On the arithmetic of simplest sextic fields and related Thue equations

Günter Lettl, Attila Pethő, Paul Voutier*

1991 Mathematics Subject Classification: 11D41, 11R27.

1. Introduction

In a recent paper [LPV] we investigated Thue inequalities of the form

$$|F_t(X,Y)| \leq k(t),$$

where, for a parameter $t \in \mathbb{Z}$, the form F_t is given by

$$\begin{aligned} F_t(X,Y) = X^6 - 2tX^5Y - (5t+15)X^4Y^2 \\ - 20X^3Y^3 + 5tX^2Y^4 + (2t+6)XY^5 + Y^6. \end{aligned}$$

Using the automorphisms of this form, it suffices to look for relatively prime solutions $(x,y) \in \mathbb{Z}^2$ with $-\frac{y}{2} < x \leq y$ (see Lemma 2 of [LPV]). From the results proved there, it follows that for $t \geq 89$ and $t \leq -92$ the only such solutions of the family of Thue equations

$$|F_t(X,Y)| = 1 \quad \text{or} \quad = 27 \tag{1}$$

are $(0,1)$ and $(1,1)$. In [LPV] the hypergeometric method was used to obtain this result, but one can show that for small values of t this method can never be successfully applied to solve (1). The aim of this paper is to prove the following theorem, which extends the above result for all $t \in \mathbb{Z}$.

Theorem 1. *For $t \in \mathbb{Z}$, the only solutions $(x,y) \in \mathbb{Z}^2$ of*

$$|F_t(x,y)| = 1 \quad \textit{or} \quad = 27$$

with $-\frac{y}{2} < x \leq y$ are $(0,1)$ and $(1,1)$.

[*] Supported partly by the Hungarian–Austrian governmental scientific and technological cooperation and partly by the Hungarian National Foundation for Scientific Research Grant No. 16791/95.

Offprint from: Number Theory, Eds.: Győry/Pethő/Sós

To prove this theorem for $-91 \leq t \leq 88$ we use the usual method for solving Thue equations. So we need to investigate the arithmetic of the underlying number fields, use lower bounds for linear forms in logarithms to obtain initial bounds and then complete the proof by means of computational diophantine results.

We prove a result about the unit group (of rank 5) of the corresponding order of the simplest sextic fields (i.e. the fields generated by the roots of $F_t(X,1)$), which is of interest for its own. This is in perfect analogy to the results of E. Thomas [Th1] for simplest cubic fields and of Lettl & Pethő [LP] for simplest quartic fields. Let us note that there is a gap in the proof of Proposition 1 in [LP], which is corrected by Nakamula & Pethő [NP].

From A. Baker's classical work [B] one knows that there exist effectively computable upper bounds for the solutions of Thue equations. For the practical solution of the Thue equations under consideration we will follow Bilu & Hanrot [BH], who have developed a nice idea to reduce Baker's bound for higher degrees.

For algebraic manipulations and some calculations, we used the computer algebra package MAPLE V running on a PC and on a SUN workstation.

2. Arithmetic in an order of the simplest sextic fields

For $t \in \mathbb{Z}$ we consider the family of polynomials

$$\begin{aligned} P &:= X^6 - 2tX^5 - (5t+15)X^4 - 20X^3 + 5tX^2 + (2t+6)X + 1 \\ &= \prod_{i=1}^{6}(X - \beta_i), \end{aligned} \tag{2}$$

with discriminant $\operatorname{disc}(P) = 6^6(t^2+3t+9)^5$. For $t \notin \{-8,-3,0,5\}$ the polynomial P is irreducible over $\mathbb{Q}[X]$ (see [G2]) and its roots generate a cyclic number field K of degree 6 over $\mathbb{Q}$. By Lemma 2.a) of [LPV] it suffices to consider the values $-1 \leq t \neq 0, 5$. First, we fix a numbering of the roots β_i of P and state some useful relations between them. Bounds for the β_i's are given in Lemma 3 of [LPV].

Lemma 1.

(a) *Let the indices of the roots β_i of P be chosen such that we have*

$$\beta_6 < \beta_5 < \beta_4 < \beta_3 < \beta_2 < \beta_1 = \beta.$$

The Galois group Gal $(K/\mathbb{Q})$ *is generated by* $\sigma\colon \beta \rightarrow \frac{\beta-1}{\beta+2}$, *and with the above numbering of the roots we have* $\sigma(\beta_i) = \beta_{i+1 (\mathrm{mod}\ 6)}$.

(b) *The following relations hold:*

$$\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6 = 1 \qquad \beta_1+\beta_2+\beta_3+\beta_4+\beta_5+\beta_6 = 2t$$

$$\beta_1\beta_3\beta_5 = \beta_2\beta_4\beta_6 = 1 \tag{3}$$

Proof. See Section 3 of [

of β as given in Lemma

Let k_3 denote the c

$\varphi = (\beta\,\sigma^3(\beta))^{-1}$ is an e

algebraic conjugates of

$\varphi_1 =$

$\varphi_2 =$

$\varphi_3 =$

and have the following

cally as $t \rightarrow \infty$":

Using (5) and Lemma 1

mial of φ is $\operatorname{Min}(\varphi) = X$

$(t^2+3t+9)^2$ (see M.N.

Let k_2 denote the qu

$\xi = \beta_1 + \beta_3 + \beta_5$ is an

We calculated that

ξ

thus $\operatorname{Min}(\xi) = X^2 - 2tX$

$4(t^2+3t+9)$. One che

thus $k_2 = \mathbb{Q}(\xi)$ and we

$\xi = \beta_1$

$\xi' = \beta_2$

$$\beta_1^{-1} = -1 - \beta_5 \qquad \frac{\beta_1 - \beta_4}{2} + 1 = \frac{\beta_4}{\beta_3} \tag{4}$$

Proof. See Section 3 of [LPV]. To prove (3) and (4), just express the β_i's in terms of β as given in Lemma 3 of [LPV]. □

Let k_3 denote the cubic subfield of K, i.e. the field fixed by σ^3. Obviously, $\varphi = (\beta\sigma^3(\beta))^{-1}$ is an element of k_3. We choose the following numbering of the algebraic conjugates of φ:

$$\begin{aligned} \varphi_1 &= \frac{\beta_1 + \beta_4}{2} = \frac{1}{\beta_3\beta_6} = \frac{(\beta+1)(\beta-1)}{2\beta+1} \\ \varphi_2 &= \frac{\beta_2 + \beta_5}{2} = \frac{1}{\beta_1\beta_4} = -\frac{2\beta+1}{\beta(\beta+2)} \\ \varphi_3 &= \frac{\beta_3 + \beta_6}{2} = \frac{1}{\beta_2\beta_5} = -\frac{\beta(\beta+2)}{(\beta+1)(\beta-1)} \end{aligned} \tag{5}$$

and have the following relations between the φ_i 's, where $\sim$ stands for "asymtotically as $t \longrightarrow \infty$":

$$\begin{aligned} &\varphi_1 && \sim t + 1 \\ &\varphi_2 = \sigma(\varphi_1) && = -\frac{1}{1+\varphi_1} \sim -\frac{1}{t} \\ &\varphi_3 = \sigma^2(\varphi_1) && = -1 - \frac{1}{\varphi_1} \sim -1 - \frac{1}{t} \end{aligned}$$

Using (5) and Lemma 1.(b) one calculates that the (irreducible) minimal polynomial of φ is $\mathrm{Min}(\varphi) = X^3 - tX^2 - (t+3)X - 1$ with discriminant $\mathrm{disc}(\mathrm{Min}(\varphi)) = (t^2+3t+9)^2$ (see M.N. Gras [G2]); thus k_3 is a simplest cubic field and $k_3 = \mathbb{Q}(\varphi)$.

