On Quartic Thue Equations with Trivial Solutions

R. J. Stroeker

Mathematics of Computation, Vol. 52, No. 185 (Jan., 1989), 175-187.

Stable URL:
http://links.jstor.org/sici?sici=0025-5718%28198901%2952%3A185%3C175%3AOQTEWT%3E2.0.CO%3B2-S

Mathematics of Computation is currently published by American Mathematical Society.

MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 175–187

On Quartic Thue Equations with Trivial Solutions

By R. J. Stroeker

Abstract. Let $\mathbf{K}$ be a quartic number field with negative absolute discriminant and let $\mathbf{L} = \mathbf{Q}(\sqrt{d})$ be its real quadratic subfield, with $d \equiv 3 \pmod 4$. Moreover, assume $\mathbf{K}$ to be embedded in the reals. Further, let $\xi > 1$ generate the subgroup of units relative to $\mathbf{L}$ in the group of positive units of $\mathbf{K}$. Under certain conditions, which can be explicitly checked, and for suitable linear forms $X(u,v)$ and $Y(u,v)$ with coefficients in $\mathbf{Z}[\sqrt{d}]$, the diophantine equation

$$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X(u,v) + Y(u,v)\xi^2) = 1,$$

which is a quartic Thue equation in the indeterminates u and v, has only trivial solutions, that is, solutions given by $XY = 0$.

Information on a substantial number of equations of this type and their associated number fields is incorporated in a few tables.

1. Introduction. A homogeneous polynomial in two indeterminates x and y is commonly known as a binary form. Given such a binary form f of degree at least three with rational integer coefficients, and a fixed rational integer k, the equation

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

is called a *Thue equation.* Thue equations are examples of polynomial diophantine equations, and the usual object of study is to gather information on the existence, the number and the actual values of integer solutions. If $f \in \mathbf{Z}[x,y]$ is irreducible, then Eq. (1) is an example of a *norm form equation.* A justification for this name may be found in the representation of f as

$$f(x,y) = \mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(x - y\xi), \tag{2}$$

where ξ is a root of the equation $f(t,1) = 0$ and $\mathbf{K}$ is the number field generated by ξ over the rationals $\mathbf{Q}$. The field $\mathbf{K}$ is often referred to as a field *associated* with the Thue equation (1).

In order to solve a given diophantine equation of polynomial type, it often proves sufficient to solve finitely many Thue equations which can be explicitly derived from the original diophantine equation. This technique has a long history (see [6]), and even today it is used extensively (see [5], [12], [15] and [17]).

Thue equations have been solved in a variety of ways. Axel Thue showed in 1909 (see [14]) that for irreducible f, Eq. (1) has at most a finite number of solutions in rational integers x and y. His proof is ineffective in the sense that it does not give any informaton on the size of the solutions or their number. His techniques are rooted in the theory of diophantine approximation. Later Gel'fond and others

Received March 31, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D25, 11R27.

refined and extended these approximation methods and in the sixties Alan Baker built upon the foundation laid by Gel'fond the impressive structure of his theory of linear forms in the logarithms of algebraic numbers. This so-called *Gel'fond-Baker method* provides a powerful tool to solve, at least in principle, Thue equations effectively by explicitly giving upper bounds for their solutions (see [1]). But mostly these bounds are so large as to be virtually useless for the purpose of actually finding all solutions. Only recently have techniques been developed to adapt the Gel'fond-Baker method to Thue equations so that in certain cases the upper bounds can be reduced to manageable proportions (see [2] and [16]).

Another route was taken by Mordell, Nagell and others and has a distinct algebraic flavor. Considering (1) as a norm form equation associated with an appropriate number field $\mathbf{K}$, divisibility techniques and congruence considerations, followed, if necessary, by Skolem's p-adic method, often result in a complete solution (see [13]). However, a drawback of this method is that in order to solve each individual Thue equation, a great many hard calculations need to be performed. This is true for both analytic and algebraic methods of solution. Only when dealing with a Thue equation which happens to have no solutions at all, this lack of solutions can usually be established in a rather trivial manner.

In this paper a substantial class of Thue equations is considered, equations which do admit solutions but only the obvious ones. These equations are associated with quartic fields $\mathbf{K}$ of negative absolute discriminant. To be more precise, we consider certain equations of type

$$\text{Norm}_{\mathbf{K}/\mathbf{Q}}(x - y\xi) = 1, \tag{3}$$

where $\mathbf{K} = \mathbf{Q}(\xi)$ and where x and y are linear forms in u and v with coefficients in the ring of integers of the unique real quadratic subfield $\mathbf{L}$ of $\mathbf{K}$. We shall give a description of a method to solve such equations effectively. Use is made of the divisibility properties of the elements of certain recurrence sequences associated with the subfield $\mathbf{L}$. An important feature of this method is the avoidance of a construction of a set of fundamental units for $\mathbf{K}$. A few specific cases shall be worked out in detail. In two tables the results on a series of selected equations and associated fields are listed. A sample of equations, complete solutions of which are provided, is given below:

$$(u+v)^4 - 12u^2v^2 = 1, \qquad u^4 - 24uv^3 - 24v^4 = 1,$$
$$u^4 - 6u^2v^2 - 3v^4 = 1, \qquad u^4 - 30u^2v^2 - 27v^4 = 1.$$

2. The Associated Number Fields. In this section we shall describe the number field $\mathbf{K}$ and its relevant properties, with special emphasis on the unit structure of $\mathbf{K}$.

Throughout the sequel, $\mathbf{K}$ shall be a number field of absolute degree 4, with a real quadratic subfield $\mathbf{L} = \mathbf{Q}(\sqrt{d})$, where d is squarefree and $d \equiv 3 \pmod 4$. Moreover, it is assumed that $\mathbf{K}$ is not totally real, so that the absolute discriminant $\mathscr{D}_{\mathbf{K}}$ of $\mathbf{K}$ is negative.

