three or four variables, etc. Since in our case the use of two variables leads to good numerical results in reasonable time, we did not try this possibility.

2.5. *Final Enumeration*

Unfortunately, the reduced bound B_0' may also be too large for direct enumeration, because one has to check $(2B_0'+1)^r$ possibilities for the vector $\mathbf{b}$. One can imagine several ways to overcome this difficulty:

- use of the continued fraction expansions of $\alpha^{(1)}$, ..., $\alpha^{(s)}$, see [Pe90] and [TW89] for the details;
- sieving modulo several primes, as in [TW92] and [Sm95], for instance;
- use of Fincke–Pohst algorithm for finding all short vectors in a lattice, as in [We87] and [TW92], for instance.

In [Bi94] one further approach to final enumeration was proposed, based on the inequality (31). As a direct consequence of the latter, we obtain

PROPOSITION 2.5.1. *For* $1 \leqslant i \leqslant r$ *put*

$$b'_i = \delta_{i_1}^{-1}\delta_i b_{i_1} - \delta_{i_1}^{-1}(\delta_i \lambda_{i_1} - \delta_{i_1}\lambda_i),$$

where i_1 *is defined from* (35). *Suppose that* $|x| > X_3 = \max(X_2, (2c_{12})^{1/n})$. *Then*

$$|b_i - b'_i| < 1/2 \qquad (1 \leqslant i \leqslant r). \tag{52}$$

Thus, if $x > X_3$, then b_i is the nearest integer to b'_i. This means that the vector $\mathbf{b}$ is defined uniquely as soon as b_{i_1} is given. Therefore we have to check only $2B'_0 + 1$ possibilities for the vector $\mathbf{b}$.

Remark 2.5.2. As most of the constants above, X_3 actually depends on the value of the index $i_0 \in \{1, ..., s\}$, defined in Proposition 2.2.1. We put

$$\hat{X}_3 = \max_{1 \leqslant i_0 \leqslant s} X_3^{(i_0)}.$$

2.6. *The Algorithm*

As described above, we may propose the following algorithm for solving Thue equations.

Step 1. Find the set M and a system of basic units of the field $\mathbf{K}$.

Step 2. Find all solutions (x, y) satisfying $|x| \leqslant \hat{X}_3$.

Step 3. Fix an index $i_0 \in \{1, ..., s\}$ and $\mu \in \pm \mathrm{M}$.

Step 4. Compute Baker's bound B_0.

Step 5. Find the reduced bound B'_0, as described in Subsection 2.4.

Step 6. Using Proposition 2.5.1, find all possibilities for the vector $\mathbf{b}$, and for each of them verify whether it really corresponds to a solution (x, y) of the Thue equation (1).

Step 7. Repeat steps 4–6 for all pairs $(i_0, \mu) \in \{1, ..., s\} \times \pm \mathrm{M}$.

3. THE EXAMPLES

In this section, we present a detailed solution of some concrete Thue equations of high degree.

3.1. *Generalities*

We first give a few details related to the computations described hereafter.

3.1.1. *Families of Thue Equations*

In practice, Thue equations often occur in finite families $f(x, y) = a_i$, where a_i belong to a finite set of non-zero integers. See [Vo95] for an example. Therefore we introduced several minor changes into the algorithm, in order to enable it to solve such families simultaneously. Namely, in the definitions of X_0 and c_1 we replaced $|a|$ by $\max_i |a_i|$, and replaced the set M by $\bigcup_i \mathrm{M}_i$, where M_i is defined for a_i as M for a. Also, since δ depends only in i_0 but independent in μ, we fixed i_0 and performed the steps 4–6 of the algorithm simultaneously for all μ.

3.1.2. *The Constants*

Recall that most of the constants depend on $i_0 \in \{1, ..., s\}$ and $\mu \in \mathrm{M}$. We give for each constant its worst (maximal or minimal) value.