Let k_2 denote the quadratic subfield of K, i.e. the field fixed by σ^2. Obviously, $\xi = \beta_1 + \beta_3 + \beta_5$ is an element of k_2, with algebraic conjugate $\xi' = \beta_2 + \beta_4 + \beta_6$. We calculated that

$$\xi + \xi' = 2t \qquad \text{and} \qquad \xi\xi' = -3t - 9,$$

thus $\mathrm{Min}(\xi) = X^2 - 2tX - (3t+9)$ is the minimal polynomial of ξ and $\mathrm{disc}(\mathrm{Min}(\xi)) = 4(t^2 + 3t + 9)$. One checks that for $t \neq -8, -3, 0, 5$ this polynomial is irreducible, thus $k_2 = \mathbb{Q}(\xi)$ and we have

$$\begin{aligned} \xi\ &= \beta_1 + \beta_3 + \beta_5 = t + \sqrt{t^2 + 3t + 9} \sim 2t + \frac{3}{2} \\ \xi' &= \beta_2 + \beta_4 + \beta_6 = t - \sqrt{t^2 + 3t + 9} \sim -\frac{3}{2} - \frac{27}{8t} \end{aligned}$$

We want to find the discriminant, "nice" $\mathbb{Z}$-bases and the unit group of the order

$$\mathfrak{O} := \mathbb{Z}[\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6] \subset K$$

as well as for the corresponding orders in the subfields

$$\mathfrak{o}_2 := \mathfrak{O} \cap k_2 \quad \text{and} \quad \mathfrak{o}_3 := \mathfrak{O} \cap k_3.$$

Theorem 2.
(a) *The order* $\mathfrak{O} = \mathbb{Z}[\beta_1, \beta_2]$ *admits* $\mathbb{Z}$*-bases*

$$\begin{aligned}\mathfrak{O} &= (1, \beta_1, \beta_1^2, \beta_1^3, \beta_2, \beta_2^2)_{\mathbb{Z}} = (\beta_1, \beta_2, \beta_3, \varphi_1, \varphi_2, 1)_{\mathbb{Z}} \\ &= (\beta_1, \beta_3, \beta_5, \varphi_1, \varphi_3, 1)_{\mathbb{Z}},\end{aligned} \tag{6}$$

and we have $\operatorname{disc}(\mathfrak{O}) = 2^6(t^2 + 3t + 9)^5$.
(b) *The order* $\mathfrak{o}_3 = \mathbb{Z}[\varphi_1] = \mathbb{Z}[\varphi_1, \varphi_2, \varphi_3]$ *admits* $\mathbb{Z}$*-bases*

$$\mathfrak{o}_3 = (1, \varphi_1, \varphi_1^2)_{\mathbb{Z}} = (1, \varphi_1, \varphi_2)_{\mathbb{Z}},$$

and we have $\operatorname{disc}(\mathfrak{o}_3) = (t^2 + 3t + 9)^2$.
(c) *The order* $\mathfrak{o}_2 = \mathbb{Z}[\xi] = \mathbb{Z}[\sqrt{t^2 + 3t + 9}]$ *admits the* $\mathbb{Z}$*-basis*

$$\mathfrak{o}_2 = (1, \sqrt{t^2 + 3t + 9})_{\mathbb{Z}}, \qquad \textit{and we have} \qquad \operatorname{disc}(\mathfrak{o}_2) = 4(t^2 + 3t + 9).$$

Remark. Let f_2, f_3 and $f = \operatorname{lcm}(f_2, f_3)$ denote the conductors of the fields k_2, k_3 and K, resp. The conductor-discriminant formula yields $d_{k_2} = f_2$, $d_{k_3} = f_3^2$ and $d_K = f^2 f_3^2 f_2$, where d_L denotes the discriminant of an algebraic number field L (see p. 2 of [G2]). From Theorem 2 we can immediately deduce that $\mathfrak{O}$ is the maximal order of K if and only if $\mathfrak{o}_2$ and $\mathfrak{o}_3$ are maximal.

Put $T = t^2 + 3t + 9$. If T is squarefree and $T \not\equiv 0, 1 \pmod 4$ (which is equivalent to $t \equiv 2, 3 \pmod 4$), we have $\operatorname{disc}(\mathfrak{o}_2) = 4T = f_2$. If furthermore $3 \nmid t$ or $t \equiv 12 \pmod{27}$, we have $\operatorname{disc}(\mathfrak{o}_3) = T^2 = f_3^2$ (see Prop. 2 of [G1]). By a result of Erdős [Er] or a proof similar to that of Lemma 8.8 in [N], one can show that there exist infinitely many $t \in \mathbb{N}$ satisfying these conditions, i.e. $\mathfrak{O}$ equals the ring of integers of K for infinitely many $t \in \mathbb{N}$.

Proof of Theorem 2. (a) Since β_i is an algebraic unit, $\mathbb{Z}[\beta_i]$ contains also all negative powers of β_i. Thus from (3) we obtain $\mathfrak{O} = \mathbb{Z}[\beta_1, \beta_2, \beta_5, \beta_6]$, and using the first part of (4) and the conjugated formula $\beta_2^{-1} = -1 - \beta_6$ we see that $\mathfrak{O} = \mathbb{Z}[\beta_1, \beta_2]$.

Let $\mathfrak{O}' := \mathbb{Z}[\beta_1] = (1, \beta_1, \beta_1^2, \beta_1^3, \beta_1^4, \beta_1^5)_{\mathbb{Z}}$ with $\operatorname{disc}(\mathfrak{O}') = \operatorname{disc}(P) = 6^6(t^2+3t+9)^5$. One calculates that

$$\beta_2 = \sum_{i=0}^{5} x_i \beta_1^i \quad \text{with } x_5 = -\frac{1}{9} \text{ and } 9x_i \in \mathbb{Z} \text{ for } 0 \le i \le 5,$$

thus $\mathfrak{O}' \subset \mathfrak{O}'' := (1, \beta_1,$
disc$(\mathfrak{O}'') = 9 \cdot 2^6(t^2 + 3$

$$\beta_2^2 = \sum_{i=0}^{4} x_i \beta_1^i +$$

thus $\mathfrak{O}'' \subset \mathfrak{O}''' := (1,$
$2^6(t^2 + 3t + 9)^5$.

One verifies that β
ring containing β_1 and
stated $\mathbb{Z}$-bases for $\mathfrak{O}$, or
obvious.

(b) The only import
are well known (see e.g
of $\mathfrak{O}$, which are invaria
write an arbitrary $\alpha \in$

$$\alpha = x_1\beta_1 + x$$

and calculate that

$$\sigma^3(\alpha) =$$

From $\alpha = \sigma^3(\alpha)$ we ob
arbitrary, thus $\mathfrak{o}_3 = (1,$

(c) By definition, $\mathfrak{o}_2$
σ^2. Using the third $\mathbb{Z}$-b

$$\alpha = x_1\beta_1 + x_2$$

and calculate that

$$\sigma^2(\alpha) = x_3\beta_1 +$$

From $\alpha = \sigma^2(\alpha)$ we ob
and $x_4 = x_5 = 0$, thus

Remark. One can als

$$\mathfrak{O} =$$

by calculating the disc

Our main interest is
at least of a subgroup

Let $\varepsilon > 1$ be the fi
plicitly be calculated fr
have

thus $\mathfrak{O}' \subset \mathfrak{O}'' := (1, \beta_1, \beta_1^2, \beta_1^3, \beta_1^4, \beta_2)_{\mathbb{Z}}$ with $(\mathfrak{O}'' : \mathfrak{O}') = 9$ and $\operatorname{disc}(\mathfrak{O}'') = 9 \cdot 2^6(t^2 + 3t + 9)^5$. Once more, one calculates

$$\beta_2^2 = \sum_{i=0}^{4} x_i \beta_1^i + x_5 \beta_2 \qquad \text{with } x_4 = \frac{1}{3} \ \text{ and } \ 3x_i \in \mathbb{Z} \text{ for } 0 \le i \le 5,$$

thus $\mathfrak{O}'' \subset \mathfrak{O}''' := (1, \beta_1, \beta_1^2, \beta_1^3, \beta_2, \beta_2^2)_{\mathbb{Z}}$ with $(\mathfrak{O}''' : \mathfrak{O}'') = 3$, thus $\operatorname{disc}(\mathfrak{O}''') = 2^6(t^2 + 3t + 9)^5$.

One verifies that $\beta_2^3, \beta_1^i \beta_2^j \in \mathfrak{O}'''$ for $1 \le i \le 3, 1 \le j \le 2$, thus $\mathfrak{O}'''$ is a ring containing β_1 and β_2, and therefore $\mathfrak{O}''' = \mathfrak{O}$. To verify also the last two stated $\mathbb{Z}$-bases for $\mathfrak{O}$, one just calculates their discriminants, since one inclusion is obvious.