The unit group of $\mathbf{L}$ is denoted by $\mathscr{U}_{\mathbf{L}} = \langle \pm 1 \rangle \times \mathscr{U}_{\mathbf{L}}^+$, where $\mathscr{U}_{\mathbf{L}}^+ = \langle \varepsilon \rangle$ with fundamental unit $\varepsilon > 1$ of $\mathbf{L}$. Likewise, the unit group of $\mathbf{K}$ is denoted by $\mathscr{U}_{\mathbf{K}} = \langle \pm 1 \rangle \times \mathscr{U}_{\mathbf{K}}^+$, where $\mathscr{U}_{\mathbf{K}}^+$ is a free abelian group of rank two, generated by, say the

fundamental units ε_1 and ε_2. Now define $\mathscr{U}^+_{\mathbf{K/L}} = \{\eta \in \mathscr{O}_{\mathbf{K}} \mid \mathrm{Norm}_{\mathbf{K/L}}(\eta) = 1, \eta > 0\}$, where $\mathscr{O}_{\mathbf{K}}$ denotes the ring of integers of $\mathbf{K}$. Obviously, this relative unit group $\mathscr{U}^+_{\mathbf{K/L}}$ has rank 1. Assume $\mathscr{U}^+_{\mathbf{K/L}}$ is generated by $\xi > 1$, so that $\mathscr{U}^+_{\mathbf{K/L}} = \langle\xi\rangle$. Then ξ satisfies the equation

$$x^2 - \theta x + 1 = 0, \tag{4}$$

where $\theta := \xi + \xi^{-1} \in \mathscr{O}_{\mathbf{L}}$, the ring of integers of $\mathbf{L}$.

Define $a, b \in \mathbf{Z}$ by

$$\theta = a + b\sqrt{d}, \tag{5}$$

and let $\overline{\theta} = a - b\sqrt{d}$ be its $\mathbf{L}$-conjugate. Since ξ is real and because $\mathbf{K}$ is not totally real, we have

$$\overline{\theta}^2 - 4 < 0 < \theta^2 - 4.$$

This immediately implies that

$$|a - b\sqrt{d}| < 2 \quad \text{with } a \geq 1 \text{ and } b \geq 1, \tag{6}$$

as $\theta > 0$. Note that the minimal polynomial for ξ is the monic reciprocal polynomial

$$x^4 - sx^3 + tx^2 - sx + 1, \quad \text{with } s = 2a \text{ and } t = a^2 - db^2 + 2, \tag{7}$$

so that Eq. (3) becomes

$$x^4 - sx^3y + tx^2y^2 - sxy^3 + y^4 = 1. \tag{8}$$

Equation (8) represents the type of diophantine equation to be investigated in this paper.

Let $\eta \in \mathscr{U}^+_{\mathbf{K/L}} = \langle\xi\rangle$, so that $\eta = \xi^k$ for some $k \in \mathbf{Z}$, and suppose X and Y are linear forms in u and v with coefficients in $\mathscr{O}_{\mathbf{L}}$. Then

$$\mathrm{Norm}_{\mathbf{K/Q}}(X(u,v) + Y(u,v)\eta) = 1 \tag{9}$$

is a Thue equation in the rational integer variables u and v. If it is assumed that $\{\varepsilon, \xi\}$ is a set of fundamental units for $\mathscr{O}_{\mathbf{K}}$—recall that ε is a fundamental unit of $\mathscr{O}_{\mathbf{L}}$—then (9) may be rewritten as

$$X(u,v) + Y(u,v)\xi^k = \pm\varepsilon^m\xi^n \tag{10}$$

with $m, n \in \mathbf{Z}$. We may drop the $\pm$ sign in (10) without loss of generality, by adjusting the signs of X and Y. Also assume $k \geq 1$. As the conjugacy map, characterized by $\xi \mapsto \xi^{-1}$, leaves the elements of $\mathbf{L}$ unchanged, the conjugate equation to (10) is

$$X(u,v) + Y(u,v)\xi^{-k} = \varepsilon^m\xi^{-n},$$

so that,

$$-X(u,v)\varepsilon^{-m} = \frac{\xi^{n-k} - \xi^{-n+k}}{\xi^k - \xi^{-k}}, \qquad Y(u,v)\varepsilon^{-m} = \frac{\xi^n - \xi^{-n}}{\xi^k - \xi^{-k}}. \tag{11}$$

The elements $s_n := (\xi^n - \xi^{-n})/(\xi - \xi^{-1})$ of the sequence $(s_n)_{n\in\mathbf{Z}}$ are $\mathbf{L}$-integers and system (11) reads in terms of the elements of (s_n):

$$-X(u,v)\varepsilon^{-m} = \frac{s_{n-k}}{s_k}, \qquad Y(u,v)\varepsilon^{-m} = \frac{s_n}{s_k}. \tag{12}$$

Obvious solutions are given by $n = 0$ and $n = k$, because $s_0 = 0$, so that $X(u,v) = 0$ and $Y(u,v) = \varepsilon^m$ or $X(u,v) = \varepsilon^m$ and $Y(u,v) = 0$. These solutions shall be referred to as the *trivial solutions.* Clearly, it depends on the divisibility properties of the elements of the sequence (s_n) whether any nontrivial solutions exist. In the special case that 2 exactly divides $k (2 \| k)$, we can give information on the exponent to which XY is divisible by the unique prime ideal divisor of 2 in $\mathcal{O}_{\mathbf{L}}$, provided $XY \neq 0$.

A precise formulation is given in the following theorem.

THEOREM 1. *Let $\xi > 1$ be a real root of the equation*

$$x^4 - sx^3 + tx^2 - sx + 1 = 0,$$

where $s = 2a$, $t = a^2 - db^2 + 2$, and a, b, and d are any three **odd** *positive integers such that*

- *d is squarefree and $d \equiv 3 \pmod 4$,*
- *$|a - b\sqrt{d}| < 2$.*

Further, $\mathbf{K} = \mathbf{Q}(\xi)$ and $\mathbf{L} = \mathbf{Q}(\sqrt{d})$ is the real quadratic subfield of $\mathbf{K}$.

