JOURNAL OF NUMBER THEORY 29, 166–195 (1988)

On the Application of Skolem's p-adic Method to the Solution of Thue Equations

R. J. STROEKER

Econometric Institute, Erasmus University,
P.O. Box 1738, 3000 DR Rotterdam, The Netherlands

AND

N. TZANAKIS*

Department of Mathematics, University of Crete,
P.O. Box 470, Iraklion, Crete, Greece

Communicated by D. J. Lewis

Received March 16, 1987; revised September 14, 1987

An algebraic method is discussed for solving diophantine equations of Thue type associated with totally real normal extensions of degree 4 over the rationals. Use is made of a p-adic argument due to Skolem. The method is illustrated by a detailed description of the solution of the Thue equation

$$x^4 - 4x^2y^2 + y^4 = -47.$$

Some of the tricks used in the process of solving this equation may be applied more widely. These aspects are discussed at length.

I. INTRODUCTION

1. The main body of this paper is devoted to a description of an algebraic method for solving diophantine equations of Thue type, associated with certain totally real quartic fields. In order to clarify our argumentation we have singled out a specific equation, namely

$$x^4 - 4x^2y^2 + y^4 = -47, \tag{1.1}$$

which we solve completely in Section II. More about the reasons for choosing this particular equation is revealed in Section 4 of this Introduction.

* A considerable part of the present paper was prepared when the second named author held a visiting position at the Econometric Institute of Erasmus University Rotterdam. He gratefully acknowledges the financial support granted to him by this host institution.

0022-314X/88 $3.00

Although we deal principally with Eq. (1.1), we believe the crucial parts of our argumentation to be valid in more generality. We feel that a detailed exposition of a special case like (1.1), with a clear indication of approaches that are applicable in a broader sense, could be very useful for gaining a deeper understanding of our method and of the underlying difficulties in general. In Section IV a step by step description is given of the method used to solve (1.1), accompanied by a discussion as to how this method may be adapted to solve other equations of similar type. At the end of our exposition some ideas and arguments are discussed that are of a more general nature, in the sense that they can also be applied to different diophantine problems.

Anticipating the brief overview of the main ideas of our method which is given in the final section of this introduction, we could mention that we shall work in a quadratic extension of the totally real quartic field associated with the relevant quartic equation in order to obtain a suitable system of exponential equations to which Skolem's p-adic method may be applied.

2. Thue equations can be characterized as follows. Let f be an irreducible form in $\mathbb{Z}[x, y]$ of degree at least 3. By a celebrated theorem of Thue [28], we know that the diophantine equation (a so-called Thue equation)

$$f(x, y) = c \tag{1.2}$$

for any constant c, has at most a finite number of solutions in rational integers x and y. Unfortunately, the proof of Thue's theorem is ineffective. This means that for any given equation of type (1.2), Thue's proof does not shed any light on its solvability, neither does it provide an effective method for finding the solution values if such exist.

Moreover, Matiyasevich showed in 1970 [18] that there is no general purpose algorithm by which every diophantine equation can be solved.

As a result, in the past decades, many individual equations have been dealt with and quite a few successful methods and techniques have been developed to attack such diophantine problems. Most of these methods are elementary or have a distinct algebraic flavor. They nearly always depend on congruence considerations and artful factorization in suitable algebraic number fields.

Another group of methods derives from Baker's method on linear forms in the logarithms of algebraic numbers [1]. In [10] it is shown how this method can be used to solve diophantine equations. In contrast to the algebraic case, so far rather few Thue equations have been completely solved by analytic methods, in the sense that, as a result, all solutions can

be explicitly listed. In most cases only extremely large upper bounds for the size of the solutions are provided. Examples of equations or systems of equations that have been solved by Baker's method can be found in [2, 4, 11, 25], and the very recent papers [5, 19, 32].