(b) The only important thing to prove is that $\mathfrak{o}_3 = \mathbb{Z}[\varphi_1]$, all other statements are well known (see e.g. [MPL]). By definition, $\mathfrak{o}_3$ just consists of those elements of $\mathfrak{O}$, which are invariant under σ^3. Using the second $\mathbb{Z}$-basis given in (6), we can write an arbitrary $\alpha \in \mathfrak{O}$ as

$$\alpha = x_1\beta_1 + x_2\beta_2 + x_3\beta_3 + x_4\varphi_1 + x_5\varphi_2 + x_6 \quad \text{with} \quad x_i \in \mathbb{Z}, \tag{7}$$

and calculate that

$$\begin{aligned} \sigma^3(\alpha) = {} & -x_1\beta_1 - x_2\beta_2 - x_3\beta_3 + (2x_1 - 2x_3 + x_4)\varphi_1 \\ & + (2x_2 - 2x_3 + x_5)\varphi_2 + (x_6 + 2tx_3). \end{aligned}$$

From $\alpha = \sigma^3(\alpha)$ we obtain that $x_1 = x_2 = x_3 = 0$ and $x_4, x_5, x_6 \in \mathbb{Z}$ may be arbitrary, thus $\mathfrak{o}_3 = (1, \varphi_1, \varphi_2)_{\mathbb{Z}} = \mathbb{Z}[\varphi_1]$.

(c) By definition, $\mathfrak{o}_2$ consists of those elements of $\mathfrak{O}$, which are invariant under σ^2. Using the third $\mathbb{Z}$-basis given in (6), we can write an arbitrary $\alpha \in \mathfrak{O}$ as

$$\alpha = x_1\beta_1 + x_2\beta_3 + x_3\beta_5 + x_4\varphi_1 + x_5\varphi_3 + x_6 \qquad \text{with} \qquad x_i \in \mathbb{Z},$$

and calculate that

$$\sigma^2(\alpha) = x_3\beta_1 + x_1\beta_3 + x_2\beta_5 + (-x_5)\varphi_1 + (x_4 - x_5)\varphi_3 + (x_6 + tx_5).$$

From $\alpha = \sigma^2(\alpha)$ we obtain that $x_1 = x_2 = x_3 \in \mathbb{Z}$ and $x_6 \in \mathbb{Z}$ may be arbitrary, and $x_4 = x_5 = 0$, thus $\mathfrak{o}_2 = (1, \xi)_{\mathbb{Z}} = \mathbb{Z}[\sqrt{t^2 + 3t + 9}]$.

Remark. One can also show that

$$\mathfrak{O} = \mathfrak{o}_3 \oplus \beta_1 \mathfrak{o}_3 = (1, \varphi_1, \varphi_1^2, \beta_1, \beta_1\varphi_1, \beta_1\varphi_1^2)_{\mathbb{Z}}$$

by calculating the discriminant of this basis.

Our main interest is to find a basis of $\mathfrak{O}^\times$, the group of units of the ring $\mathfrak{O}$, or at least of a subgroup of $\mathfrak{O}^\times$ with small index.

Let $\varepsilon > 1$ be the fundamental unit of the quadratic order $\mathfrak{o}_2$, which can explicitly be calculated from the continued fraction expansion of $\sqrt{t^2 + 3t + 9}$; so we have

$$\mathfrak{o}_2^\times = \langle -1, \varepsilon \rangle.$$

There is no parametrization known for these units, their sizes vary considerably, and e.g. for $t = 70$ we found $\varepsilon \approx 10^{75}$.

It was proved by Thomas [Th1] that

$$\mathfrak{o}_3^\times = \langle -1, \varphi_1, \varphi_2 \rangle. \tag{8}$$

Besides these units, $\mathfrak{O}^\times$ contains the units β_i $(1 \le i \le 6)$ and $\omega_i := \frac{\beta_i}{\beta_{i+3}}$ $(1 \le i \le 3)$. The latter are relative units, i.e. one has $N_{K/k_3}(\omega_i) = N_{K/k_2}(\omega_i) = 1$, which follows from (3) (see also [G2]). Here $N_{M/L}$ denotes the norm from a field M to some subfield L. Our main result is the following

Theorem 3. *Let $\mathcal{E}$ be the group of units generated by -1, ε, β_i $(1 \le i \le 6)$, i.e.*

$$\mathcal{E} := \langle -1, \beta_1, \beta_2, \beta_4, \beta_5, \varepsilon \rangle \le \mathfrak{O}^\times.$$

Then $(\mathfrak{O}^\times : \mathcal{E}) = 1$ *or* $= 3$.

To make the proof of this theorem more comprehensible, we will separate out some partial steps in the following lemmas.

Lemma 2. *$\{\beta_1, \beta_2, \beta_4, \beta_5, \varepsilon\}$ are multiplicatively independent, therefore the index $(\mathfrak{O}^\times : \mathcal{E})$ is finite.*

Proof. It suffices to show that the regulator R of $\{\beta_1, \beta_2, \beta_4, \beta_5, \varepsilon\}$ does not vanish. Putting $L_i := \log|\beta_i|$ and remembering that $\varepsilon > 1$, we calculate

$$R = \log(\varepsilon) \det \begin{vmatrix} L_1 & L_2 & L_5 & L_6 & 1 \\ L_2 & L_3 & L_6 & L_1 & -1 \\ L_3 & L_4 & L_1 & L_2 & 1 \\ L_4 & L_5 & L_2 & L_3 & -1 \\ L_5 & L_6 & L_3 & L_4 & 1 \end{vmatrix} =$$

$$\begin{aligned} = 3\log(\varepsilon)\Big(& L_1^4 + 2L_1^3L_5 + L_1^2(L_2^2 - 2L_2L_6 + 3L_5^2 - 2L_6^2) \\ & + 2L_1(2L_2^2L_5 + 2L_2L_5L_6 + L_5^3 - L_5L_6^2) \\ & + L_2^4 + 2L_2^3L_6 + L_2^2L_5^2 + 3L_2^2L_6^2 + 4L_2L_5^2L_6 \\ & + 2L_2L_6^3 + L_5^4 + L_5^2L_6^2 + L_6^4\Big) \end{aligned}$$

To obtain the last expression, we substituted $L_3 = -L_1 - L_5$ and $L_4 = -L_2 - L_6$, both arising from (3). From the bounds for β_i, as given in Lemma 3 of [LPV], we deduce that for $t \geq 6$ we have

$$\log\left(2t+\frac{5}{2}\right) < L_1 < \log\left(2t+\frac{7}{2}\right)$$
$$-\frac{3}{t} < L_2 < -\frac{1}{t}$$
$$\frac{1}{4t} < L_5 < \frac{1}{2t}$$
$$\frac{1}{2} < \log(2) < L_6 < \log(2) + \frac{3}{4t} < 1$$

Using these bounds and neglecting small positive summands, we obtain for $t \geq 6$

$$\begin{aligned}\frac{R}{3\log(\varepsilon)} &> (L_1^2 - L_6^2)^2 + 2L_1^3L_5 + 2L_1^2(-L_2)L_6 - 2L_1L_5L_6(-2L_2 + L_6)\\ &\quad - 2(-L_2)L_6(L_2^2 + 2L_5^2 + L_6^2)\\ &> (L_1^2 - L_6^2)^2 + \frac{\log^3(2t+\frac{5}{2})}{2t} + \frac{\log^2(2t+\frac{5}{2})}{t} - \frac{2\log(2t+\frac{7}{2})}{t} - \frac{9}{t}\\ &> (L_1^2 - L_6^2)^2 > 0.\end{aligned}$$

For $t \in \{-1, 1, 2, 3, 4\}$ we used the numerical values of the roots β_i to verify $R > 0$. □

Lemma 3. *Suppose that there exist $\eta \in \mathfrak{O}^\times$ and $k, e_i \in \mathbb{Z}$ with $k \geq 2$ and $\gcd(k, e_1, e_2, e_4, e_5) = 1$ such that*

$$\eta^k = \pm\beta_1^{e_1}\beta_2^{e_2}\beta_4^{e_4}\beta_5^{e_5}.$$

Then $e_1 \equiv -e_4 \pmod{k}$, $e_2 \equiv -e_5 \pmod{k}$ and $k \equiv 1 \pmod{2}$ holds.