Suppose that ξ generates the relative unit group $\mathcal{U}^+_{\mathbf{K}/\mathbf{L}}$, and let $\{\varepsilon, \xi\}$ be a fundamental set of units for $\mathbf{K}$.

If $\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X + Y\xi^k) = 1$, with $2 \| k$ and $X, Y \in \mathcal{O}_{\mathbf{L}}$, then either $XY = 0$, or $0 \neq XY$ is exactly divisible by an odd power of the unique prime ideal divisor $\wp$ of 2 in $\mathcal{O}_{\mathbf{L}}$.

Remark 1. Before setting out to properly prove this theorem, the following remarks may be helpful to the reader.

- It is immediately clear that for any squarefree positive $d \equiv 3 \pmod 4$ there are infinitely many odd a and b with $|a - b\sqrt{d}| < 2$. Also, for such d there is a unique prime ideal divisor $\wp$ of 2 in $\mathcal{O}_{\mathbf{L}}$ and $\wp^2 = (2)$.
- At first glance, the condition concerning the free abelian unit group of $\mathbf{K}$ being generated by ε and ξ might appear rather restrictive. However, as it turns out, ε and ξ "nearly always" satisfy this condition. In Section 4 we shall describe an algorithm for checking this condition.
- In the applications (Section 5) the linear forms X and Y are always chosen in such a way that the product XY is forced to vanish. This leads to equations with trivial solutions only.
- The method can most likely be extended to include

  $$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X + Y\xi^k) = m,$$

  with $m > 1$, provided extra information is available on the prime divisors of m and the class number of $\mathbf{K}$.

3. Proof of Theorem 1. This section is devoted to a proof of Theorem 1.

The conditions placed on a, b and d guarantee the irreducibility of the defining equation of ξ over $\mathbf{Q}$. This can be seen by applying Eisenstein's criterion with prime 2 to the polynomial $f(x + 1)$, where $f(x)$ denotes the defining polynomial for ξ.

Starting with

$$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X + Y\xi^k) = 1$$

with $k \equiv 2 \pmod 4$ and $X, Y \in \mathscr{O}_{\mathbf{L}}$, we recall (see (12))

$$-X\varepsilon^{-m} = \frac{s_{n-k}}{s_k}, \qquad Y\varepsilon^{-m} = \frac{s_n}{s_k}. \tag{13}$$

Clearly, the sequence $(s_n)_{n\in\mathbf{Z}}$ defined by $s_n := (\xi^n - \xi^{-n})/(\xi - \xi^{-1})$ should be investigated. We also define the related sequence $(t_n)_{n\in\mathbf{Z}}$ by $t_n := \xi^n + \xi^{-n}$.

LEMMA 1. *The sequences (s_n) and (t_n) are as defined above.*

1. *For all $n \in \mathbf{Z}$, $s_n, t_n \in \mathscr{O}_{\mathbf{L}}$.*
2. *Let $\wp$ be the prime ideal divisor of 2 in $\mathscr{O}_{\mathbf{L}}$; then*
   - *if n is odd then $\wp \nmid s_n$ and $\wp \,\|\, t_n$,*
   - *if $n \equiv 2 \pmod 4$ then $\wp \,\|\, s_n$ and $\wp^3 \,\|\, t_n$,*
   - *if $n = 2^e n'$ with odd n' and $e \geq 2$ then $\wp^{2e} \,\|\, s_n$ and $\wp^2 \,\|\, t_n$.*

Proof. The following recurrence relations are immediate consequences of the definitions of the sequences (s_n) and (t_n)—recall that $\theta = \xi + \xi^{-1} = a + b\sqrt{d}$:

$$s_0 = 0,\ s_1 = 1, \text{ and } s_{n+1} = \theta s_n - s_{n-1} \quad \text{for } n = 1, 2, \ldots ; \tag{14}$$

$$t_0 = 2,\ t_1 = \theta, \text{ and } t_{n+1} = \theta t_n - t_{n-1} \quad \text{for } n = 1, 2, \ldots . \tag{15}$$

Now $\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(\theta) = a^2 - db^2 \equiv 2 \pmod 4$ and $\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(\theta^2 - 2) = (a^2 + db^2 - 2)^2 - 4da^2b^2 \equiv 8 \pmod{16}$. It follows that $\wp \,\|\, \theta$ and $\wp^3 \,\|\, (\theta^2 - 2)$.

Since (14) and (15) imply that for $n = 2, 3, \ldots$

$$s_{n+2} = (\theta^2 - 2)s_n - s_{n-2} \quad \text{and} \quad t_{n+2} = (\theta^2 - 2)t_n - t_{n-2},$$

the stated divisibility properties of t_n by powers of $\wp$ follow easily.

If $n = 2^e n'$ with $e \geq 1$ and odd n', because of $s_{2n} = s_n t_n$ for all n, it is readily seen that

$$s_n = s_{n'} \prod_{i=0}^{e-1} t_{2^i},$$

and the remaining divisibility properties of s_n follow immediately. This completes the proof of the lemma. □

We continue the proof of Theorem 1.

Returning to (13), because $s_{n-k}/s_k,\ s_n/s_k \in \mathscr{O}_{\mathbf{L}}$ and $\wp \,\|\, s_k$ as $k \equiv 2 \pmod 4$, we see that n has to be even.

If $2 \,\|\, n$, then $\wp \,\|\, s_n$ and hence $\wp \nmid s_n/s_k$. But $n - k \equiv 0 \pmod 4$. So if $n \neq k$, then $n - k = 2^e n'$ with $e \geq 2$ and odd n'. From Lemma 1 it then follows that $\wp^{2e} \,\|\, s_{n-k}$ and hence $\wp^{2e-1} \,\|\, s_{n-k}/s_k$. On the other hand, if $4 \mid n$ and $n \neq 0$, we put $n = 2^e n'$ with $e \geq 2$ and odd n', and consequently $\wp^{2e-1} \,\|\, s_n/s_k$. But $\wp \nmid s_{n-k}/s_k$ as $n - k \equiv 2 \pmod 4$. Hence, if $XY \neq 0$, then XY is exactly divisible by an odd power of $\wp$, and the proof of Theorem 1 is completed. □

For applications of Theorem 1 we refer the reader to Section 5.

