Ramanujan J (2017) 42:145–156
DOI 10.1007/s11139-015-9749-x

Thue equations and CM-fields

Yves Aubry[1] · **Dimitrios Poulakis**[2]

Received: 10 February 2015 / Accepted: 4 November 2015 / Published online: 20 January 2016

Abstract We obtain a polynomial-type upper bounds for the size and the number of the integral solutions of Thue equations $F(X, Y) = b$ defined over a totally real number field K, assuming that $F(X, 1)$ has a root α such that $K(\alpha)$ is a CM-field. Furthermore, we give an algorithm for the computation of the integral solutions of such an equation.

Keywords Thue equations · Integral solutions · CM-fields

Mathematics Subject Classification 11D59 · 11Y16 · 11G30 · 11G50

1 Introduction

Let $F(X, Y)$ be an irreducible binary form in $\mathbb{Z}[X, Y]$ with $\deg F \geq 3$ and $b \in \mathbb{Z} \setminus \{0\}$. In 1909, Thue [26] proved that the equation $F(X, Y) = b$ has only finitely many solutions $(x, y) \in \mathbb{Z}^2$. Thue's proof was ineffective and therefore does not provide a method to determine the integer solutions of this equation. Other non-effective proofs of Thue's result can be found in [7, Chap. X] and [20, Chap. 23].

In 1968, Baker [2], using his results on linear forms in logarithms of algebraic numbers, computed an explicit upper bound for the size of the integer solutions of Thue equations. Baker's results were improved by several authors (see for instance

✉ Dimitrios Poulakis
poulakis@math.auth.gr

Yves Aubry
yves.aubry@univ-tln.fr

1 Institut de Mathématiques de Toulon, Université de Toulon, France and Insitut de Mathématiques de Marseille, CNRS-UMR 7373, Aix-Marseille Université, Marseille, France

2 Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

[6,12,22]) but the bounds remain to be of exponential type and are thus not useful to compute integer solutions of such equations. Nevertheless, computation techniques for the resolution of Thue equations have been developed based on the above results [1,13,21,27], and the solutions of certain parameterized families of Thue equations have been obtained [14]. Furthermore, upper bounds for the number of integral solutions of Thue equations have been given [4,5,9].

In the case where all roots of the polynomial $F(X, 1)$ are non-real, we have a polynomial-type bound provided by other methods [20, Theorem 2, p. 186], [11,23]. Győry's improvement in [11, Théorème 1] holds in the case where the splitting field of $F(X, 1)$ is a CM-field, i.e., a totally imaginary quadratic extension of a totally real number field. More precisely, Győry proved the following theorem:

Theorem 1 *Let $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$ be the product of irreducible forms $G_1(X, Y), \ldots, G_l(X, Y)$ with integer coefficients such that the splitting field of $G_i(X, 1)$ is a CM-field $(i = 1, \ldots, l)$. Let m be a non-zero integer. Then, the solutions $(x, y) \in \mathbb{Z}^2$ to the equation $F(X, Y) = m$ satisfy*

$$|x| \leq 2|a_n|^{1-\frac{2l-1}{n}}|m|^{\frac{1}{n}}, \quad |y| \leq 2|a_0|^{1-\frac{2l-1}{n}}|m|^{\frac{1}{n}}.$$

If $G(X, Y)$ is a non-trivial irreducible factor of $F(X, Y)$ over $\mathbb{Z}$ such that the splitting field of $G(X, 1)$ is of CM-type, then each integer solution (x, y) of $F(X, Y) = b$ satisfies $G(x, y) = b_1$ for some divisor b_1 of b, and therefore Theorem 1 applies to this equation and gives the following result:

Corollary 1 *Suppose that $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$ is a form with integer coefficients having an irreducible factor $G(X, Y)$ over $\mathbb{Z}$ such that the splitting field of $G(X, 1)$ is a CM-field. Let m be a non-zero integer. Then, the solutions $(x, y) \in \mathbb{Z}^2$ to the equation $F(X, Y) = m$ satisfy*

$$|x| \leq 2|a_n|^{1-\frac{1}{n}}|m|^{\frac{1}{2}}, \quad |y| \leq 2|a_0|^{1-\frac{1}{n}}|m|^{\frac{1}{2}}.$$

In the same paper, Győry studied Thue equations defined over a CM-field L and also gave ([11, Théorème 2]) a polynomial upper bound for the size of their real algebraic integers' solutions in L. This result, as we shall see in the next section, implies a result similar to Corollary 1 but with a bound of exponential type.