Proof. Supposing that such an η exists, we obtain that

$$N_{K/k_3}(\eta^k) = \eta^k\,\sigma^3(\eta^k) = \beta_1^{e_1+e_4}\beta_2^{e_2+e_5}\beta_4^{e_1+e_4}\beta_5^{e_2+e_5}$$

must be a k-th power in $\mathfrak{o}_3^\times$, where we used (3) to eliminate β_3 and β_6 in the above expression. By (8) and (5) we know that $\mathfrak{o}_3^\times$ is generated by $\varphi_2 = (\beta_1\beta_4)^{-1}$ and $\varphi_3 = (\varphi_1\varphi_2)^{-1} = (\beta_2\beta_5)^{-1}$, from which we deduce the stated congruences for the e_i's. Without loosing generality, we may suppose that $\eta^k = \pm(\beta_1\beta_4^{-1})^{e_1}(\beta_2\beta_5^{-1})^{e_2}$. If k is even, this last expression must be a totally positive algebraic number. Since at least one of e_1, e_2 must be odd, one can consider the signs of the β_i's and arrives at a contradiction for any possible case. □

For $\alpha \in K$ we define

$$S_2(\alpha) := \sum_{i=0}^{5}\sigma^i(\alpha^2) \quad\text{and}\quad f(\alpha) := S_2(\alpha) + S_2(\alpha^{-1}). \tag{9}$$

We will use Theorem 2 of Lettl [L] to show that $\{\beta_1, \beta_2, \beta_4, \beta_5\}$ can be extended to a basis of the group of units $\mathfrak{O}^\times$. For this purpose we need "successive minima" $\eta_1, \eta_2, \dots$ of $\mathfrak{O}^\times$ under f, which are defined as follows:

$$f(\eta_i) := \min\{f(\alpha) \mid \alpha \in \mathfrak{O}^\times \setminus \langle -1, \eta_1, \dots, \eta_{i-1}\rangle\} \quad \text{for } 1 \le i. \tag{10}$$

Lemma 4. *With the above notations we have*

$$\begin{aligned} 4t^2 + 12t + 30 &= \min\{f(\alpha) \mid \alpha \in \mathfrak{O}^\times \setminus \{1, -1\}\} \\ &= f(\pm\varphi_i^{\pm 1}), \quad 1 \le i \le 3 \end{aligned} \tag{11}$$

and

$$\begin{aligned} 8t^2 + 24t + 66 &= \min\{f(\alpha) \mid \alpha \in \mathfrak{O}^\times \setminus \langle -1, \varphi_1, \varphi_2, \varphi_3\rangle\} \\ &= f(\pm\beta_i^{\pm 1}), \quad 1 \le i \le 6. \end{aligned} \tag{12}$$

Proof. We use the second $\mathbb{Z}$-basis from (6) to represent elements of $\mathfrak{O}$, thus any $\alpha \in \mathfrak{O}$ can be written as in (7),

$$\alpha = x_1\beta_1 + x_2\beta_2 + x_3\beta_3 + x_4\varphi_1 + x_5\varphi_2 + x_6 \qquad \text{with} \qquad x_i \in \mathbb{Z}.$$

We obtain

$$S_2(\alpha) = 6\left(\tfrac{t}{3}(x_1 + x_2 + x_3 + x_4 + x_5) + x_6\right)^2 + \tfrac{1}{3}\left(t^2 + 3t + 9\right) Q,$$

with

$$\begin{aligned} Q = {} & (-x_1 + 2x_2 - x_3 - x_4 + 2x_5)^2 + (-x_1 + 3x_3 - x_4)^2 \\ & + 2(x_1 + x_4)^2 + 6x_1^2 + 6x_2^2. \end{aligned}$$

S_2 and Q are positive definite quadratic forms in the x_i's. We have

$$\begin{aligned} S_2(\pm\varphi_i) &= 2t^2 + 4t + 12, & S_2(\pm\varphi_i^{-1}) &= 2t^2 + 8t + 18, \\ S_2(\pm\beta_i) &= 4t^2 + 10t + 30, & S_2(\pm\beta_i^{-1}) &= 4t^2 + 14t + 36, \end{aligned}$$

therefore $f(\pm\varphi_i^{\pm 1}) = 4t^2 + 12t + 30$ and $f(\pm\beta_i^{\pm 1}) = 8t^2 + 24t + 66$ as stated in (11) and (12). To prove the lemma it suffices to find all units $\alpha \in \mathfrak{O}^\times$ with

$$S_2(\alpha) \le 4t^2 + 12t + 33 = \frac{1}{2} f(\beta_i) \tag{13}$$

and to check whether $f(\alpha) \le f(\beta_i)$.

Let $\alpha \in \mathfrak{O}^\times$ be given as in (7). If $Q = 12$, we have $S_2(\alpha) \ge 4(t^2 + 3t + 9)$, which contradicts (13). Considering Q modulo 2 and 3, we see that this form can only attain values congruent to 0 or 4 modulo 6. So we first determine all $\mathbf{x} := (x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5$ with $Q(\mathbf{x}) \in \{0, 4, 6, 10\}$. Since $S_2(\alpha) = S_2(\pm\sigma^i(\alpha))$,

we may neglect all solut
arrive at the following

Case
1
2
3
4
5
6

We will determine,
± 1, and furthermore s

Case 1. $\alpha = x_6$.
This yields $\alpha = \pm 1$, th

Case 2. $\alpha = \varphi_1 + x_6$.
We have $N_{k_3/\mathbb{Q}}(\alpha) = x$
If $N_{k_3/\mathbb{Q}}(\alpha) = 1$, w
$\alpha = \varphi_1$. The quadrati
no interest for us) and
$S_2(\varphi_1 + 2) = 26 > 4t^2$
do not contradict the s
If $N_{k_3/\mathbb{Q}}(\alpha) = -1$,
$\alpha = \varphi_1 + 1 = -\varphi_2^{-1}$. T
under consideration.

Case 3. $\alpha = \frac{\beta_1 - \beta_4}{2} + x$
We put $T := t^3 + 3t +$
obtain $(x_6^2 - 1)(x_6^4 -$
and $\alpha = \frac{\beta_1 - \beta_4}{2} - 1 =$
$2t^2 + 6t + 24$ and $S_2($
The discriminant of th
of an integer if and on
$S_2(\alpha \pm 2) = 38 > 4t^2$
statement of our lemm
If $N_{K/\mathbb{Q}}(\alpha) = -1$,
$\gcd(x_6^2 - 1, x_6^2 + 1) \mid 2$,
thus $x_6^2 - 1 = \pm 1$ or

we may neglect all solutions giving conjugates or negatives of other solutions, and arrive at the following cases:

Case	$Q(\mathbf{x})$	$\mathbf{x}$	α
1	0	$(0,0,0,0,0)$	x_6
2	4	$(0,0,0,1,0)$	$\varphi_1 + x_6$
3	6	$(1,0,0,-1,0)$	$\dfrac{\beta_1-\beta_4}{2} + x_6$
4	10	$(1,0,0,0,0)$	$\beta_1 + x_6$
5	10	$(1,0,0,0,1)$	$\beta_1 + \varphi_2 + x_6$
6	10	$(0,1,0,1,0)$	$\beta_2 + \varphi_1 + x_6$

We will determine, which values of x_6 yield units of $\mathfrak{O}$ by checking $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, and furthermore satisfy (13), which yields lower and upper bounds for x_6.

Case 1. $\alpha = x_6$.
This yields $\alpha = \pm 1$, the roots of unity of $\mathfrak{O}^{\times}$.

Case 2. $\alpha = \varphi_1 + x_6$.
We have $N_{k_3/\mathbb{Q}}(\alpha) = x_6^3 + tx_6^2 - (t+3)x_6 + 1$.

If $N_{k_3/\mathbb{Q}}(\alpha) = 1$, we obtain $x_6(x_6^2 + tx_6 - (t+3)) = 0$, and $x_6 = 0$ yields $\alpha = \varphi_1$. The quadratic factor has rational roots only for $t = -3$ (which is of no interest for us) and $t = -1$, giving $x_6 = -1$ and $x_6 = 2$. Since for $t = -1$, $S_2(\varphi_1 + 2) = 26 > 4t^2 + 12t + 33$ and $f(\varphi_1 - 1) = 54 > 8t^2 + 24t + 66$, these units do not contradict the statement of Lemma 4.

If $N_{k_3/\mathbb{Q}}(\alpha) = -1$, we obtain $(x_6 - 1)(x_6^2 + (t+1)x_6 - 2) = 0$, and $x_6 = 1$ yields $\alpha = \varphi_1 + 1 = -\varphi_2^{-1}$. The quadratic factor has no rational roots for the values of t under consideration.