4. Generators of the Positive Unit Group. In this section the set $\{\varepsilon, \xi\}$ of $\mathbf{K}$-units will be examined in an attempt to find verifiable conditions that need to be imposed in order to use these units as fundamental units for $\mathbf{K}$. As usual, ε is a fundamental unit of $\mathbf{L}$ and ξ is defined by (6) and (7).

First assume that ξ is a generator of the relative unit group $\mathscr{U}^+_{\mathbf{K}/\mathbf{L}}$, i.e., ξ is not a perfect power of a unit $\eta > 1$. Then ξ may serve as one of the two generators of

$\mathscr{U}_{\mathbf{K}}^{+}$. As a second generator we may choose ε, *provided* $\sqrt{\varepsilon}$ and $\sqrt{\varepsilon\xi}$ do not belong to $\mathbf{K}$ (see [7], [8]). The next theorem asserts that neither ε nor $\varepsilon\xi$ is a perfect square in $\mathscr{O}_{\mathbf{K}}$. The following notation will be adopted for the minimal polynomial of a unit $\eta \in \mathscr{O}_{\mathbf{K}}$:

$$x^4 - s_\eta x^3 + t_\eta x^2 - u_\eta x + 1. \tag{16}$$

THEOREM 2. *Let a, b and d be odd rational integers restricted by the conditions formulated in Theorem* 1. *Further, let $\varepsilon > 1$ be a generator of $\mathscr{U}_{\mathbf{L}}^{+}$ and let $\xi > 1$ be a generator of $\mathscr{U}_{\mathbf{K/L}}^{+}$ with minimal polynomial of type* (16) *and $s_\xi = u_\xi = 2a$, $t_\xi = a^2 - db^2 + 2$.*

Then ξ and ε generate $\mathscr{U}_{\mathbf{K}}^{+}$.

Proof. First consider the case of ε. Let $x^2 - 2wx + 1$ be the minimal polynomial of ε. Then the rational integer w is positive and $w > 1$ as $\varepsilon > 1$. Further, $\varepsilon = w + \sqrt{w^2 - 1}$. Now let $\varepsilon_1 := \sqrt{\varepsilon}$; then $x^4 - 2wx^2 + 1$ is the minimal polynomial for ε_1, for $\varepsilon_1 \notin \mathscr{O}_{\mathbf{L}}$ as ε is a fundamental unit of $\mathbf{L}$. Then obviously all field conjugates of ε_1 must be real, and this means that $\varepsilon_1 \notin \mathbf{K}$.

Next it will be shown that $\sqrt{\varepsilon\xi}$ does not belong to $\mathbf{K}$. As usual, let $\theta := \xi + \xi^{-1} = a + b\sqrt{d}$. The field conjugates of $\varepsilon\xi$ are $\varepsilon\xi$, $\varepsilon\xi^{-1}$, $\varepsilon^{-1}\overline{\xi}$, $\varepsilon^{-1}\overline{\xi}^{-1}$, where $\xi, \xi^{-1}, \overline{\xi}, \overline{\xi}^{-1}$ are the field conjugates of ξ. If $\overline{\theta}$ denotes $\overline{\xi} + \overline{\xi}^{-1}$, then

$$\begin{aligned} s_{\varepsilon\xi} &= \theta\varepsilon + \overline{\theta}\varepsilon^{-1} \equiv 2 \pmod 4, \\ t_{\varepsilon\xi} &= \varepsilon^2 + \varepsilon^{-2} + \theta\overline{\theta} \equiv 0 \pmod 4, \\ u_{\varepsilon\xi} &= \overline{\theta}\varepsilon + \theta\varepsilon^{-1} \equiv 2 \pmod 4, \end{aligned} \tag{17}$$

as is easily checked (see (16)). Now suppose $\varepsilon\xi$ is a perfect square in $\mathbf{K}$. Let $\beta := \sqrt{\varepsilon\xi}$. Then, it is not hard to verify that

$$\begin{aligned} s_{\varepsilon\xi} &= s_\beta^2 - 2t_\beta, \\ t_{\varepsilon\xi} &= t_\beta^2 - 2s_\beta u_\beta + 2, \\ u_{\varepsilon\xi} &= u_\beta^2 - 2t_\beta. \end{aligned}$$

Clearly, all of s_β, t_β and u_β must be even, as $s_{\varepsilon\xi}$, $t_{\varepsilon\xi}$ and $u_{\varepsilon\xi}$ are even. But this contradicts (17), thus completing the proof of the theorem. □

In order to apply the main theorem (Theorem 1), it follows from Theorem 2 that one only has to make sure that ξ given by (7) for suitable values of a, b and d indeed generates $\mathscr{U}_{\mathbf{K/L}}^{+}$. This can be achieved by checking that ξ is not a perfect power in $\mathscr{O}_{\mathbf{K}}$. The following lemmas provide an algorithmic approach to solve this problem. Both lemmas are due to Nakamula—in [8] they are stated without proof and [9] only provides a proof for Lemma 2 below.

The first lemma gives an upper bound for the exponent n in $\xi = \eta^n$ with $\eta \in \mathscr{U}_{\mathbf{K/L}}^{+}$.

LEMMA 2 (NAKAMULA). *If $\xi = \eta^n$ with $\eta \in \mathscr{U}_{\mathbf{K/L}}^{+}$ and $n \in \mathbf{N}$, then*

$$n < \frac{2\log\xi}{\log\left(\sqrt[3]{\frac{|\mathscr{D}|}{4} + 8^3} - 7\right)},$$

where $\mathscr{D}$ is the absolute discriminant of $\mathbf{K}$.