3. At the present time, it appears that for every cubic Thue equation the p-adic method of Skolem can be successfully applied; and although no proof guarantees its effectiveness, in all specific equations to which it has been applied it worked successfully. For a description of the p-adic method in general, we refer to [6, 13, 15, 17, 22, 23, 30]. In case the cubic form f has negative discriminant, one can apply Skolem's technique directly, because, in this case, there is only one fundamental unit in the field generated by a root of $f(x, 1) = 0$ (it should be mentioned that the computations needed in a search for such a unit are sometimes far from trivial), but if f is totally real this is impossible. However, in case of the latter, it has been shown by Ljunggren [16] and also by Tzanakis [29] that solving Eq. (1.2) is equivalent to solving a finite number of quartic Thue equations

$$g(x, y) = 1, \tag{1.3}$$

where each of the forms g involved has negative discriminant; for such quartic Thue equations the p-adic method of Skolem stands a fair chance of working successfully.

One of the most notorious equations of this type

$$x^3 - 3xy^2 - y^3 = 1, \tag{1.4}$$

was solved in the way described by Tzanakis [29]. The first to solve this equation was Ljunggren. In [14] he used an ingenious trick, working in a quadratic extension of the field associated with the cubic form of (1.4).

As the cubic case has been settled, next in line is the quartic equation. We have mentioned above that Skolem's method can be applied, provided the associated quartic form f has negative discriminant. However, in case f is totally real, this method cannot be applied, at least not directly, because there is one unknown exponent more than there are independent equations relating these unknowns.

4. It appears that for Thue equations associated with a totally real quartic field, there is no known *algebraic* approach as promising in general as the method mentioned above for dealing with cubic equations and quartic equations associated with a form of negative discriminant.

To illustrate an approach that might fill this gap in certain cases, we prefer to select a quartic Thue equation that has not been solved previously by any known method. The form associated with Eq. (1.1) seems a natural

choice: it has the required properties and it is simple in appearance. This equation is a special case of

$$x^4 - 4x^2y^2 + y^4 = c, \tag{1.5}$$

where c is a non-zero constant. Some motivation as to the reason for considering equations of this type at all is given in [27]. It is easy to prove by elementary means that the only c-values in the range $-100, ..., 100$ for which Eq. (1.5) admits solutions are $c = -47, -2, 1, 46$, and 81.

All but the case $c = -47$ can be solved by reduction to an equation, the solutions of which are known ($c = -2$, see [27]) or by applying Skolem's p-adic method in the usual way ($c = 1, 46$ and 81, see [30]). There is nothing more special about Eq. (1.1) than the mere fact that all existing factorization and generally algebraic methods seem to fail in this particular case. To the best of our knowledge, a case involving a totally real binary quartic has never been successfully attempted by. algebraic methods; at least such an approach has not appeared in print. Only recently we received two preprints [5, 19] in which certain Thue equations associated with totally real quartic fields are solved by Baker's transcendental method. Apparently, the calculations involved are quite costly in the sense that they take up a great deal of computer time.

5. In Section II Eq. (1.1) will be completely solved. By means of a trick, which can be seen as the quartic equivalent of the one employed by Ljunggren in [14]—in our case we work in a number field of absolute degree 8—we shall reduce (1.1) to a p-adic system to which Skolem's method can be applied successfully with prime $p = 71$.

We shall show that the only solutions of (1.1) in rational integers x and y are given by $(x, y) = (\pm 2, \pm 3)$ and $(\pm 3, \pm 2)$.

Although Section II deals with a single equation, our attention is focused on the method rather than on this particular equation. The two most important ingredients of our method, which also may be used profitably in different settings, are the manipulation of units and the application of Skolem's p-adic method. In Section IV these matters are discussed in great detail. Also, leaving Eq. (1.1) for what it is, a more general discription of the method is given as applied to quartic Thue equations associated with totally real normal extensions of $\mathbb{Q}$.

Finally, the proofs of a number of technical lemmas that are needed in Section II are deferred to Section III, so as to avoid unnecessary interruptions of the line of reasoning. Because units play such a decisive role in our exposition, the lemmas on the properties of units are stated and proved there where they are needed.

II. Solution of $x^4 - 4x^2y^2 + y^4 = -47$

1. In this section we set the scene for the actual solving of Eq. (1.1). Ultimately (the proof is clinched in the final section) we shall prove the

THEOREM 1. *The title equation* (1.1) *has no other solutions than those given by the eight pairs* $(x, y) = (\pm 2, \pm 3), (\pm 3, \pm 2)$.