Case 3. $\alpha = \frac{\beta_1-\beta_4}{2} + x_6$.
We put $T := t^3 + 3t + 9$ and have $N_{K/\mathbb{Q}}(\alpha) = x_6^6 - (x_6^2 - 1)^2 T$. If $N_{K/\mathbb{Q}}(\alpha) = 1$, we obtain $(x_6^2 - 1)(x_6^4 - (T-1)x_6^2 + (T+1)) = 0$. $x_6 = \pm 1$ yields $\alpha = \frac{\beta_1-\beta_4}{2} + 1 = \frac{\beta_4}{\beta_3}$ and $\alpha = \frac{\beta_1-\beta_4}{2} - 1 = -\frac{\beta_1}{\beta_6}$, where we used the second part of (4). But $S_2\left(\frac{\beta_2}{\beta_1}\right) = 2t^2 + 6t + 24$ and $S_2\left(\frac{\beta_1}{\beta_2}\right) = 8t^2 + 24t + 78$ yields $f\left(\frac{\beta_2}{\beta_1}\right) = 10t^2 + 30t + 102 > f(\beta_i)$. The discriminant of the biquadratic factor equals $(T-3)^2 - 12$, which is a square of an integer if and only if $T - 3 = \pm 4$. We obtain $t = -1$ and $x_6 = \pm 2$, but again $S_2(\alpha \pm 2) = 38 > 4t^2 + 12t + 33$ shows, that these units do not contradict the statement of our lemma.

If $N_{K/\mathbb{Q}}(\alpha) = -1$, we obtain $(x_6^2 + 1)(x_6^4 - x_6^2 + 1) - (x_6^2 - 1)^2 T = 0$. Since $\gcd(x_6^2 - 1, x_6^2 + 1) \mid 2$, either $x_6^2 - 1$ or $\frac{x_6^2-1}{2}$ must divide $x_6^4 - x_6^2 + 1 = x_6^2(x_6^2 - 1) + 1$, thus $x_6^2 - 1 = \pm 1$ or $\frac{x_6^2-1}{2} = \pm 1$, which yields as only integral solution $x_6 = 0$.

This implies $T-1=0$, which yields no real values for t. So in Case 3 we found no units contradicting (11) or (12).

In *Cases* 4–6 we have $Q=10$, thus $S_2(\alpha) \le 4t^2+12t+33$ is equivalent to $\left(\frac{t}{3}\sum_{i=1}^{5} x_i + x_6\right)^2 \le \frac{t^2}{9}+\frac{t}{3}+\frac{1}{2} < \left(\frac{t}{3}+1\right)^2$. Thus we can restrict ourselves to values x_6 with

$$-\frac{t}{3}-1 < \frac{t}{3}\cdot\sum_{i=1}^{5} x_i + x_6 < \frac{t}{3}+1. \tag{14}$$

Case 4. $\alpha = \beta_1 + x_6$.
We have $N_{K/\mathbb{Q}}(\alpha) = P(-x_6)$ with P given by (2), and (14) specializes to $-\frac{2t}{3}-1 < x_6 < 1$. For $x_6 = 0$ we have $N_{K/\mathbb{Q}}(\alpha) = 1$ and obtain $\alpha = \beta_1$. By the above lower bound, $x_6 \le -1$ is only to be considered for $t \ge 1$. We know that P has six real roots, which for $t \ge 1$ are all outside the interval $[1, 2t]$. Since P is concave in this interval, we obtain that $P(-x_6) \le \max\{P(1), P(2t)\} = -27$ for $-2t \le x_6 \le -1$, thus there are no further solutions of $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Case 5. $\alpha = \beta_1 + \varphi_2 + x_6$.
We have $N_{K/\mathbb{Q}}(\alpha) = g(x_6)$ with

$$\begin{aligned} g(X) &= X^6 + 4tX^5 + (5t^2-5t-15)X^4 + (2t^3-10t^2-30t+16)X^3 \\ &\quad - (5t^3+12t^2-44t-27)X^2 + (2t^3+22t^2+2t-48)X \\ &\quad - (5t^2+15t-19). \end{aligned}$$

By (14) we only need to consider values x_6 with

$$-t-1 < x_6 < -\frac{t}{3}+1.$$

From $g(1) = -t^3$, $g(0) = -5t^2-15t+19$ and $g(-1) = -9t^3-24t^2+48t+64$ we obtain the special solutions $x_6 = 1$ for $t=-1$ and $x_6 = 0$ for $t = 1$. Since $f(\beta_1+\varphi_2+1) = 78 > 8t^2+24t+66$ for $t=-1$ and $f(\beta_1+\varphi_2) = 638 > 8t^2+24t+66$ for $t=1$, these units do not contradict (12).

By the above lower bound for x_6, we can now restrict ourselves to $t \ge 2$. We obtain that $g(-2t-2) < 0$, $g(-t-1) > 0$ and $g(-t+1) < 0$, thus g has (at least) 3 real zeros less than $-t+1$. Similarly, one finds that g also has 3 real zeros larger than 0. Since g has no zero in the interval $[-t+1, 0]$, we obtain for $-t+1 \le x_6 \le 0$ and $t \ge 2$ that $g(x_6) \le \max\{g(-t+1), g(0)\} \le -8$. Finally, $g(-t) > 1$ shows that also in this case there exists no unit contradicting our lemma.

Case 6. $\alpha = \beta_2 + \varphi_1 + x_6$.
This time we have $N_{K/\mathbb{Q}}(\alpha) = g(x_6)$ with

$$\begin{aligned} g(X) &= X^6 + 4tX^5 + (5t^2-5t-15)X^4 + (2t^3-12t^2-36t-2)X^3 - \\ &\quad - (7t^3+15t^2-35t-54)X^2 + (6t^3+40t^2+56t+6)X \\ &\quad - (9t^2+27t+17). \end{aligned}$$

Again, we only need to

For $t=-1$, $g(1) = t^3 +$
may restrict ourselves t
and $g(-t) < 0$, g has
than 0. We conclude t
no further solutions of

Proof of Theorem 3. Fi
a basis of $\mathfrak{O}^\times$ (are "fu
S_2 and f in (9) agree
the following units are

$$\eta_1 := \varphi_2 =$$

Here we used (3), (8)
units as needed for (10
of $\mathfrak{O}^\times$. Since $\pm\varphi_2\varphi_3\beta_1$
Theorem 2.(a) of [L]
Now we apply Theore

$$\varepsilon_1 := \varphi_2 = \frac{}{\beta_1}$$

Since by Lemma 3 k
unit η of the form

$$\eta^5 = \pm$$

(In the above lines w
Everywhere else in t
order $\mathfrak{o}_2$. The reader
Using the congrue
the following possibili

$$\eta^5 = \frac{\beta_1^2\beta_2}{\beta_4^2\beta_5},$$

Considering the sizes
in the first 4 cases fo

Again, we only need to consider values x_6 with

$$-t-1 < x_6 < -\frac{t}{3} + 1.$$

For $t = -1$, $g(1) = t^3 + 9t^2 + 27t + 25 \neq \pm 1$. Because of the above bounds, we now may restrict ourselves to $t \geq 1$ and $-t \leq x_6 \leq 0$. Since $g(-t-3) < 0$, $g(-t-2) > 0$ and $g(-t) < 0$, g has 3 real zeros less than $-t$, and similarly, 3 real zeros larger than 0. We conclude that for $-t \leq x_6 \leq 0$ $g(x_6) \leq \max\{g(-t), g(0)\} \leq -53$, thus no further solutions of $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ exist. □

Proof of Theorem 3. First we want to show that $\{\beta_1, \beta_2, \beta_4, \beta_5\}$ can be extended to a basis of $\mathfrak{O}^\times$ (are "fundamental units" in the terminology of [L]). The functions S_2 and f in (9) agree with S_2 and F_2 in (1) of [L]. From Lemma 4 we deduce that the following units are successive minima of $\mathfrak{O}^\times$ under f:

$$\eta_1 := \varphi_2 = \frac{1}{\beta_1\beta_4}, \quad \eta_2 := \varphi_3 = \frac{1}{\beta_2\beta_5}, \quad \eta_3 := \beta_1, \quad \eta_4 := \beta_2.$$

Here we used (3), (8) and Lemma 2 to check multiplicative (in-)dependence of the units as needed for (10). By Theorem 1 of [L], $\{\varphi_2, \varphi_3\}$ can be extended to a basis of $\mathfrak{O}^\times$. Since $\pm\varphi_2\varphi_3\beta_1$ is not totally positive, K does not contain $\sqrt{\pm\varphi_2\varphi_3\beta_1}$ and Theorem 2.(a) of [L] shows that we can take β_1 as a third basis element for $\mathfrak{O}^\times$. Now we apply Theorem 2.(b) of [L] with

$$\varepsilon_1 := \varphi_2 = \frac{1}{\beta_1\beta_4}, \quad \varepsilon_2 := \varphi_3 = \frac{1}{\beta_2\beta_5}, \quad \varepsilon_3 := \beta_1 \quad \text{and} \quad \varepsilon := \beta_2.$$

Since by Lemma 3 k must be odd, we only have to check whether $\mathfrak{O}$ contains any unit η of the form

$$\eta^5 = \pm\varepsilon^2\varepsilon_i^{\pm 2}\varepsilon_j^{\pm 1}\varepsilon_k^{\pm 1} \qquad \text{or} \qquad \eta^3 = \pm\varepsilon\,\varepsilon_1^{\pm 1}\varepsilon_2^{\pm 1}\varepsilon_3^{\pm 1}.$$

(In the above lines we used $\varepsilon := \beta_2$ to be in accordance with the notation in [L]. Everywhere else in this paper, ε denotes the fundamental unit of the quadratic order $\mathfrak{o}_2$. The reader is kindly asked to apologize this ambiguity!)