In this paper, we consider Thue equations $F(X, Y) = b$ defined over a totally real number field K. Simplifying Győry's approach, we obtain (Theorem 2) polynomial-type bounds for the size and the number of their integral solutions over K, assuming that $F(X, 1)$ has a root α such that the field $K(\alpha)$ is a CM-field. In case where the splitting field is a CM-field, we are in the situation of [11, Théorème 2]. Whenever all roots of the polynomial $F(X, 1)$ are non-real and $K \neq \mathbb{Q}$, we obtain much better bounds than those already known [23]. Moreover, whenever $F(X, 1)$ has a real and a non-real root, we obtain polynomial-type bounds that the Baker's method was not able to provide other than exponential bounds. Furthermore, the method of the proof of Theorem 2 provides us with an algorithm for the determination of the solutions of such equations.

We illustrate our result by giving two examples of infinite families of Thue equations $F(X, Y) = b$ satisfying the hypothesis of Theorem 2: First we consider Thue equations over some totally real subfields K of cyclotomic fields N such that the splitting field L of $F(X, 1)$ over K is contained in N. In this case, L is an abelian extension of K. Next, we give a family of equations $F(X, Y) = b$ such that $F(X, 1)$ has a root α for which $K(\alpha)$ is a biquadratic CM-field. These families contain equations such that $F(X, 1)$ has also real roots, and therefore the only method for having upper bound for the size of their solutions is the Baker's method which provides only bounds of exponential type. Finally, we give two examples of determination of solutions of equations satisfying the hypothesis of Theorem 2, using our algorithm.

2 New bounds

We introduce a few notations. Let K be a number field. We consider the set of absolute values of K by extending the ordinary absolute value $|\cdot|$ of $\mathbb{Q}$ and, for every prime p, by extending the p-adic absolute value $|\cdot|_p$ with $|p|_p = p^{-1}$. Let $M(K)$ be an indexing set of symbols v such that $|\cdot|_v$, $v \in M(K)$, are all of the above absolute values of K. Given such an absolute value $|\cdot|_v$ on K, we denote by d_v its local degree. Let $\mathbf{x} = (x_0 : \ldots : x_n)$ be a point of the projective space $\mathbb{P}^n(K)$ over K. We define the field height $H_K(\mathbf{x})$ of $\mathbf{x}$ by

$$H_K(\mathbf{x}) = \prod_{v \in M(K)} \max\{|x_0|_v, \ldots, |x_n|_v\}^{d_v}.$$

Let d be the degree of K. We define the absolute height $H(\mathbf{x})$ by $H(\mathbf{x}) = H_K(\mathbf{x})^{1/d}$. For $x \in K$, we put $H_K(x) = H_K((1 : x))$ and $H(x) = H((1 : x))$. If $G \in K[X_1, \ldots, X_m]$, then we define $H_K(G)$ and $H(G)$ of G as the field height and the absolute height, respectively, of the point whose coordinates are the coefficients of G (in any order). For an account of the properties of heights, see [15,16,25]. Furthermore, we denote by O_K and N_K the ring of integers of K and the norm relative to the extension $K/\mathbb{Q}$, respectively. Finally, for every $z \in \mathbb{C}$, we denote, usually, by $\bar{z}$ its complex conjugate.

We prove the following theorem:

Theorem 2 *Let K be a totally real number field of degree d. Let $b \in O_K \setminus \{0\}$ and $F(X, Y) \in O_K[X, Y]$ be a form of degree $n \geq 2$. Suppose that $F(X, 1)$ has a root α such that $K(\alpha)$ is a CM-field. Then the solutions $(x, y) \in O_K^2$ of $F(X, Y) = b$ satisfy*

$$H(x) < \Omega_1 \quad \text{and} \quad H(y) < \Omega_2$$

for the following values of Ω_1 and Ω_2. If the coefficients of X^n and Y^n are ± 1, then

$$\Omega_1 = \Omega_2 = 32 H(b)^{1/n} H(F)^{1+1/n} N_K(b)^{2/d}.$$

If only the coefficient of X^n is ± 1, then

$$\Omega_1 = 2^9 H(b)^{1/n} H(F)^{2+1/n} N_K(b)^{4/d} \text{ and } \Omega_2 = 32 H(b)^{1/n} H(F)^{1+1/n} N_K(b)^{2/d}.$$

If both the coefficients of X^n and Y^n are $\neq \pm 1$, then

$$\Omega_1 = 2^9 H(b)^{1/n} H(\Gamma)^{2n+1} N_K(b)^{4/d} H(a_0) N_K(a_0)^{4(n-1)/d}$$

and

$$\Omega_2 = 32 H(b)^{1/n} H(\Gamma)^{n+1} N_K(b)^{2/d} H(a_0) N_K(a_0)^{2(n-1)/d},$$

where a_0 is the coefficient of X^n and Γ a point of the projective space with 1 and the coefficients of $F(X, Y)$ as coordinates. Furthermore, the number of integral solutions over K to the equation $F(X, Y) = b$ is at most

$$72 \cdot 4^{dn} N_K(b)^{2n}.$$

In case where b is a unit of O_K, this number is at most $2wn$, where w is the number of the roots of unity in $K(\alpha)$.