We start to work in the field $\mathbb{K} = \mathbb{Q}(\rho)$, where ρ is defined by $\rho^4 - 4\rho^2 + 1 = 0$. Clearly, $\mathbb{K}$ is a totally real field and the conjugates of ρ are $-\rho$, ρ^{-1}, and $-\rho^{-1}$.

Equation (1.1) is equivalent to

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x + y\rho) = -47. \tag{2.1}$$

From the definition of ρ it follows easily that $47\rho^2 = (3 - 2\rho)(3 + 2\rho)(2 - 3\rho)(2 + 3\rho)$ and since ρ is a unit, the ideal (47) splits into four different prime ideals, namely the ideals

$$(3 - 2\rho),\ (3 + 2\rho),\ (2 - 3\rho),\ \text{and}\ (2 + 3\rho). \tag{2.2}$$

Consequently, (2.1) implies that

$$(x + y\rho) =: \mathfrak{p} \tag{2.3}$$

is one of the prime ideals mentioned in (2.2). We assert that we may take $\mathfrak{p} = (2 + 3\rho)$, without any loss of generality. Indeed, if $(x + y\rho) = (2 - 3\rho)$ then, in view of the automorphism characterized by $\rho \mapsto -\rho$, we have also the ideal relation $(x - y\rho) = (2 + 3\rho)$, which is obtained by simply replacing y by $-y$. Moreover, if $(x + y\rho) = (3 + 2\rho)$, then, analogously, we obtain the relation $(x + y\rho^{-1}) = (3 + 2\rho^{-1})$ and since ρ is a unit, this gives $(y + x\rho) = (2 + 3\rho)$. Clearly this can be effected by interchanging x and y in (1.1). Similarly, if $(x + y\rho) = (3 - 2\rho)$, we replace $-y$ by x and x by y to obtain $(x + y\rho) = (2 + 3\rho)$. Thus, in view of (2.3) and the above, we get

$$x + y\rho = \varepsilon(2 + 3\rho), \tag{2.4}$$

where ε is a unit of $\mathbb{K}$. In $\mathbb{K}$ we have three fundamental units. From the tables of Pohst and Zassenhaus [20], we find a triad of fundamental units in $\mathbb{K}$:

$$\varepsilon_1 = \rho, \qquad \varepsilon_2 = -2 - 3\rho + \rho^2 + \rho^3, \qquad \varepsilon_3 = 3 + 4\rho - \rho^2 - \rho^3$$

with

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\varepsilon_i) = +1 \qquad (i = 1, 2, 3).$$

As a consequence, (2.4) implies a relation

$$x + y\rho = \pm E(\rho),$$

where $E(\rho) := \varepsilon_1^{a_1}\varepsilon_2^{a_2}(\varepsilon_1\varepsilon_3)^{a_3}(2+3\rho)$ and $a_1, a_2, a_3 \in \mathbb{Z}$. The minus sign in the relation above may be ignored on replacing (x, y) by $(-x, -y)$, if necessary. Then, considering all the conjugate relations, eliminating y, we get $E(\rho) + E(-\rho) = E(\rho^{-1}) + E(-\rho^{-1})$, which can also be written as

$$A_1A_2A_3(2+3\rho) = A_1(-2+3\rho) + A_2(3+2\rho) + A_3(-3+2\rho), \quad (2.5)$$

where

$$A_1 := \varepsilon_1^{2a_1+1}(-1)^{a_1+a_3}, \qquad A_2 := \varepsilon_2^{2a_2}(-1)^{a_2+a_3},$$

and

$$A_3 := (\varepsilon_1\varepsilon_3)^{2a_3}(-1)^{a_1+a_2}.$$

Note that the A_i's are units of $\mathbb{K}$. Analogously, eliminating x gives $E(\rho) - E(-\rho) = \rho^2(E(\rho^{-1}) - E(-\rho^{-1}))$, or

$$A_1A_2A_3(2+3\rho) = A_1(2-3\rho) + A_2\rho^2(3+2\rho) + A_3\rho^2(3-2\rho). \quad (2.6)$$