Using the congruence conditions for the exponents of the β_i's from Lemma 3, the following possibilities remain:

$$\eta^5 = \frac{\beta_1^2\beta_2}{\beta_4^2\beta_5}, \qquad \eta^5 = \frac{\beta_4^2\beta_2}{\beta_1^2\beta_5} = \frac{\beta_4\beta_3}{\beta_1\beta_6}, \qquad \eta^5 = \frac{\beta_1\beta_2}{\beta_4\beta_5}, \qquad \eta^5 = \frac{\beta_4\beta_2}{\beta_1\beta_5} = \frac{\beta_3}{\beta_6},$$

$$\eta^3 = \frac{\beta_1\beta_2}{\beta_4\beta_5}, \qquad \eta^3 = \frac{\beta_3}{\beta_6}.$$

Considering the sizes of the β_i's and using Lemma 3.a) of [LPV] we can show that in the first 4 cases for $t \geq 6$

$$S_2(\eta) \leq 3 \cdot \left|\frac{\beta_6^2\beta_1}{\beta_3^2\beta_4}\right|^{\frac{2}{5}} + 3 < 4t^2 + 12t + 33,$$

but the existence of such a unit η would contradict (12) of Lemma 4. Similarly, in the latter 2 cases we obtain for $t \geq 9$

$$S_2(\eta) \leq 3 \cdot \left|\frac{\beta_6\beta_1}{\beta_3\beta_4}\right|^{\frac{2}{3}} + 3 < 4t^2 + 12t + 33.$$

A numerical computation shows that also for the remaining values of t we always have $S_2(\eta) < 4t^2 + 12t + 33$, up to 2 exceptions for $t = -1$. But then $S_2(\eta)$ is no rational integer, thus there exist no such η in our sextic orders, and $\{\varphi_2, \varphi_3, \beta_1, \beta_2\}$ and also $\{\beta_1, \beta_2, \beta_4, \beta_5\}$ can be extended to a basis of $\mathfrak{O}^\times$.

So we have $\mathfrak{O}^\times = \langle -1, \beta_1, \beta_2, \beta_4, \beta_5, \eta\rangle$ with some $\eta \in \mathfrak{O}^\times$, and by Lemma 2

$$\eta^k = \beta_1^{e_1}\beta_2^{e_2}\beta_4^{e_4}\beta_5^{e_5}\varepsilon^e$$

with $k, e, e_1, e_2, e_4, e_5 \in \mathbb{Z}$, $e \neq 0$ and $\gcd(k, e, e_1, e_2, e_4, e_5) = 1$. Now we use the same argument as at the end of the proof of Proposition 1 in [LP]. Consider the absolute value of the relative norm map from K to k_2

$$\begin{aligned} \mathcal{N} : \mathfrak{O}^\times &\to \langle\varepsilon\rangle \\ \gamma &\mapsto |N_{K/k_2}(\gamma)|. \end{aligned}$$

From (3) we see that $\mathcal{N}(\beta_i) = 1$, thus $\langle -1, \beta_1, \beta_2, \beta_4, \beta_5\rangle \subset \ker(\mathcal{N})$. On the other hand, $\mathcal{N}(\varepsilon) = \varepsilon^3$ and $e \neq 0$ show that $\mathcal{N}(\eta) \neq 1$, and we obtain $\ker(\mathcal{N}) = \langle -1, \beta_1, \beta_2, \beta_4, \beta_5\rangle$.

Put $\mathcal{N}(\eta) = \varepsilon^{3m+j}$ with $m \in \mathbb{Z}$ and $j \in \{0, 1, 2\}$. If $j = 0$, $\mathcal{N}(\eta\varepsilon^{-m}) = 1$ and $\eta\varepsilon^{-m} \in \ker(\mathcal{N})$ implies that $\mathfrak{O}^\times = \langle -1, \beta_1, \beta_2, \beta_4, \beta_5, \varepsilon\rangle$.

If $j = 1, 2$, $\eta^3\varepsilon^{-3m-j} \in \ker(\mathcal{N}) = \langle -1, \beta_1, \beta_2, \beta_4, \beta_5\rangle$ and we obtain that $(\mathfrak{O}^\times : \langle -1, \beta_1, \beta_2, \beta_4, \beta_5, \varepsilon\rangle) = 3$. □

Remark. From the above proof and Lemma 3 one can deduce that the index of the unit groups is 3 if and only if there exists an $\eta \in \mathfrak{O}^\times$ with $\eta^3 = \varepsilon\left(\frac{\beta_1\beta_2}{\beta_4\beta_5}\right)^e$ for some $e \in \{-1, 0, 1\}$. In this case, $\mathfrak{O}^\times = \langle -1, \beta_1, \beta_2, \beta_4, \beta_5, \eta\rangle$.

The index $(\mathfrak{O}^\times : \mathcal{E})$ can indeed be equal to 3. For $t = 10$, $\mathfrak{O}$ is the maximal order of K and $\eta = \left(\varepsilon\frac{\beta_4\beta_5}{\beta_1\beta_2}\right)^{1/3}$ belongs to K. It is a zero of the polynomial

$$X^6 + 6956X^5 - 200701X^4 - 155126760X^3 - 200701X^2 + 6956X + 1.$$

3. Proof of Theorem 1

In this section we will completely solve the Thue equation (1) for all $t \in \mathbb{Z}$. As already mentioned in the introduction, we can restrict ourselves to solutions $(x, y) \in \mathbb{Z}^2$ with $-\frac{y}{2} < x \leq y$. Each such solution yields 5 further solutions by Lemma 2 of [LPV].

Since $F_t(Y, X) = F_{-t-3}(X, Y)$, we may restrict ourselves to $-1 \leq t$. From $F_t(X - Y, X + 2Y) = -27\,F_t(X, Y)$ we see that each $(x, y) \in \mathbb{Z}^2$ with $|F_t(x, y)| = 1$

yields $|F_t(x-y, x+2y)|=$
One finds that $F_t(x', y')$
obtains $(x, y) = \Big(\frac{2x'+y'}{3}$
between the integral solu
it suffices to investigate

For $t \in \{0, 5\}$, F_t fa
$F_5 = F_{-2}^{(3)}\,F_{12}^{(3)}$, where

$$F_t^{(3)}(X$$

thus in these cases The
Theorem 1 follows from

So we only have to ca
Let us suppose that for
$2 \leq y$ and $|F_t(x, y)| =$
computation using the n
a convergent to β_m with

$$\left|\frac{x}{y} - \beta_m\right.$$

Since we will follow the e
we will number all cons
the role of x and y. The
consideration, mostly th

Using Theorem 3 we ob

$$x - \beta_j y = \pm$$

(The indices of the β_i's

For $m = 2$ we choose k
calculate

$$\frac{7}{6}\left|\frac{\beta}{(\beta_m - \beta}\right.$$

yields $|F_t(x-y, x+2y)| = 27$. On the other hand, let $(x', y') \in \mathbb{Z}^2$ with $|F_t(x', y')| = 27$. One finds that $F_t(x', y') \equiv (x' - y')^2 \equiv 0 \pmod 3$, thus $x' \equiv y' \pmod 3$ and one obtains $(x, y) = \left(\frac{2x'+y'}{3}, \frac{-x'+y'}{3}\right) \in \mathbb{Z}^2$ with $|F_t(x,y)| = 1$. So there is a bijection between the integral solutions of $|F_t(X,Y)| = 1$ and those of $|F_t(X,Y)| = 27$, thus it suffices to investigate only the first equation.