The proof of this result is relied on the following property of CM-fields. A non-real algebraic number field L is a CM-field if and only if L is closed under the operation of complex conjugation and complex conjugation commutes with all the $\mathbb{Q}$-monomorphisms of L into $\mathbb{C}$ ([3], [10, Théorème 1], [17, Lemma 2]).

When $K = \mathbb{Q}$ and the splitting field of $F(X, 1)$ over $\mathbb{Q}$ is an abelian totally imaginary extension, the hypothesis on complex conjugation is obviously satisfied. If the coefficient of X^n is ± 1, it is interesting to notice that our bounds are essentially independent of the degree of the form $F(X, Y)$. Thus, in case where $H(F)$ and $H(b)$ are not too large, an exhaustive search can provide the integer solutions we are looking for.

Finally, it should be noticed that in case $K = \mathbb{Q}$, Corollary 1 provides a better upper bound than Theorem 2. Furthermore, if $F(X, Y)$ is irreducible and $K \neq \mathbb{Q}$, then [11, Théorème 2] gives upper bounds similar to Theorem 2. Suppose $K \neq \mathbb{Q}$ and $F_1(X, Y)$ is a non-trivial irreducible factor of $F(X, Y)$ over O_K of degree ν such that the splitting field of $F_1(X, 1)$ is of CM-type. Then each solution $(x, y) \in O_K^2$ of $F(X, Y) = b$ satisfies $F_1(x, y) = b_1$ for some divisor b_1 of b. Note that we do not know the height of b_1. For this we use [12, Lemma 3] which yields a unit $\epsilon \in O_k$ having

$$H(b_1 \epsilon^\nu) \leq N_K(b_1)^{1/d} \exp\{c \nu R_K\},$$

where c is an explicit constant and R_K the regulator of K. Thus, we have $F_1(\epsilon x, \epsilon y) = b_1 \epsilon^\nu$ and therefore, using [11, Théorème 2], we obtain upper bounds for $H(x)$ and $H(y)$ with an extra factor which is exponential in respect of R_K and hence it is clearly worse than that of Theorem 2.

3 Examples

In this section, we give two examples in order to illustrate our result. We denote by $F^*(X, Y)$ the homogenization of a polynomial $F(X) \in \mathbb{C}[X]$.

Example 1 Let p be a prime with $p \equiv 1 \pmod 4$ and ζ_p a pth primitive root of unity in $\mathbb{C}$. Then the quadratic field $\mathbb{Q}(\sqrt{p})$ is a subfield of $\mathbb{Q}(\zeta_p)$. The field $\mathbb{Q}(\zeta_p)$ is a cyclic extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$.

Let $\alpha \in \mathbb{Z}[\zeta_p]$ be a primitive element of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p})$ and $\alpha_1, \dots, \alpha_m$, with $m = (p-1)/2$, all the distinct conjugates of α over $\mathbb{Q}(\sqrt{p})$. The largest real field contained in $\mathbb{Q}(\zeta_p)$ is $K_p = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ which is a totally real number field. Let $\beta \in K_p$ be a primitive element of the extension $K_p/\mathbb{Q}(\sqrt{p})$ and $\beta_1, \dots, \beta_n$, where $n = (p-1)/4$, all the distinct conjugates of β over $\mathbb{Q}(\sqrt{p})$. Then the polynomial

$$F(X) = (X - \alpha_1) \cdots (X - \alpha_m)(X - \beta_1) \cdots (X - \beta_n)$$

belongs to $\mathbb{Q}(\sqrt{p})[X]$ and has real and non-real roots. Furthermore, we have $\mathbb{Q}(\sqrt{p})(a_i) = \mathbb{Q}(\zeta_p)$ which is a CM-field. Consequently, for every non-zero $b \in \mathbb{Z}[(1+\sqrt{p})/2]$, the Thue equation $F^*(X, Y) = b$ satisfies the hypothesis of Theorem 2. Note that this equation satisfies also the hypothesis of [11, Théorème 2].