Proof. See [9]. □

The next lemma gives an algorithm for checking possible values of n in $\xi = \eta^n$, providing at the same time a minimal polynomial (16) for η.

LEMMA 3 (NAKAMULA). *Let* $\xi \in \mathscr{U}^+_{\mathbf{K}/\mathbf{L}}$, $\xi > 1$, *and* $n \in \mathbf{N}$. *Put* $\eta := \sqrt[n]{\xi}$ *and* $\alpha := \eta + \eta^{-1}$.

Then $\eta \in \mathbf{K} \cap \mathbf{R}$ *if and only if there are* $s, t \in \mathbf{Z}$ *such that*

$$|s - \alpha| < 2, \qquad t = 2 + \alpha(s - \alpha) \tag{18}$$

and

$$s_\xi = f_n(\alpha) + f_n(s - \alpha), \qquad t_\xi = 2 + f_n(\alpha) \cdot f_n(s - \alpha),$$

where the polynomials $f_k \in \mathbf{Z}[x]$ *are given by the recurrence*

$$f_k(x) = x f_{k-1}(x) - f_{k-2}(x) \quad \text{for } k \in \mathbf{Z},\ f_0(x) = 2,\ f_1(x) = x.$$

Moreover, $s = s_\eta = u_\eta$ *and* $t = t_\eta$ *are the coefficients in the minimal polynomial* (16) *of* η.

Proof. If $\eta \in \mathbf{K} \cap \mathbf{R}$ then η has a defining polynomial of type (7), because ξ has a similar defining polynomial and the field conjugates of η follow immediately from those of ξ. As

$$x^4 - s_\eta x^3 + t_\eta x^2 - s_\eta x + 1 = (x^2 - \alpha x + 1)(x^2 - \overline{\alpha} x + 1)$$

identically, it follows that $s_\eta = \alpha + \overline{\alpha}$, $t_\eta = 2 + \alpha\overline{\alpha}$, where $|\overline{\alpha}| < 2$. Consequently, (18) is satisfied with $s = s_\eta$ and $t = t_\eta$.

On putting $\alpha_n := \xi + \xi^{-1}$, we see that $s_\xi = \alpha_n + \overline{\alpha}_n$ and $t_\xi = 2 + \alpha_n \cdot \overline{\alpha}_n$. Moreover, $\alpha_n = \eta^n + \eta^{-n} =: f_n(\alpha)$. From this the stated properties of the polynomials f_k are easily checked. See also (15).

The converse follows likewise. □

COROLLARY. *If* $\xi \in \mathscr{U}^+_{\mathbf{K}/\mathbf{L}}$, *then* ξ *is never a perfect square.*

This follows immediately from Lemma 3 with $n = 2$ by using parity considerations as in Lemma 2. □

5. Applications and Examples. Let $X = X(u, v)$ and $Y = Y(u, v)$ be linear forms in u and v with coefficients in $\mathscr{O}_\mathbf{L}$. Consider

$$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X + Y\xi^k) = 1$$

with $k \equiv 2 \pmod 4$ (see (9)). This equation may be written as

$$\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(X^2 + XY\theta_k + Y^2) = 1 \tag{19}$$

with $\theta_k := \xi^k + \xi^{-k}$.

On putting $X^2 + XY\theta_k + Y^2 = F + G\sqrt{d}$, Eq. (19) becomes

$$F^2 - dG^2 = 1, \tag{20}$$

which is a quartic Thue equation in u and v, as F and G are binary quadratic forms in u and v with rational integer coefficients.

Application 1.

- Choose odd positive integers a, b and d such that d is squarefree with $d \equiv 3 \pmod 4$ and $|a - b\sqrt{d}| < 2$.

- Then use Lemmas 2 and 3 to check that ξ given by (7) is not a perfect power in $\mathbf{K}$.
- Choose $k \equiv 2 \pmod 4$.
- Next choose linear forms X and Y in $\mathscr{O}_{\mathbf{L}}[u, v]$ such that for all rational integers u and v, $\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(XY)$ is exactly divisible by a power of 4, unless $XY = 0$.

Then the diophantine equation (19) can have no other solutions than the trivial ones, i.e., the solutions given by $XY = 0$. □

Remark 2.

- As $\wp^e \| XY$ is equivalent to
$$2^e \| \mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(XY),$$
Application 1 is a direct consequence of Theorems 1 and 2.
- In order to apply Lemma 2, we need to determine the absolute discriminant $\mathscr{D}$ of the associated field $\mathbf{K}$. This can be done using the techniques and results of Vaughan's paper (see [18]).
Alternatively, if ξ is given by (7), then the discriminant of ξ equals
$$\mathscr{D}(\xi) = 2^6 b^4 d^2 \frac{(a+2)^2 - db^2}{2} \cdot \frac{(a-2)^2 - db^2}{2}$$
and $\mathscr{D}$ divides $\mathscr{D}(\xi)$. Standard techniques can now be used to calculate $\mathscr{D}$ (e.g., see [4]).
- Also note that, if $\alpha := \xi - \xi^{-1}$ and $\xi > 1$, then $\alpha = \sqrt{A + B\sqrt{d}}$ with $A := a^2 + db^2 - 4$, $B := 2ab$ and $\mathbf{K} = \mathbf{Q}(\alpha)$.

Example 1. Let $d = 3$ and $a = b = 1$. Then $\mathbf{K} = \mathbf{Q}(\alpha)$ with $\alpha = \sqrt{2\sqrt{3}}$ and $\theta = \xi + \xi^{-1} = 1 + \sqrt{3}$. Now choose $X = u$, $Y = v$ and $k = 2$ in Eq. (19). Then (20) becomes
$$(u+v)^4 - 12u^2v^2 = 1.$$
Also, for $X = u(2 + \sqrt{3})$, $Y = v$ and $k = 2$, we get from (20)
$$(u-v)^4 + 24uv^3 = 1,$$
an equation which can be found in [10]. In both cases,
$$\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(XY) = \mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(uv) = u^2v^2,$$
so that the norm condition of Application 1 is satisfied. Table 1 tells us that ξ is not a perfect power in $\mathbf{K}$. Consequently, both equations have only trivial solutions, given by $uv = 0$. □

How can one decide whether a given quartic diophantine equation is suitable for application along the lines indicated above? Obviously, the associated field has to be of the right type. But there are also other considerations.