Eliminating the product $A_1A_2A_3$ by subtracting (2.5) from (2.6) leads to

$$2(3\rho-2)\frac{A_1}{A_2} + (2\rho-3)(\rho^2+1)\frac{A_3}{A_2} = (2\rho+3)(\rho^2-1).$$

Since $a_1 \equiv a_2 \equiv a_3 \pmod 2$ (cf. Lemma 5 of Section III) and $\rho^2 + 1 = \sqrt{6}\,\rho$, this relation can be written as

$$\alpha X^2 + \beta Y^2 = \alpha + \beta, \quad (2.7)$$

where $\alpha := (3\rho-2)\sqrt{2}$, $\beta := (2\rho-3)\sqrt{3}$, so that $\alpha + \beta = 2\rho + 3$ and

$$X = \varepsilon_1^{a_1}\varepsilon_2^{-a_2}, \qquad Y = (\varepsilon_1\varepsilon_3)^{a_3}\varepsilon_2^{-a_2}.$$

From the definitions of α and β it follows that

$$-\alpha\beta = 13\rho^2 - 36\rho + 13 = (1+\rho^2)(13-6\sqrt{6}) = (1+\rho)^2(75-31\sqrt{6})$$
$$= (1+\rho)^2\eta^2 = \theta^2,$$

where, by definition

$$\eta = \sqrt{75-31\sqrt{6}} \in i\mathbb{R} \qquad \text{and} \qquad \theta = \eta(1+\rho).$$

Now (2.7) may be rewritten as

$$(\alpha X)^2 - (\theta Y)^2 = \alpha(\alpha + \beta). \tag{2.8}$$

We define $\mathbb{L} = \mathbb{Q}(\eta)$, $\mathbb{M} = \mathbb{Q}(\theta)$ and we note that $\mathbb{M} = \mathbb{Q}(\rho, \eta)$ (see Lemma 6 of Section III) is an octic extension of $\mathbb{Q}$. Ideal factorization in the field $\mathbb{M}$ gives

$$(2\rho + 3) = \mathfrak{q}\mathfrak{q}',$$

with $\mathfrak{q} := (2\rho + 3, 2\theta + 3)$ and $\mathfrak{q}' := (2\rho + 3, 2\theta - 3)$, and

$$(3\rho - 2) = \mathfrak{a}^2,$$

with $\mathfrak{a} := (3\rho - 2, \eta)$. Hence, under the conjugation map characterized by $\theta \mapsto -\theta$, the ideal $\mathfrak{q}$ is mapped to $\mathfrak{q}'$ and $\mathfrak{a}$ is mapped to itself.

Now (2.8) may be written in ideal form as

$$\left(\frac{\alpha}{1+\rho} X - \eta Y\right)\left(\frac{\alpha}{1+\rho} X + \eta Y\right) = \mathfrak{q}\mathfrak{q}'\mathfrak{a}^2.$$

Note that $\sqrt{2} = \rho^{-1}(\rho + 1)(\rho - 1)$, so that $\alpha/(1 + \rho) = \rho^{-1}(\rho - 1)(3\rho - 2)$ is integral. Consequently,

$$\left(\frac{\alpha}{1+\rho} X + \eta Y\right) = \mathfrak{q}\mathfrak{a} \text{ or } \mathfrak{q}'\mathfrak{a}.$$

Choose the sign of Y such that the former possibility is adopted. On the other hand, since $X = Y = 1$ gives a solution, while $\mathfrak{q}'$ does not divide $\alpha/(1 + \rho) + \eta$, it follows that $(\alpha/(1 + \rho) + \eta) = \mathfrak{q}\mathfrak{a}$. Hence

$$\left(\frac{\alpha}{1+\rho} X + \eta Y\right) = \left(\frac{\alpha}{1+\rho} + \eta\right)$$

and thus

$$\alpha X + \theta Y = \zeta(\alpha + \theta), \tag{2.9}$$

where ζ is a unit of $\mathbb{M}$ and, in fact, it is a unit of the order

$$\mathcal{O} := \mathbb{Z}[1, \rho, \rho^2, \rho^3, \eta, \eta\rho, \eta\rho^2, \eta\rho^3].$$