Then, using [25, Theorem 5.9, p. 211] and [25, Lemma 5.10, p. 213], Theorem 2 gives the following upper bound for the heights of solutions $x, y \in \mathbb{Z}[(1+\sqrt{p})/2]$:

$$H(x) < 2^{(3p+17)/4}(H(\alpha)^2 H(\beta))^{(3p+1)/6} H(b)^{4/3(p-1)} N_{\mathbb{Q}(\sqrt{p})}(b)$$

and

$$H(y) < 2^{(3p+13)/2}(H(\alpha)^2 H(\beta))^{5(p-1)/6} H(b)^{4/3(p-1)} N_{\mathbb{Q}(\sqrt{p})}(b)^2.$$

If we consider the particular case where $\Phi_p(X)$ is the p-th cyclotomic polynomial, then [11, Section 2] implies that the maximum of the absolute heights of all algebraic integers $x, y \in K_p$ with $\Phi_p^*(x, y) = 1$ is $< 2^{(p-1)/2}$. Theorem 2 improves this result by yielding the bound 32.

Example 2 Let d be a positive integer ≥ 2 and $r = m + n\sqrt{d}$, where m, n are integers such that $m > 0$ and $m^2 - n^2 d > 0$. The minimal polynomial of r over $\mathbb{Q}$ is

$$M(X) = X^2 - 2mX + m^2 - dn^2.$$

Then, the polynomial

$$P(X) = M(-X^2) = X^4 + 2mX^2 + m^2 - dn^2$$

is the minimal polynomial of $\sqrt{-r}$ over $\mathbb{Q}$. Since $m > 0$ and $m^2 - n^2 d > 0$, their roots are not real and so $\mathbb{Q}(\sqrt{d}, \sqrt{-r})$ is a CM-field. If $Q(X) \in \mathbb{Z}[\sqrt{d}][X] \setminus \mathbb{Z}$, then we set

$$F(X) = (X^2 + (m + n\sqrt{d})Y^2)Q(X).$$

So, for every non-zero $b \in \mathbb{Z}[\sqrt{d}]$, the Thue equation $F^*(X, Y) = b$ over $K = \mathbb{Q}(\sqrt{d})$ satisfies the hypothesis of Theorem 2. Suppose that $Q(X)$ is monic and $\deg Q = q > 0$. By [15, Remark B.7.4], we have

$$H(F) \leq 4H(m + n\sqrt{d})H(Q).$$

Thus, Theorem 2 yields the following upper bounds for the height of integral solutions of the above equations over K:

$$H(x) < 2^{13+1/q} H(b)^{1/2q} (H(m + n\sqrt{d})H(Q))^{2+1/q} N_K(b)^2,$$
$$H(y) < 2^{7+1/q} H(b)^{1/2q} (H(m + n\sqrt{d})H(Q))^{1+1/q} N_K(b).$$

Note that in case where the splitting field of $F(X)$ is not a CM-field, [11, Théorème 2] cannot be applied. Furthermore, Baker's method can provide only bounds of exponential type.

4 Proof of Theorem 2

Write

$$F(X, Y) = a_0(X - \alpha_1 Y) \cdots (X - \alpha_n Y).$$

First, we consider the case where $a_0 = \pm 1$. If $a_0 = -1$, we replace $F(X, Y)$ by $-F(X, Y)$ and b by $-b$ and then we may suppose that $a_0 = 1$. By our hypothesis, there is j such that $K_j = K(\alpha_j)$ is a CM-field.

Let $x, y \in O_K$ such that $xy \neq 0$ and $F(x, y) = b$. We set $b_j := x - \alpha_j y$. Since K is a totally real number field, we have $x - \bar{\alpha}_j y = \bar{b}_j$. Setting $\rho_j = \bar{b}_j / b_j$, we obtain the system

$$x - \alpha_j y = b_j, \quad x - \bar{\alpha}_j y = \rho_j b_j.$$

Eliminating b_j from the above two equations, we get $x = Ay$ where we have set

$$A = \frac{\bar{\alpha}_j - \alpha_j \rho_j}{1 - \rho_j}.$$

We have

$$H(A) \leq H(\bar{\alpha}_j - \alpha_j \rho_j) H(1 - \rho_j) \leq 4H(\alpha_j)^2 H(\rho_j)^2.$$