For $t \in \{0, 5\}$, F_t factors into two "simple" cubic forms $F_0 = F_{-3}^{(3)} F_3^{(3)}$ and $F_5 = F_{-2}^{(3)} F_{12}^{(3)}$, where

$$F_t^{(3)}(X,Y) = X^3 - tX^2Y - (t+3)XY^2 - Y^3,$$

thus in these cases Theorem 1 follows from Theorem 2 in [Th2]. For $t \geq 89$, Theorem 1 follows from Corollary 1 in [LPV].

So we only have to care about the cases $t \in T_0 := \{-1, 1, 2, 3, 4\}$ and $6 \leq t \leq 88$. Let us suppose that for such a t there is some $(x, y) \in \mathbb{Z}^2$ with $-\frac{y}{2} < x \leq y$, $2 \leq y$ and $|F_t(x,y)| = 1$. Theorem 1.a) of [LPV] and, for $t \in T_0$, an analogous computation using the numerical values of the roots β_i of P show that $\frac{x}{y}$ must be a convergent to β_m with $m \in \{2, 3\}$ and

$$\left|\frac{x}{y} - \beta_m\right| < \frac{c_1}{y^6} \quad \text{with} \quad c_1 = \begin{cases} 0.082 & \text{if } m = 2, \\ 0.494 & \text{if } m = 3. \end{cases}$$

Since we will follow the exposition of Bilu & Hanrot [BH] to obtain Baker's bound, we will number all constants c_i according to that paper, but we will interchange the role of x and y. The constants will be chosen to hold for all values of t under consideration, mostly they arise from the case $t = -1$, as e.g. for

$$\min_{1 \leq i < j \leq 6} |\beta_i - \beta_j| > c_2 = 0.4646.$$

Using Theorem 3 we obtain for $1 \leq j \leq 6$ that

$$x - \beta_j y = \pm \beta_j^{b_1} \beta_{j+1}^{b_2} \beta_{j+3}^{b_3} \beta_{j+4}^{b_4} \varepsilon^{(-1)^{j+1} b_5} \quad \text{with} \quad 3b_i \in \mathbb{Z}. \tag{15}$$

(The indices of the β_i's are to be taken (mod 6).) From Siegel's identity we get

$$\left| \frac{\beta_m - \beta_k}{\beta_m - \beta_l} \, \frac{x - \beta_l y}{x - \beta_k y} - 1 \right| \leq \frac{c_3}{y^6}. \tag{16}$$

For $m = 2$ we choose $k = 6$, $l = 4$, and for $m = 3$ we take $k = 1$, $l = 5$ and calculate

$$\frac{7}{6} \left| \frac{\beta_l - \beta_k}{(\beta_m - \beta_l)(\beta_m - \beta_k)} \right| c_1 \leq c_3 = \begin{cases} 0.0598 & \text{if } m = 2, \\ 0.71 & \text{if } m = 3. \end{cases}$$

Inserting (15) into (16), our choice of k and l makes ε disappear, and using $\frac{\beta_2-\beta_6}{\beta_2-\beta_4} = -\beta_6$ we arrive for $m = 2, 3$ at the linear forms

$$\begin{aligned}\Lambda_m = \log|\beta_{m-2}^3| + 3b_1 \log\left|\frac{\beta_{m+2}}{\beta_{m-2}}\right| + 3b_2 \log\left|\frac{\beta_{m+3}}{\beta_{m-1}}\right| \\ + 3b_3 \log\left|\frac{\beta_{m-1}}{\beta_{m+1}}\right| + 3b_4 \log\left|\frac{\beta_m}{\beta_{m+2}}\right|.\end{aligned} \tag{17}$$

Note that we have to use a factor 3 to clear the probable denominators of the b_i's. Now we get

$$|\Lambda_m| < c_4 y^{-6} \qquad \text{with } c_4 = \begin{cases} 0.25 & \text{for } m = 2, \\ 3.00 & \text{for } m = 3. \end{cases}$$

Taking absolute values and logarithms of (15) we get a system of linear equations for the b_i's with matrix

$$\begin{pmatrix} L_1 & L_2 & L_4 & L_5 & \log(\varepsilon) \\ L_2 & L_3 & L_5 & L_6 & -\log(\varepsilon) \\ L_3 & L_4 & L_6 & L_1 & \log(\varepsilon) \\ L_4 & L_5 & L_1 & L_2 & -\log(\varepsilon) \\ L_5 & L_6 & L_2 & L_3 & \log(\varepsilon) \\ L_6 & L_1 & L_3 & L_4 & -\log(\varepsilon) \end{pmatrix}, \tag{18}$$

where we put $L_i := \log|\beta_i|$ as in the proof of Lemma 2. Delete the m-th row of this matrix and denote its inverse by A. Following the "third observation" of [BH], we have

$$B := \max\{3|b_i| \mid 1 \le i \le 5\} \le c_5 \log(y) + c_6,$$

where for both $m = 2, 3$ we calculate

$$c_5 = c_7 = 8.25 \qquad \text{and} \qquad c_6 = c_8 = 6.36.$$

Since all b_i's are real, we have $b_{r+1} = 0$ and $B = B'$ with the notations of [BH]. Finally, for $m = 2, 3$ we arrive at

$$|\Lambda_m| < c_9 \exp(-c_{10} B) \qquad \text{with } c_9 = 307 \text{ and } c_{10} = 0.727. \tag{19}$$

Let $h(\cdot)$ denote the absolute logarithmic height of algebraic numbers. For $-1 \le t \le 88$ we calculated that

$$h(\beta_i^3) = 3h(\beta_i) = \frac{1}{2}\log\left(\frac{\beta_6}{\beta_3}\right) < 3$$

and

$$h\left(\frac{\beta_j}{\beta_{j+2}}\right) = \frac{1}{6}\log\left(-\frac{\beta_1\beta_6}{\beta_3\beta_4}\right) < 2.$$

Using the bound of Baker & Wüstholz (as stated in Theorem 2.3.1 of [BH]), we get for the linear forms Λ_m of (17)

$$|\Lambda_m| > \exp(-c_{11}\log B) \qquad \text{with } c_{11} = 5.042 \cdot 10^{30}.$$

Checking this lower b

$B = $

Although we made
involved algebraic nun
Baker & Davenport [
bounds to more mana
the continued fraction
Schulenberg [PSch] an
complete solution of T
linear form in logarith
numerical diophantine
find the solutions corr
another reduction tec
for solutions x and y
reduction (see Pethő [
step we need to compu
precision.

The essential new
not only one but $r -$
r algebraic numbers.
transformed into a sys
To any such inequality
can be applied. Moreo
with a constant Y_3, car
subspace. With this ide

After these historic
our situation. Remark
will not indicate this e
which we obtain from

and

λ_i

where $k(j) = j$ if $1 \le$
that

and put

Checking this lower bound against the upper bound given in (19) yields

$$B = \max\{3|b_i| \mid 1 \le i \le 5\} < B_0 = 5.225 \cdot 10^{32}. \tag{20}$$

Although we made use of the special nature of the number fields K and the involved algebraic numbers, the obtained upper bound for B is very large. It was Baker & Davenport [BD] who first developed techniques to reduce these large bounds to more manageable ones. Their method was based on computations of the continued fraction expansion of certain real numbers. Ellison [El], Pethő & Schulenberg [PSch] and Tzanakis & de Weger [TW] adapted their method for a complete solution of Thue equations. All of them used only the information of one linear form in logarithms of algebraic numbers. They used different techniques of numerical diophantine approximation to reduce the initial very large bound. To find the solutions corrresponding to exponents below the reduced bound one needs another reduction technique. First one converts the bound for B into a bound for solutions x and y by using relation (15) and applies the continued fraction reduction (see Pethő [P] or Tzanakis & de Weger [TW]). For the second reduction step we need to compute the zeros associated to the given binary form with high precision.

The essential new idea of Bilu & Hanrot [BH] is that Thue equations imply not only one but $r-1$ independent inequalities for linear forms in logarithms of r algebraic numbers. Using elementary linear algebra, these inequalities can be transformed into a system of $r-1$ inequalities, each involving only two unknowns. To any such inequality, the very simple reduction method of Baker & Davenport can be applied. Moreover, the exponents associated to solutions for which $|y| > Y_3$, with a constant Y_3, can be located on a line instead of an $(r-1)$-dimensional linear subspace. With this idea, Bilu & Hanrot solved Thue equations of degree 19 and 33.