3.1.3. *The Program*

The computations were performed by a program written in C, using the PARI/GP programming library, version 1.39.03, in a Sparc 10. Its listing can be obtained via e-mail from the second author.

3.2. *The Equations* $y^{19} + 2x^{19} = \pm 1, \pm 2$

The field $\mathbf{K} = \mathbf{Q}(\sqrt[19]{2})$ has one real and 9 pairs of complex embeddings, whence $r = 9$. We used the system of fundamental units given in [Po93, p. 60]. The one-element set $\mathrm{M} = \{\sqrt[19]{2}\}$ is a complete system of non-associate solutions of $N_{\mathbf{K}/\mathbf{Q}}(\beta) = 2$ in the ideal $(1, \sqrt[19]{2}) = (1)$.

Here are the values of the main constants, rounded in the proper direction:

$$c_1 = 14310 \qquad c_2 = 0.341 \qquad c_3 = 12817$$

$$c_5 = 2.39 \qquad c_6 = 1.09 \qquad c_{12} = 277579$$

$$c_{14} = 1.54 \times 10^9 \qquad c_{15} = 7.976 \qquad \hat{X}_3 = 2$$

The Baker bound was $B_0 = 2.32 \cdot 10^{92}$. After the first reduction step with $\kappa = 10$ we obtained $B_0 = 29$. After the second reduction step with $\kappa = 100$ we obtained $B_0 = 4$.

The entries of the matrix (19) were computed with error at most 2×10^{-202}. The entries of the inverse matrix A were found with error at most 5×10^{-200}. This gave us δ with precision 2×10^{-199}. Since we used $\kappa \leqslant 100$, our computations were correct.

After the final enumeration step we obtained four solutions $(1, -1)$, $(-1, 1)$, $(0, 1)$, $(0, -1)$ for the equation $y^{19} + 2x^{19} = \pm 1$ and two solutions $(1, 0)$, $(-1, 0)$ for the equation $y^{19} + 2x^{19} = \pm 2$.

The total computational time was 11.7 s.

3.3. *The Real Cyclotomic Equation*

Let $n > 12$ and P the largest prime divisor of $n/(n, 3)$ (that is P is the largest prime divisor of n unless $n = 2^l \cdot 3$, in which case $P = 2$). The Diophantine equations

$$F_n(x, y) = \prod_{\substack{(k, n) = 1 \\ 1 \leqslant k \leqslant n/2}} \left(y - x \cdot 2 \cos \frac{2\pi k}{n} \right) = \pm 1, \pm P \tag{53}$$

occurs in study of certain linear recurrences [Vo95]. P. Voutier [ibid] solved (53) for all $n \leqslant 29$, but he used certain specific features of these equations.

In this subsection we illustrate our general method by solving completely the equations (53) for $n = 67$. In this case $P = 67$ and

$$\begin{aligned} F_{67}(x, y) &= \prod_{1 \leqslant k \leqslant 33} \left(y - x \cdot 2 \cos \frac{2\pi k}{67} \right) \\ &= y^{33} + y^{32}x - 32y^{31}x^2 - 31y^{30}x^3 + 465y^{29}x^4 \\ &\quad + 435y^{28}x^5 - 4060y^{27}x^6 \\ &\quad - 3654y^{26}x^7 + 23751y^{25}x^8 + 20475y^{24}x^9 \\ &\quad - 98280y^{23}x^{10} - 80730y^{22}x^{11} \\ &\quad + 296010y^{21}x^{12} + 230230y^{20}x^{13} \\ &\quad - 657800y^{19}x^{14} - 480700y^{18}x^{15} \\ &\quad + 1081575y^{17}x^{16} + 735471y^{16}x^{17} \\ &\quad - 1307504y^{15}x^{18} - 817190y^{14}x^{19} \\ &\quad + 1144066y^{13}x^{20} + 646646y^{12}x^{21} \\ &\quad - 705432y^{11}x^{22} - 352716y^{10}x^{23} \\ &\quad + 293930y^9x^{24} + 125970y^8x^{25} - 77520y^7x^{26} - 27132y^6x^{27} \\ &\quad + 11628y^5x^{28} + 3060y^4x^{29} - 816y^6x^{30} \\ &\quad - 136y^2x^{31} + 17yx^{32} + x^{33}. \end{aligned}$$