Since α_j is not real, using [18], we deduce $H(\alpha_j) < 2H(F)^{1/2}$. It follows that

$$H(A) \leq 16H(F)H(\rho_j)^2.$$

Substituting in the equation $F(x, y) = b$, we deduce that

$$y^n F(A, 1) = b,$$

and thus

$$H(y)^n \leq H(F(A, 1))H(b) \leq (n+1)H(F)H(A)^n H(b).$$

Using the bound for $H(A)$, we obtain

$$H(y)^n \leq (n+1)16^n H(b)H(F)^{n+1}H(\rho_j)^{2n}. \tag{1}$$

Next, we shall compute a bound for the height of ρ_j. We denote by G_j the set of $\mathbb{Q}$-embeddings $\sigma : K_j \to \mathbb{C}$. Since K_j is a CM-field, [10, Théorème 1] yields that the complex conjugation commutes with all the elements of G_j. Further, K_j is closed under the operation of complex conjugation whence we get $\bar{\alpha}_j \in K_j$ and so $\bar{b}_j \in K_j$. Thus, for every $\sigma \in G_j$, we have $\sigma(\bar{b}_j) = \overline{\sigma(b_j)}$. It follows that

$$|\sigma(\rho_j)| = \frac{|\sigma(\bar{b}_j)|}{|\sigma(b_j)|} = \frac{|\overline{\sigma(b_j)}|}{|\sigma(b_j)|} = 1.$$

Let $I_j(X)$ be the minimal polynomial of ρ_j over $\mathbb{Q}$ and $C_j(X)$ be the characteristic polynomial of ρ_j relative to the extension $K_j/\mathbb{Q}$. Then, we have

$$C_j(X) = I_j(X)^{[K_j:\mathbb{Q}(\rho_j)]}.$$

The elements $\alpha_j, \bar{\alpha}_j$ are algebraic integers of K_j and so $b_j, \bar{b}_j$ are algebraic integers of K_j. It follows that the polynomial

$$\Pi_j(X) = \prod_{\sigma \in G_j} \sigma(b_j)(X - \sigma(\rho_j)) = \prod_{\sigma \in G_j} \sigma(b_j) C_j(X) = N_{K_j}(b_j) I_j(X)^{[K_j:\mathbb{Q}(\rho_j)]}$$

has integer coefficients. We denote by m_j the least common multiple of the denominators of the coefficients of $I_j(X)$. Then, we deduce that

$$m_j^{[K_j:\mathbb{Q}(\rho_j)]} \big| N_{K_j}(b_j).$$

Since $N_{K_j}(b_j) | N_{K_j}(b)$, we get

$$m_j^{[K_j:\mathbb{Q}(\rho_j)]} \big| N_{K_j}(b).$$

As we saw above, all the conjugates $\rho_{j1}, \ldots, \rho_{j\mu}$ ($\mu \leq dn$), of ρ_j are of absolute value 1. By [16, p. 54], we have

$$H(\rho_j) = \left(m_j \prod_{i=1}^{\mu} \max\{1, |\rho_{ji}|\right)^{1/[\mathbb{Q}(\rho_j):\mathbb{Q}]} = m_j^{1/[\mathbb{Q}(\rho_j):\mathbb{Q}]}.$$

Thus, we deduce

$$H_{K_j}(\rho_j) \big| N_{K_j}(b) \tag{2}$$

whence

$$H(\rho_j) \leq N_K(b)^{1/d}. \tag{3}$$

Combining the inequalities (1) and (3), we get

$$H(y) \leq 32 H(b)^{1/n} H(F)^{1+1/n} N_K(b)^{2/d}.$$

We have

$$H(x) \leq H(A)H(y) \leq 16 H(F) H(\rho_j)^2 H(y)$$

whence we obtain

$$H(x) \leq 2^9 H(b)^{1/n} H(F)^{2+1/n} N_K(b)^{4/d}.$$

Suppose now that $a_0 \neq \pm 1$. Write $F(X, 1) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$. Then $a_0\alpha_i$ is a root of $f(X) = X^n + a_1 X^{n-1} + a_2 a_0 X^{n-2} + \cdots + a_n a_0^{n-1}$ and thus $a_0\alpha_i$ is an algebraic integer. Denote by $F_1(X, Y)$ the homogenization of $f(X)$. If $(x, y) \in O_K^2$ is a solution to $F(X, Y) = b$, then $(a_0 x, y)$ is a solution to $F_1(X, Y) = b a_0^{n-1}$. Denote by Γ a point in the projective space with 1 and the coefficients of F as coordinates. Then we have $H(F_1) \leq H(\Gamma)^n$, and finally we obtain

$$H(y) \leq 32 H(b)^{1/n} H(\Gamma)^{n+1} N_K(b)^{2/d} H(a_0) N_K(a_0)^{2(n-1)/d}$$

and

$$H(x) \leq 2^9 H(b)^{1/n} H(\Gamma)^{2n+1} N_K(b)^{4/d} H(a_0) N_K(a_0)^{4(n-1)/d}.$$