We have also the conjugate relation, which corresponds to the automorphism characterized by $\theta \mapsto -\theta$,

$$\alpha X - \theta Y = \zeta'(\alpha - \theta), \tag{2.10}$$

where $\zeta\zeta' = 1$, as can be seen from (2.8) and the relation $\alpha^2 - \theta^2 = \alpha(\alpha + \beta)$. But $\zeta\zeta' = 1$ is equivalent to

$$\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\zeta) = 1,$$

so that $\zeta \in \mathscr{U}_0$, where $\mathscr{U}_0$ is the subgroup of the unit group $\mathscr{U}$ of $\mathbb{M}$, consisting of those units of $\mathscr{O}$ with norm relative to $\mathbb{K}$ equal to $+1$. By Lemma 7 of Section III, the group $\mathscr{U}_0$ has two generators of infinite order λ_1 and λ_2, say, and -1 is its only generator of finite order. Thus we can write

$$\zeta = \pm\lambda_1^{b_1}\lambda_2^{b_2}, \qquad \text{with} \quad b_1, b_2 \in \mathbb{Z}. \tag{2.11}$$

On adding (2.9) and (2.10) we obtain the following expressions for X and Y:

$$X = \frac{\zeta(\alpha+\theta) + \zeta'(\alpha-\theta)}{2\alpha}, \qquad Y = \frac{\zeta(\alpha+\theta) - \zeta'(\alpha-\theta)}{2\theta}. \tag{2.12}$$

Since by their initial definition, X and Y are units of $\mathbb{K}$, we have

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(X) = 1 = \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(Y). \tag{2.13}$$

As the quantities X and Y depend on ζ and ζ' only, the norm functions in (2.13) can be considered as polynomial functions with coefficients in $\mathbb{M}$, of the eight conjugates $\zeta^{(i)}$ $(i = 1, ..., 8)$ of ζ. To be more precise,

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(X) = 1 \text{ is equivalent to } G_1(\zeta^{(1)}, ..., \zeta^{(8)}) = -188$$

and

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(Y) = 1 \text{ is equivalent to } G_2(\zeta^{(1)}, ..., \zeta^{(8)}) = -2,$$

where $G_j \in \mathbb{M}[t_1, ..., t_8]$, $j = 1, 2$, and $G_i(\zeta^{(1)}, ..., \zeta^{(8)})$, $i = 1, 2$, are the norms of αX and $(1+\rho)Y$, respectively (we have taken into account that $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha) = -4 \cdot 47 = -188$ and $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(1+\rho) = -2$; see also immediately after (2.29)). For the sake of convenience, we write

$$G(\zeta) := (G_1(\zeta^{(1)}, ..., \zeta^{(8)}), G_2(\zeta^{(1)}, ..., \zeta^{(8)}))$$

so that $G(\zeta)$ represents a pair of rational integers for every unit $\zeta \in \mathscr{O}$.

We say that ζ is an *acceptable unit* if it satisfies $G(\zeta) = (-188, -2)$. Also, for any rational prime p, we say that ζ is an *acceptable unit modulo p* if it satisfies $G(\zeta) \equiv (-188, -2) \pmod{p}$.

We conclude this section with pointing out that our original task of finding all solutions of (1.1) has been reduced to determining all acceptable

units $\zeta \in \mathcal{U}_0$. We intend to show that $+1$ and -1 are the only such units. As is easily traced back through the previous arguments, this means that the eight pairs $(x, y) = (\pm 2, \pm 3)$ and $(\pm 3, \pm 2)$ give the only solutions of (1.1).

2. In order to find the explicit p-adic system in the unknown exponents b_1 and b_2 to which (2.13) leads, we first have to know the generators λ_1 and λ_2 of the group $\mathcal{U}_0$. In general, it is not very difficult to find a pair of independent units [21, 24]. However, to prove or disprove that a given set of independent units, having the right cardinality, constitutes a fundamental set, is far from easy.

Having little hope of finding a fundamental set $\{\lambda_1, \lambda_2\}$ in a reasonable amount of time and with adequate effort, we tried instead to find a pair of merely *independent* units ζ_1, ζ_2 that "behaves p-adically as a pair of fundamental units." What we mean by this will be explained in the following proposition (see also Section 5 of [9], Section 4 of [26], and Section 7.2 of [7]).