PROPOSITION 3.3.1. *Let p be an odd prime.*

1. *The $(p-3)/2$ numbers*

$$\frac{\sin(k\pi/p)}{\sin(\pi/p)}, \qquad k = 2, ..., \frac{p-1}{2}, \tag{54}$$

are independent units of the field $\mathbf{K}=\mathbf{Q}(\cos(2\pi/p))$. *If* $p\leqslant 67$ *then* (54) *is a system of fundamental units.*

2. *Let* $\alpha=2\cos(2\pi/p)$. *Then the one-element set* $\mathrm{M}=\{2-\alpha\}$ *is a complete system of non-associate solutions of* $N_{\mathbf{K}/\mathbf{Q}}(\beta)=p$ *in the ideal* $I=(1,\alpha)=(1)$.

Proof. 1. It is a classical fact [BS66, Ch. V, Section 5, Th. 2] that the numbers in (54) are independent units which generate a subgroup of index $h(\mathbf{K})$ in the group of all positive units of the field $\mathbf{K}$. On the other hand, for $p\leqslant 67$ the class number $h(\mathbf{K})$ is 1 [Ma78]. This proves the first assertion.

2. Put $\mathbf{L}=\mathbf{Q}(\xi)$ where $\xi=\exp(2\pi i/p)$. Then the prime decomposition of p in $\mathbf{L}$ is $p=\mathscr{P}^{p-1}$, where $\mathscr{P}=(1-\xi)$ [BS66, Ch. III, Section 1, L. 1]. Therefore the prime decomposition of p in $\mathbf{K}$ is $p=\wp^{(p-1)/2}$, where $\wp=N_{\mathbf{L}/\mathbf{K}}\mathscr{P}=(2-\alpha)$. It remains to note that any $\beta\in I$ satisfying $N_{\mathbf{K}/\mathbf{Q}}(\beta)=p$ generates the ideal $\wp$.

The (worst) values of the main constants are:

$$c_1=1.33\times 10^{10} \qquad c_2=0.017 \qquad c_3=8.31\times 10^{11}$$

$$c_5=3.76 \qquad c_6=2.11 \qquad c_{12}=7.86\times 10^{12}$$

$$c_{14}=8.18\times 10^{20} \qquad c_{15}=10.0 \qquad \hat{X}_3=2.55$$

Baker's bound $B_0\leqslant 1.26\times 10^{204}$. After the first reduction step we obtained $B_0\leqslant 59$. After the second step we obtained $B_0\leqslant 6$.

The entries of the matrix (19) were computed with error at most 6×10^{-492}. The entries of the matrix $A=A^{(1)}$ were found with error at most 4×10^{-488}. Using (48), we found the matrices $A^{(2)},\ldots,A^{(32)}$ with precision 2×10^{-439}. This gave us $\delta^{(1)},\ldots,\delta^{(32)}$ with precision 3×10^{-438}. Since we used $\kappa\leqslant 1000$, our computations were correct.

The total computational time for this example was 28 minutes and 22 seconds. We found that all solutions of the equation $F_{67}(x,y)=1$ are

$$(0,1),\qquad (1,0),\qquad (-1,-1),\qquad (1,-1),\qquad (-1,2),$$

and the single solution of the equation $F_{67}(x,y)=67$ is $(1,2)$. (The solutions for $F_{67}(x,y)=-1,\ -67$ are the negations of those listed above.)

Combining Lemma 1 from [Vo95, Sect. 2] with our computations, we prove that the 67th term of any Lucas or Lehmer sequence has a primitive divisor. We refer to [Vo95] for definitions and further information.