Now suppose that b is a unit in O_K. Then inequality (2) implies that $H(\rho_j) = 1$ and so Kronecker's theorem yields that ρ_j is a root of unity. Let w be the number of the roots of unity in K_j. Then we have w choices for A (for the roots of unity $\neq \pm 1$) and, since y is real, the equation $y^n F(A, 1) = b$ gives us at most $2w$ choices for y. Considering also the solutions of the equation with $xy = 0$, we deduce that the number of integral solutions to the equation $F(X, Y) = b$ is at most $2wn$. Finally, suppose that b is not a unit in O_K. Using [24, Lemma 8B], we obtain that the number of elements $\rho_j \in K_j$ with $H(\rho_j) \leq N_K(b)^{1/d}$ is bounded by

$$36 \cdot 4^{dn} N_K(b)^{2n}$$

and so the result follows.

5 An algorithm

In this section, we give an algorithm for the computation of the integral solutions to $F(X, Y) = b$ based on the proof of Theorem 2.

SOLVE-THUE-1

Input: A totally real number field K, a form $F(X, Y) \in O_K[X, Y]$ with $F(X, 1)$ monic, $b \in O_K \setminus \{0\}$ and α a root of $F(X, 1)$ such that $K(\alpha)$ is a CM-field.

Output: The integral solutions of $F(X, Y) = b$ over K.

(1) Compute the set Λ of all the elements $\rho \in K(\alpha) \setminus K$ having the absolute values of all their conjugates equal to 1 and $H_{K(\alpha)}(\rho) | N_{K(\alpha)}(b)$. If b is a unit of O_K, then the set Λ consists of all the roots of unity of $K(\alpha)$ which does not belong to K.

(2) Compute the set Ξ of elements ξ of K of the form

$$\xi = \frac{\bar{\alpha} - \alpha\rho}{1 - \rho},$$

where $\rho \in \Lambda$.

(3) Compute the set S of elements $y \in O_K$ such that there is $\xi \in \Xi \cup \{(\bar{\alpha} + \alpha)/2\}$ with

$$y^n F(\xi, 1) = b.$$

(4) Output the solutions $(x, y) \in O_K^2$ to $F(X, Y) = b$ with $y \in S$ and the solutions $(x, y) \in O_K^2$ with $xy = 0$.

Proof of Correctness. Let $(x, y) \in O_K^2$ be a solution to $F(X, Y) = b$ with $xy \neq 0$. We set $x - \alpha y = \beta$ and $\rho = \bar{\beta}/\beta$. From the proof of Theorem 2, we have $x = yA$, where

$$A = \frac{\bar{\alpha} - \alpha\rho}{1 - \rho},$$

and so $y^n F(A, 1) = b$. Since $x, y \in K$, we get $A \in K$. Furthermore, by (2) we have that $H_{K(\alpha)}(\rho)$ divides $N_{K(\alpha)}(b)$. Moreover, we have seen that either $\rho \notin K$ or $\rho = -1$ (and in this case $A = (\bar{\alpha} + \alpha)/2$). Finally, if b is a unit, then we have that $H(\rho) = 1$ and so ρ is a root of unity in $K(\alpha)$.

Note that there are algorithms for the computation of the elements of a number field of bounded height [8] and for the computation of roots of unity in a number field [19, Annexe C]. As far as we know, there are no implementations for such algorithms. The other computations can be carried out by a computational system such as MAGMA or MAPLE.

Remark 1 By [16, p. 54], the leading coefficient m of the minimal polynomial of ρ is equal to $H_{K(\alpha)}(\rho)$. Thus, $m\rho \in O_K$.

Finally, we give two examples of Thue equations that satisfy the hypothesis of Theorem 2 for which we use the previous algorithm to determine all the integral solutions, the first one having a right-hand side a unit but not the second one.

Example 3 The only solutions of the equation

$$(X^2 + Y^2)(X^2 - \sqrt{2}XY + Y^2) = 1$$

over $\mathbb{Z}[\sqrt{2}]$ are $(X, Y) = (\pm 1, 0), (0, \pm 1)$.

Proof The complex number i is a root of $X^2 + 1$ and $K = \mathbb{Q}(\sqrt{2}, i)$ is a CM-field. The roots of unity lying in $K \setminus \mathbb{Q}(\sqrt{2})$ are $\pm i$. Next, we compute

$$\xi_{\pm} = \frac{-i - i(\pm i)}{1 - (\pm i)} = \pm 1.$$

Thus, we have the equations $y^4 2(2 \pm \sqrt{2}) = 1$. If there is $y \in \mathbb{Z}[\sqrt{2}]$ satisfying one of these equations, then 2 is a unit in $\mathbb{Z}[\sqrt{2}]$, which is a contradiction since its norm is not equal to ± 1. Furthermore, the solutions $(x, y) \in O_K^2$ with $xy = 0$ are $(\pm 1, 0)$ and $(0, \pm 1)$.