After these historical notes we show how the Bilu & Hanrot reduction works in our situation. Remark that all the parameters below depend on t and m, but we will not indicate this explicitly. Let $A = (a_{ij})_{1\le i,j\le 5}$ be the inverse of the matrix which we obtain from the matrix (18) by removing its m-th row. Put

$$\delta_i = \sum_{j=1}^{5} a_{ij} \qquad 1 \le i \le 5$$

and

$$\lambda_i = \sum_{j=1}^{5} a_{ij} \log|\beta_m - \beta_{k(j)}| \qquad 1 \le i \le 5,$$

where $k(j) = j$ if $1 \le j < m$, and $k(j) = j+1$ if $m \le j \le 5$. Let u be chosen such that

$$|\delta_u| = \max_{1\le i\le 5} |\delta_i|$$

and put

$$\delta_{ui} = \frac{\delta_i}{\delta_u}, \qquad \lambda_{ui} = \frac{\delta_i\lambda_u - \delta_u\lambda_i}{\delta_u}$$

for all $1 \le i \le 5$, $i \ne u$. Then we obtain (c.f. Proposition 2.4.1. of [BH]) the following system of inequalities

$$\begin{aligned} |(3b_i) - (3b_u)\delta_{ui} + 3\lambda_{ui}| &\le c_{14}\exp(-c_{15}B), \qquad 1 \le i \le 5,\ i \ne u \\ B = \max\{3|b_j| \mid 1 \le j \le 5\} &\le B_0 = 5.225 \cdot 10^{32} \end{aligned} \tag{21}$$

with $c_{15} = \frac{6}{c_5} = c_{10} = 0.727$ and $c_{14} = \begin{cases} 413 & \text{if } m = 2, \\ 2474 & \text{if } m = 3. \end{cases}$

To solve (21) we use the method of [BH], Section 2.4.2. Consider the subsystem

$$\begin{aligned} |(3b_i) - (3b_u)\delta_{ui} + 3\lambda_{ui}| &\le c_{14}\exp(-c_{15}B) \\ B &\le B_0 = 5.225 \cdot 10^{32} \end{aligned}$$

of (21) for a single $i \ne u$. Let κ be a not very large number (in our computations we took $\kappa = 10$) and compute the convergents p_n/q_n of the continued fraction expansion of δ_{ui} until $q_n > \kappa B_0$. If $\|q_n\lambda_{ui}\| > \kappa^{-1}$, where $\|\cdot\|$ denotes the distance to the nearest integer, then we obtain a new estimate for B:

$$B \le c_{15}^{-1}\Big(\log q_n + \log\frac{c_{14}}{\|q_n\lambda_{ui}\| - \kappa^{-1}}\Big).$$

We can of course iterate this procedure until the new bound can not be reduced further.

We implemented the above procedure for our sextic Thue equations in MAPLE. We did not use the absolute bounds for $c_1, \ldots, c_{14}$, but computed for each case their actual values. The reason is that this caused only minor extra programming work, but the reduced bound became in most cases considerably smaller.

We found $u = 1$ for both $m = 2$ and $m = 3$. We performed the Baker & Davenport reduction to all four systems of inequalities of type (21) and took the smallest reduced bound as the new bound for B. The direction, i.e. the index for which we obtained the best bound varied depending on t. After the reduction we obtained in all cases $B \le 6$. The final upper bound decreased with t. We achieved $B \le 1$ for $t \ge 10$ for both $m = 2, 3$, and even $B = 0$ for $m = 2$ and $t \ge 46$. To locate the possible solutions below these bounds we used Proposition 2.5.1 of [BH]. Remark that $Y_3 = 1$ for our Thue equations. We never found a solution with $|y| \ge 2$, which finishes the proof for this case. The only solutions with $y = 1$ are $(x, y) = (0, 1), (1, 1)$, thus the proof of Theorem 1 is completed.

[B] Baker, A., Con
Trans. Roy. So

[BD] Baker, A., Dav
J. Math. Oxfor

[BH] Bilu, Y., Hanr
60 (1996), 373-

[El] Ellison, W.J.,
Th. Nombres,
No. 11.

[Er] Erdős, P., Arit
(1953), 416–42

[G1] Gras, M.N., Su
gene. Ann. Sci.

[G2] — Familles d'
Math. Fac. Sci.

[L] Lettl, G., Fin
Cambridge Phi

[LP] Lettl, G., Peth
Abh. Math. Se

[LPV] Lettl, G., Pet
Amer. Math. S

[MPL] Mignotte, M.,
$x^3 - (n-1)x^2$

[NP] Nakamula, K.,
ings, 409–421.

[N] Narkiewicz, W
ed.). Springer,

[P] Pethő, A., On
103–109.

[PSch] Pethő, A., Sch
Debrecen 34 (

[Th1] Thomas, E., F
Angew. Math.

[Th2] — Complete
Theory 34 (19

References

[B] Baker, A., Contributions to the theory of Diophantine equations I and II. Philos. Trans. Roy. Soc. London, Ser. A 263 (1968), 173–208.

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

[BH] Bilu, Y., Hanrot, G., Solving Thue equations of high degree. J. Number Theory 60 (1996), 373–392.

[El] Ellison, W.J., Recipes for solving diophantine problems by Baker's method. Sem. Th. Nombres, Talence: Lab. Theorie Nombres, C.N.R.S. (1970–1971), Exp. No. 11.

[Er] Erdős, P., Arithmetical properties of polynomials. J. London Math. Soc. (1) 28 (1953), 416–425.

[G1] Gras, M.N., Sur les corps cubiques cycliques dont l'anneau des entiers est monogene. Ann. Sci. Univ. Besançon 3 (6) (1973).

[G2] — Familles d'unités dans les extensions cycliques réelles de degré 6 de $\mathbb{Q}$. Publ. Math. Fac. Sci. Besançon 2 (1984–1986).

[L] Lettl, G., Finding fundamental units in algebraic number fields. Math. Proc. Cambridge Philos. Soc. 98 (1985), 383–388.

[LP] Lettl, G., Pethő, A., Complete solution of a family of quartic Thue equations. Abh. Math. Seminar Hamburg 65 (1995), 365–383.

[LPV] Lettl, G., Pethő, A., Voutier, P., Simple families of Thue inequalities. Trans. Amer. Math. Soc. (to appear).

[MPL] Mignotte, M., Pethő, A., Lemmermeyer, F., On the family of Thue equations $x^3 - (n-1)x^2y - (n+2)xy^2 - y^3 = k$. Acta Arithm. 76 (1996), 245–269.

[NP] Nakamula, K., Pethő, A., Squares in binary recurrence sequences. In these poceedings, 409–421.

[N] Narkiewicz, W., Elementary and Analytic Theory of Algebraic Numbers (2nd ed.). Springer, 1990.

[P] Pethő, A., On the resolution of Thue inequalities. J. Symbolic Comput. 4 (1987), 103–109.

[PSch] Pethő, A., Schulenberg, R., Effektives Lösen von Thue Gleichungen. Publ. Math. Debrecen 34 (1987), 189–196.

[Th1] Thomas, E., Fundametal units for orders in certain cubic number fields. J. Reine Angew. Math. 310 (1979), 33–55.

[Th2] — Complete solutions to a family of cubic Diophantine equations. J. Number Theory 34 (1990), 235–250.

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

Addresses of the authors:

Günter Lettl
Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
A-8010 Graz
Austria

E-mail: guenter.lettl@kfunigraz.ac.at

Attila Pethő
Institute of Mathematics and Informatics
Kossuth Lajos University
H-4010 Debrecen, P.O. Box 12
Hungary

E-mail: pethoe@math.klte.hu

Paul Voutier
Department of Mathematics
University of Colorado
Boulder, CO 80309
U.S.A.

E-mail: voutier@euclid.colorado.edu

On the a
fields a

Günter

1991 Mathematics Subj

In a recent paper [LP

where, for a paramete

$F_t(X,Y$

Using the automorph
lutions $(x,y) \in \mathbb{Z}^2$ wi
proved there, it follow
family of Thue equati

are $(0,1)$ and $(1,1)$.
this result, but one ca
successfully applied t
theorem, which exten

Theorem 1. *For $t \in$*

with $-\frac{y}{2} < x \le y$ are

* Supported partly
logical cooperatio
Research Grant N

Offprint from: Number T