Application 2. Let

$$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(x + y\alpha) = 1 \quad \text{with } x, y \in \mathbf{Z} \tag{21}$$

be a given diophantine equation with associated real quartic field $\mathbf{K} = \mathbf{Q}(\alpha)$ of type $(r, s) = (2, 1)$, where r and s are the number of real and complex embeddings of $\mathbf{K}$, respectively. Further, let $\mathbf{L} = \mathbf{Q}(\sqrt{d})$ be the real quadratic subfield of $\mathbf{K}$.

- Check that $d \equiv 3 \pmod 4$.

- Choose $u, v \in \mathbf{L}$ such that $\eta = v\alpha \in \mathscr{U}^+_{\mathbf{K/L}}$ and $\eta = \xi^k$ with $k \equiv 2 \pmod 4$.
- Check, by using Lemmas 2 and 3, that ξ is not a perfect power in $\mathbf{K}$.

Then Eq. (21) has only trivial solutions if for all $x, y \in \mathbf{Z}$ for which $y' := y/v \in \mathscr{O}_{\mathbf{L}}$, $\mathrm{Norm}_{\mathbf{L/Q}}(XY)$ is exactly divisible by a power of 4, where $X := x - uy'$ and $Y := y'$. □

Remark 3.

- Searching for η and ξ, let $\beta := \sqrt{A + B\sqrt{d}}$ be an integral generator of $\mathbf{K}$. It is not hard to find a suitable $\eta \in \mathscr{U}^+_{\mathbf{K/L}}$ of the form $\eta = a + b\beta$ with $a, b \in \mathbf{L}$. Indeed, only one solution (a, b) of the $\mathbf{L}$-equation $a^2 - b^2\beta^2 = 1$ is needed. Then $\alpha = a' + b'\beta$, for certain a' and b' of $\mathbf{L}$. Next apply Lemma 3 to find k.
- It is clear from the above construction of X and Y that

$$4^e \parallel \mathrm{Norm}_{\mathbf{L/Q}}(XY)$$

places a condition on the integers x and y. This means that the assertion may be rephrased by saying that there can be no nontrivial solutions of a specific form, given by certain congruences modulo powers of 2.

Example 2. We try to solve the following equation

$$x^4 - 6x^2y^2 - 3y^4 = 1, \tag{22}$$

which may be rewritten as (21) with $\alpha = \sqrt{3 + 2\sqrt{3}}$ and $\mathbf{K} = \mathbf{Q}(\alpha)$. We try to find an $\eta = u + v\alpha \in \mathscr{U}^+_{\mathbf{K/L}}$ with $u, v \in \mathbf{L} = \mathbf{Q}(\sqrt{3})$. Then

$$1 = \eta\eta' = (u + v\alpha)(u - v\alpha) = u^2 - v^2(3 + 2\sqrt{3}),$$

a solution of which is given by $u = 1 + \sqrt{3}, v = 1$. Use Lemma 3 to check that $\eta = \xi^2$, where $2\xi = 1 + \sqrt{3} + \sqrt{2\sqrt{3}}$. Then

$$x + y\alpha = x - (1 + \sqrt{3})y + y\xi^2 = X + Y\xi^2$$

with $X := x - (1 + \sqrt{3})y$, $Y := y$. From the original equation it can be seen that x has to be odd. Hence $\wp \nmid X$, and Y is divisible by an even power of $\wp$, unless $XY = 0$.

As a result, no other solutions exist than those given by $y = 0$, provided ξ is not a perfect power in $\mathbf{K}$. This can be verified by Lemma 3 (see also Table 1). So Eq. (22) has solutions $(x, y) = (\pm 1, 0)$ and no others. □

More examples are given in Table 2.

6. Construction of the Tables. Table 1 lists a few number fields, their discriminants and the unit structure of $\mathscr{U}^+_{\mathbf{K/L}}$. The discriminants are calculated using [18]. To determine the unit structure, use is made of Nakamula's bound (see Lemma 2).

To get a fair impression of the possible equations that can be dealt with, the following observations are useful.

The quadratic form $Q := X^2 + XY\theta_k + Y^2$ with linear forms $X, Y \in \mathscr{O}_{\mathbf{L}}[u, v]$, may be written in terms of u and v as

$$Q = \vec{u}^T B \vec{u},$$

TABLE 1

Associated number fields

Absolute discriminant $\mathscr{D}$ of $\mathbf{K} = \mathbf{Q}(\xi)$

$\xi + \xi^{-1} = a + b\sqrt{d}, \mathscr{U}^{+}_{\mathbf{K}/\mathbf{L}} = \langle \epsilon \rangle, \xi = \epsilon^{n}$

$$\text{Bound} = 2\log \xi / \log \left(\sqrt[3]{\frac{|\mathscr{D}|}{4}} + 8^3 - 7 \right)$$