ACKNOWLEDGMENTS

We thank H. Cohen, J.-M. Deshouillers, M. Olivier, N. Smart, N. Tzanakis, and K. Wildanger for valuable discussions and suggestions. We are especially indebted to Benne de Weger, Fernando Rodriguez Villegas, and the referee for their helpful comments.

The research of the first named author was supported by the *Bourse Chateaubriand du Gouvernement Français* and *the Sondernforschungsbereich* 170 "*Geometrie und Analysis*." He thanks the laboratory "Mathématiques Stochastiques" in Bordeaux and SFB 170 in Göttingen for their hospitality during the preparation of this article.

REFERENCES

[Ba66] A. Baker, Linear forms in the logarithms of algebraic numbers, I, *Mathematica* **13** (1966), 204–216; II, *Mathematica* **14** (1967), 102–107; III, *Mathematica* **14** (1967), 220–228; IV, *Mathematica* **15** (1968), 204–216.

[Ba68] A. Baker, Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms, *Philos. Trans. R. Soc. London Ser. A* **263** (1968), 173–191.

[BD69] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford (2)* **20** (1969), 129–137.

[BW93] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

[BBCO94] C. Batut, D. Bernardi, H. Cohen, and M. Olivier, "User's Guide to PARI/GP version 1.39.00," available by anonymous ftp from megrez.ceremab.u-bordeaux.fr.

[Bi94] Yu. Bilu, Solving superelliptic Diophantine equations by the method of Gelfond–Baker, Preprint 94-09, Mathématiques Stochastiques, Univ. Bordeaux 2, 1994.

[BS66] Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.

[Co93] H. Cohen, "A Course in Computational Algebraic Number Theory," Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, Berlin/New York, 1993.

[Ge52] A. O. Gelfond, "Transcendent and Algebraic Numbers," Moscow, 1952 [Russian]; English trans., Dover, New York, 1960.

[Ma78] J. M. Masley, Class numbers of real cyclic number fields with small conductor, *Compositio Math.* **37** (1978), 297–319.

[MW94] M. Mignotte and B. M. M. de Weger, On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 76 = y^5$, *Glasgow Math. J.*, to appear.

[Pe90] A. Pethö, Computational methods for the resolution of Diophantine equations, *in* "Number Theory: Proc. First Conf. Can. Number Th. Ass., Banff, 1988" (R. A. Mollin, Ed.), pp. 477–492, de Gruyter, 1990.

[PW87] A. Pethö and B. M. M. de Weger, Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan–Nagell Equation, *Math. Comp.* **47** (1987), 713–727.

[Po93] M. E. Pohst, "Computational Algebraic Number Theory," DMV Seminar, Vol. 21, Birkhäuser, Basel, 1993.

[PZ89] M. E. Pohst and H. Zassenhaus, "Algorithmic Algebraic Number Theory," Cambridge Univ. Press, London/New York, 1989.

[ShT86] T. N. Shorey and R. Tijdeman, "Exponential Diophantine Equations," Cambridge Univ. Press, Cambridge, 1986.

[Sm95] N. Smart, The solution of triangularly connected decomposable form equation, *Math. Comp.* **64** (1995), 819–840.

[Sp82] V. G. Sprindžuk, "Classical Diophantine Equations in Two Unknowns," Nauka, Moscow, 1982 [Russian]; English transl., Lecture Notes in Mathematics, Vol. 1559, Springer-Verlag, Berlin/New York, 1994.

[Th09] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284–305.

[TW89] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.

[TW92] N. Tzanakis and B. M. M. de Weger, How to explicitly solve a Thue–Mahler equation, *Compositio Math.* **84** (1992), 223–288.

[Vo95] P. M. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.* **64** (1995), 869–888.

[We87] B. M. M. de Weger, Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Theory* **26** (1987), 325–367.

[We92] B. M. M. de Weger, A hyperelliptic diophantine equation related to imaginary quadratic number fields with class number 2, *J. Reine Angew. Math.* **427** (1992), 137–156.