Example 4 Consider the form

$$F(X, Y) = (X^2 + (3 - 2\sqrt{2})Y^2)(X^2 - 4XY + \sqrt{2}Y^2) \in \mathbb{Z}[\sqrt{2}][X, Y].$$

Then the only solutions of the equation $F(X, Y) = 3\sqrt{2} - 4$ over $\mathbb{Z}[\sqrt{2}]$ are $(X, Y) = (0, \pm 1)$.

Proof The given equation belongs to the family of equations of Example 2. Thus, we shall use the above algorithm for the determination of their solutions. First, we remark that the equation $F(X, 0) = 3\sqrt{2} - 4$ has no solution over $\mathbb{Z}[\sqrt{2}]$ and the only solutions of $F(0, Y) = 3\sqrt{2} - 4$ over $\mathbb{Z}[\sqrt{2}]$ are $Y = \pm 1$.

Set $y = i\sqrt{3 - 2\sqrt{2}}$ and $K = \mathbb{Q}(y)$. We have $N_K(6 - 4\sqrt{2}) = 16$. We shall compute all the elements $\rho \in K \setminus \mathbb{Q}(\sqrt{2})$ with $H_K(\rho) | 16$ and having all the absolute values of their conjugates equal to 1.

If $H_K(\rho) = 1$, then ρ is a root of unity in $K \setminus \mathbb{Q}(\sqrt{2})$. Since there are no roots of unity in K other than ± 1, we consider the case where $H_K(\rho) > 1$. Let $H_K(\rho) = 2^{\epsilon}$, where $\epsilon = 1, 2$. By Remark 1, we have $\rho = \alpha / 2^{\epsilon}$, where $\alpha \in O_K$. Using MAGMA, we get the following integral base for K:

$$\omega_0 = 1, \quad \omega_1 = y, \quad \omega_2 = \frac{1}{2}(y^2 - 1), \quad \omega_3 = \frac{1}{4}(y^3 + y^2 - y - 1).$$

Since all the conjugates of ρ have absolute value 1, we obtain the two equalities:

$$((a_0 - 2a_1) + a_1\sqrt{2})^2 + (2 - \sqrt{2})((a_2 - 2a_3) + a_3\sqrt{2})^2 = 2^{2\epsilon},$$

and

$$((a_0 - 2a_1) - a_1\sqrt{2})^2 + (2 + \sqrt{2})((a_2 - 2a_3) - a_3\sqrt{2})^2 = 2^{2\epsilon}.$$

It follows that

$$(a_0 - 2a_2)^2 + 2a_2^2 + 2(a_1 - 3a_3)^2 + 2a_3^2 = 2^{2\epsilon} \tag{4}$$

and

$$2a_0a_2 - 4a_2^2 + 8a_1a_3 - 14a_3^2 - a_1^2 = 0. \tag{5}$$

From (3) and (4), we deduce that a_0, a_1, a_2 and a_3 are even. Furthermore, we have $4|a_1$.

Suppose that $\epsilon = 1$. If a_2 or a_3 is not zero, then the left-hand side of (3) is >4 which is a contradiction. Hence $a_2 = a_3 = 0$. Similarly, we deduce that $a_1 = 0$. Then $a_0 = \pm 2$ and so $\rho \in \mathbb{Q}$ which is not the case.

Suppose next that $\epsilon = 2$. Putting $a_i = a_i'$ $(i = 0, 1, 2, 3)$, we have

$$(a_0' - 2a_2')^2 + 2{a_2'}^2 + 2(a_1' - 3a_3')^2 + 2{a_3'}^2 = 4. \tag{6}$$

If $a_0' - 2a_2' \neq 0$, then (5) implies that $a_1' = a_2' = a_3' = 0$ and so $\rho \in \mathbb{Q}$ which is a contradiction. Then $a_0' = 2a_2'$. If $a_3' = 0$, then (5) implies that $a_1' = \pm 1$ and so $a_1 = \pm 2$. Since $4|a_1$ we obtain a contradiction. Thus $a_3' = \pm 1$. If $a_1' - 3a_3' = 0$, then $a_1 = \pm 6$ and so 4 does not divide a_1 which is a contradiction. Finally suppose that $a_2' = 0$. It follows that $a_1' - 3a_3' = \pm 1$. Thus, we have

$$(a_0, a_1, a_2, a_3) = (0, 8, 0, 2), (0, -8, 0, -2), (0, 4, 0, -2), (0, -4, 0, 2).$$

We see that these values do not satisfy (4). Finally, we have $(\bar{y} + y)/2 = 0$ and we see that the equation $Y^4F(0, 1) = 3\sqrt{2} - 4$ has no solution in $\mathbb{Q}(\sqrt{2})$. Hence the result follows.