d	(a,b)	$-2^{-6}d^{-2}\mathscr{D}(\xi)$	$-2^{-6}d^{-2}\mathscr{D}$	Bound	n
3	(1,1)	3	3	1.61	1
3	(3,1)	11	11	1.71	1
3	(5,3)	$3^6 \cdot 11$	11	2.63	1
3	(7,3)	3^7	3	4.83	3
3	(7,5)	$3 \cdot 5^6$	$3 \cdot 5^2$	2.01	1
3	(9,5)	$5^4 \cdot 13 \cdot 23$	$13 \cdot 23$	1.72	1
3	(11,7)	$3 \cdot 7^4 \cdot 11^2$	$3 \cdot 11^2$	1.84	1
3	(31,19)	$3 \cdot 11^2 \cdot 19^4$	3	8.05	5
7	(1,1)	3	3	2.34	1
7	(3,1)	3^3	3	3.29	1
7	(7,3)	$3^6 \cdot 19$	$3^2 \cdot 19$	1.74	1
7	(9,3)	$3^4 \cdot 7 \cdot 29$	$7 \cdot 29$	1.78	1
7	(13,5)	$3^3 \cdot 5^6$	$3 \cdot 5^2$	2.39	1
7	(15,5)	$3^2 \cdot 5^4 \cdot 19$	$3^2 \cdot 19$	2.15	1
7	(17,7)	$3^2 \cdot 7^4 \cdot 59$	59	2.72	1
7	(19,7)	$3^3 \cdot 7^6$	3	7.02	3
11	(3,1)	$5 \cdot 7$	$5 \cdot 7$	1.53	1
11	(5,1)	19	19	2.05	1
11	(9,3)	$3^4 \cdot 5^2 \cdot 11$	11	3.34	1
11	(11,3)	$3^6 \cdot 5 \cdot 7$	$3^2 \cdot 5 \cdot 7$	1.81	1
11	(15,5)	$5^4 \cdot 7 \cdot 53$	$7 \cdot 53$	2.01	1
11	(17,5)	$5^6 \cdot 43$	$5^2 \cdot 43$	1.83	1
11	(23,7)	$7^6 \cdot 43$	$7^2 \cdot 43$	1.87	1
11	(25,7)	$5^2 \cdot 7^4 \cdot 19$	$5^2 \cdot 19$	2.20	1
15	(3,1)	$5 \cdot 7$	$5 \cdot 7$	1.61	1
15	(5,1)	$3 \cdot 17$	$3 \cdot 17$	1.70	1
15	(11,3)	$3^7 \cdot 17$	$3 \cdot 17$	2.44	1
15	(13,3)	$3^6 \cdot 5 \cdot 7$	$5 \cdot 7$	2.70	1
15	(19,5)	$3 \cdot 5^4 \cdot 11 \cdot 43$	$3 \cdot 11 \cdot 43$	2.01	1
15	(21,5)	$5^4 \cdot 7^2 \cdot 11$	$7^2 \cdot 11$	2.07	1
15	(27,7)	$5 \cdot 7^4 \cdot 11 \cdot 53$	$11 \cdot 53$	2.21	1
15	(29,7)	$3 \cdot 7^4 \cdot 113$	$3 \cdot 113$	2.38	1

where

$$\vec{u} := \begin{pmatrix} u \\ v \end{pmatrix}, \qquad B := C^T A C,$$

and the matrices

$$A := \begin{pmatrix} 1 & \frac{1}{2}\theta_k \\ \frac{1}{2}\theta_k & 1 \end{pmatrix} \quad \text{and} \quad C := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

are defined over $\mathscr{O}_{\mathbf{L}}$. Clearly, B is symmetric. If

$$B = \begin{pmatrix} \rho & \sigma \\ \sigma & \tau \end{pmatrix},$$

TABLE 2

Solved equations

$$\mathrm{Norm}_{\mathbf{K}/\mathbf{Q}}(X + Y\xi^2) = u^4 + a_2u^2v^2 + a_1uv^3 + a_4v^4 = 1$$

$$X(u,v) = \alpha u + \beta v, Y(u,v) = \delta v$$

$$\alpha = \alpha_1 + \alpha_2\sqrt{d},\ \beta = \beta_1 + \beta_2\sqrt{d},\ \delta = \delta_1 + \delta_2\sqrt{d}$$

All equations have the trivial solutions $(u,v) = \pm(1,0)$;
the final column lists additional trivial solutions (u,v).

d	(a,b)	α_1	α_2	β_1	β_2	δ_1	δ_2	a_2	a_1	a_0	$\pm(u,v)$
3	(1,1)	1	0	−1	0	1	0	−12	24	−12	(1,1)
3	(1,1)	1	0	−1	−1	1	0	−6	0	−3	
3	(1,1)	1	0	−1	1	1	0	−30	48	69	
3	(1,1)	1	0	−5	−3	2	1	−90	0	−3	
3	(1,1)	1	0	1	−1	2	−1	6	0	−3	
3	(1,1)	1	0	1	0	2	−1	0	24	24	(1,−1)
3	(1,1)	2	1	0	1	0	1	12	72	36	
3	(1,1)	2	1	−3	−1	0	1	18	0	−27	
3	(1,1)	2	1	1	−1	2	−1	90	0	−3	
3	(3,1)	1	0	−5	−3	1	0	−102	0	−99	
3	(3,1)	1	0	−1	0	2	−1	0	72	−72	(1,1)
3	(3,1)	1	0	−1	−1	2	−1	6	0	−99	
3	(3,1)	2	1	2	1	2	−1	180	648	468	(1,−1)
3	(5,3)	1	0	−5	−4	2	−1	−192	648	−648	
3	(5,3)	1	0	−5	−5	2	−1	−186	0	−99	
3	(5,3)	2	1	−2	−3	2	−1	−12	72	−108	
3	(5,3)	2	1	−5	−5	2	−1	−6	0	−99	
3	(5,3)	2	1	1	−1	2	−1	−30	144	−27	
7	(1,1)	1	0	−3	−1	1	0	−30	0	−27	
7	(1,1)	1	0	−3	0	1	0	−44	168	−188	(1,1)
7	(1,1)	1	0	−3	1	8	−3	222	0	−27	
7	(3,1)	1	0	−7	−3	0	−1	−222	0	−27	
11	(3,1)	1	0	−9	−3	1	0	−358	0	−35	
11	(3,1)	10	3	0	1	0	1	396	2904	484	
11	(3,1)	10	3	−33	−9	0	1	418	0	−4235	
11	(3,1)	10	3	−66	−19	0	1	396	−2904	484	
15	(3,1)	1	0	−11	−3	1	0	−510	0	−315	
15	(3,1)	4	1	4	1	1	0	0	360	360	
15	(3,1)	4	1	−26	−7	1	0	0	−360	360	
15	(3,1)	4	1	−11	−3	1	0	30	0	−315	

then

$$\rho = \alpha^2 + \alpha\gamma\theta_k + \gamma^2,$$
$$\sigma = \alpha\beta + \gamma\delta + \tfrac{1}{2}\theta_k(\alpha\delta + \beta\gamma),$$
$$\tau = \beta^2 + \beta\delta\theta_k + \delta^2.$$

Further, $\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(Q\overline{Q})$ (see (19)) may be written as

$$a_4u^4 + a_3u^3v + a_2u^2v^2 + a_1uv^3 + a_0v^4 = 1, \tag{23}$$

with

$$a_4 = \rho\overline{\rho},$$
$$a_3 = 2(\rho\overline{\sigma} + \overline{\rho}\sigma),$$
$$a_2 = 4\sigma\overline{\sigma} + \rho\overline{\tau} + \overline{\rho}\tau,$$
$$a_1 = 2(\sigma\overline{\tau} + \overline{\sigma}\tau),$$
$$a_0 = \tau\overline{\tau}.$$

Equation (23) must have a trivial solution, for which $(u, v) = (1, 0)$ is selected. This choice corresponds to

$$X = \alpha u + \beta v = \alpha, \qquad Y = \gamma u + \delta v = \gamma,$$

so that ρ is a unit of $\mathscr{O}_{\mathbf{L}}$, that is to say, $\rho\overline{\rho} = a_4 = 1$. By means of a unimodular transformation of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

the coefficient a_3 can be made to vanish, which implies that $\sigma\rho^{-1} \in \mathbf{Z}[\sqrt{d}]$. Further, for reasons of simplicity, choose $\gamma = 0$. Moreover, δ will be chosen such that $\wp \nmid \delta$, so that Y is never exactly divisible by an odd power of $\wp$. All this means that

- α is a unit, as $\rho = \alpha^2$ is a unit.
- $\beta = -\frac{1}{2}\theta_k\delta + \alpha\sigma\rho^{-1} = -\frac{1}{2}\theta_k\delta + \alpha n\sqrt{d}$ with $n \in \mathbf{Z}$.
- $\gamma = 0$.
- $\wp \nmid \delta$.

Table 2 gives a selection of equations resulting from linear forms X and Y chosen accordingly. Moreover, without exception, we have chosen $k = 2$ for these equations.

Note that it remains to be checked that $X = \alpha u + \beta v$ and $Y = \delta v$ satisfy the norm requirement: if $XY \neq 0$ then $\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(XY)$ is exactly divisible by a power of 4. In most cases this is just a matter of checking the parity of u and v by means of a suitable congruence modulo 8.

Econometric Institute
Erasmus University Rotterdam
P.O. Box 1738
3000 DR Rotterdam, The Netherlands
E-mail: stroeker@hroeur5.bitnet

1. A. BAKER, "Contributions to the theory of diophantine equations I: On the representation of integers by binary forms, II: The diophantine equation $y^2 = x^3 + k$," *Philos. Trans. Roy. Soc. London. Ser A*, v. 263, 1968, pp. 173–208.

2. A. BAKER & H. DAVENPORT, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$," *Quart. J. Math. Oxford Ser.* (2), v. 20, 1969, pp. 129–137.

3. A. BREMNER, "A diophantine equation arising from tight 4-designs," *Osaka J. Math.*, v. 16, 1979, pp. 353–356.

4. L. HOLTZER, *Zahlentheorie, Teil* I, Math. Naturw. Bibl. 13, Teubner Verlag, Leipzig, 1958.

5. H. LONDON & R. FINKELSTEIN, "On Mordell's equation $y^2 - k = x^3$," *Bowling Green State Univ. Press*, 1973.

6. L. J. MORDELL, *Diophantine Equations*, Pure and Appl. Math., vol. 30, Academic Press, New York, 1969.

7. TRYGVE NAGELL, "Sur quelques questions dans la théorie des corps biquadratiques," *Ark. Mat.*, v. 4, 1962, pp. 347–376.

8. KEN NAKAMULA, "Class number calculation and elliptic unit II," *Proc. Japan Acad.*, v. 57A, 1981, pp. 117–120.

9. KEN NAKAMULA, "Class number calculation of a quartic field from the elliptic unit," *Acta Arith.*, v. 45, 1985, pp. 215–227.

10. R. J. STROEKER, "On the diophantine equation $(2y^2 - 3)^2 = x^2(3x^2 - 2)$ in connection with the existence of non-trivial tight 4-designs," *Indag. Math.*, v. 43, 1981, pp. 353–358.

11. R. J. STROEKER, "On classes of biquadratic diophantine equations with trivial solutions only," *Abstracts Amer. Math. Soc.*, v. 35, 1984, p. 441.

12. R. J. STROEKER & R. TIJDEMAN, "Diophantine equations," in *Computational Methods in Number Theory*, Part II, MC Tracts 155, Centre Math. Comp. Sci., Amsterdam, 1982, pp. 321–369.

13. R. J. STROEKER & N. TZANAKIS, "On the application of Skolem's p-adic method to the solution of Thue equations," *J. Number Theory*, v. 29, 1988, pp. 166–195.

14. A. THUE, "Über Annäherungswerte algebraischer Zahlen," *J. Reine Angew. Math.*, v. 135, 1909, pp. 284–305.

15. NIKOS TZANAKIS, "On the diophantine equation $x^2 - Dy^4 = k$," *Acta Arith.*, v. 46, 1986, pp. 257–269.

16. N. TZANAKIS & B. M. M. DE WEGER, *On the Practical Solution of the Thue Equation*, Memorandum 668, Fac. Appl. Math. Un. of Twente, 1987.

17. SABURÔ UCHIYAMA, "Solution of a diophantine problem," *Tsukuba J. Math.*, v. 8, 1984, pp. 131–157.

18. THERESA P. VAUGHAN, "The discriminant of a quadratic extension of an algebraic field," *Math. Comp.*, v. 40, 1983, pp. 685–707.