Acknowledgements This work was done during the visit of the second author at the Department of Mathematics of the University of Toulon. The second author wants to thank the department for its warm hospitality and fruitful collaboration. The authors would also like to thank Stéphane Louboutin and Kalman Győry for fruitful discussions.

References

1. Bilu, Y., Hanrot, G.: Solving Thue equations of high degree. J. Number Theory **60**, 373–392 (1996)
2. Baker, A.: Contribution to the theory of Diophantine equations, I. On representation of integers by binary forms. Philos. Trans. R. Soc. Lond. Ser. A **263**, 173–191 (1968)

3. Blanksby, P.E., Loxton, J.H.: A note on the characterization of CM-fields. J. Aust. Math. Soc. (Series A) **26**, 26–30 (1978)
4. Brindza, B., Evertse, J.-H., Győry, K.: Bounds for the solutions of some Diophantine equations in terms of discriminants. J. Aust. Math. Soc. Ser. A **51**(1), 8–26 (1991)
5. Brindza, B., Pintér, Á., van der Poorten, A., Waldschmidt, M.: On the distribution of solutions of Thue's equations. Number Theory in Progress, vol. 1 (Zakopane-Koscielisko, 1997), ed. K. Győry, H. Iwaniec, and J. Urbanowicz, pp. 35–46. de Gruyter, Berlin (1999)
6. Bugeaud, Y., Győry, K.: Bounds for the solutions of Thue–Mahler equations and norm form equations. Acta Arith. **74**, 273–292 (1996)
7. Dickson, L.E.: Introduction to the Theory of Numbers. Dover, New York (1957)
8. Doyle, J.R., Krumm, D.: Computing algebraic numbers of bounded height. Math. Comput. (to appear)
9. Evertse, J.-H.: The number of solutions of decomposable form equations. Invent. Math. **122**, 559–601 (1995)
10. Győry, K.: Sur une classe des corps de nombres algébriques et ses applications. Publ. Math. **22**, 151–175 (1975)
11. Győry, K.: Représentation des nombres entiers par des formes binaires. Publ. Math. Debrecen **24**(3–4), 363–375 (1977)
12. Győry, K., Yu, K.: Bounds for the solutions of S-unit equations and decomposable form equations. Acta Arith. **123**(1), 9–41 (2006)
13. Hanrot, G.: Solving Thue equations without the full unit group. Math. Comput. **69**(229), 395–405 (2000)
14. Heuberger, C.: Parametrized Thue Equations: A Survey. In: Proceedings of the RIMS Symposium "Analytic Number Theory and Surrounding Areas", Kyoto, Oct 18–22, 2004, RIMS Kôkyûroku vol. 1511, August 2006, pp. 82–91
15. Hindry, M., Silverman, J.H.: Diophantine Geometry: An Introduction. Springer, New York (2000)
16. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
17. Louboutin, S., Okazaki, R., Olivier, M.: The class number one problem for some non-abelian normal CM-fields. Trans. Am. Math. Soc. **349**(9), 3657–3678 (1997)
18. Mignotte, M.: An inequality of the greatest roots of a polynomial. Elemente der Math. **46**, 85–86 (1991)
19. Molin, P.: Integration numerique et calculs de fonctions L, Thèse de Doctorat, Université de Bordeaux I (2010)
20. Mordell, L.J.: Diophantine Equations, Pure and Applied Mathematics, vol. 30. Academic Press, London (1969)
21. Pethő, A.: On the resolution of Thue inequalities. J. Symb. Comput. **4**, 103–109 (1987)
22. Poulakis, D.: Integer points on algebraic curves with exceptional units. J. Aust. Math. Soc. **63**, 145–164 (1997)
23. Poulakis, D.: Polynomial bounds for the solutions of a class of Diophantine equations. J. Number Theory **66**(2), 271–281 (1997)
24. Schmidt, W., Schmidt, W.M.: Diophantine Approximation and Diophantine Equations. Springer, Berlin (1991)
25. Silverman, J.H.: Arithmetic of Elliptic Curves. Springer, New York (1986)
26. Thue, A.: Über Annäherungswerte algebraischer Zahlen. J. Reine Angew. Math. **135**, 284–305 (1909)
27. Tzanakis, N., de Weger, B.M.M.: On the practical solution of the Thue equation. J. Number Theory **31**(2), 99–132 (1989)