PROPOSITION 1. *Let λ_1, λ_2 be an unknown pair of fundamental units for the unit group $\mathcal{U}_0$ and let ζ_1, ζ_2 be a known pair of independent units of $\mathcal{U}_0$. Put*

$$\zeta_1 = \pm \lambda_1^{m_1} \lambda_2^{m_2}, \zeta_2 = \pm \lambda_1^{n_1} \lambda_2^{n_2} \qquad \text{with} \quad m_1, m_2, n_1, n_2 \in \mathbb{Z} \tag{2.14}$$

and

$$D := \begin{vmatrix} m_1 & m_2 \\ n_1 & n_2 \end{vmatrix} \qquad (\text{obviously, } D \neq 0).$$

Let p be an odd prime and let e_p denote the least positive integer such that $\alpha^{e_p} \equiv 1 \pmod{p}$ for every $\alpha \in \mathcal{O}$, relatively prime to p. Also denote by $q = q(p)$ the least positive integer such that

$$\zeta_i^q \equiv 1 \pmod{p}, \qquad \text{for} \quad i = 1, 2. \tag{2.15}$$

Further, assume that

(1) $(D, pe_p) = 1$, (2.16)

(2) *if $\zeta = \lambda_1^{b_1} \lambda_2^{b_2}$ is acceptable then $b_1 \equiv b_2 \equiv 0 \pmod{q}$,* (2.17)

(3) *the only unit $\zeta \in \mathcal{U}_0$ that can be expressed in the form $\zeta = (\zeta_1^q)^M (\zeta_2^q)^N$, where M and N are p-adic integers, is $\zeta = 1$.* (2.18)

Then the only acceptable units of $\mathcal{U}_0$ are ± 1.

Proof. We show first that

$$\lambda_i^q \equiv 1 \pmod{p}, \qquad \text{for} \quad i = 1, 2. \tag{2.19}$$

By (2.14) and the fact that D does not vanish, there exist rational integers x_{ij} for $i, j = 1, 2$, such that $\lambda_i^D = \zeta_1^{x_{i1}} \zeta_2^{x_{i2}}$, for $i = 1, 2$, and thus, on taking qth powers, we get

$$\lambda_i^{qD} \equiv 1 \pmod{p}, \qquad \text{for} \quad i = 1, 2. \tag{2.20}$$

Next, in view of (2.16), there exist two rational integers r and s such that $rD + se_p = 1$. Then (2.20) implies that $\lambda_i^{q(1-se_p)} \equiv 1 \pmod{p}$ for $i = 1, 2$. In view of the definition of e_p, (2.19) now follows.

Let $\zeta \in \mathscr{U}_0$ be an acceptable unit and write $\zeta = \pm \lambda_1^{b_1} \lambda_2^{b_2}$ with $b_1, b_2 \in \mathbb{Z}$. Since $-\zeta$ is also acceptable, we may ignore the minus sign and it remains to prove that $\zeta = \lambda_1^{b_1} \lambda_2^{b_2}$ equals 1. By (2.17) we may write $b_i = qB_i$ with $B_i \in \mathbb{Z}$ $(i = 1, 2)$ and in view of (2.14)

$$\zeta^D = \{(\lambda_1^q)^{B_1} (\lambda_2^q)^{B_2}\}^D = \pm (\zeta_1^q)^{(n_2 B_1 - n_1 B_2)} (\zeta_2^q)^{(-m_2 B_1 + m_1 B_2)}, \tag{2.21}$$

while by (2.15), (2.19), and $p \neq 2$ we see that the plus sign holds. This relation (2.21) can be viewed as a relation in the p-adic field, where the right-hand side as well as the bracketed quantity $\{\cdots\}$ are p-adic binomial power series. Also note that $(n_2 B_1 - n_1 B_2)/D$ and $(-m_2 B_1 + m_1 B_2)/D$ are p-adic integers, in view of (2.16). Therefore,

$$\zeta = (\zeta_1^q)^{(n_2 B_1 - n_1 B_2)/D} (\zeta_2^q)^{(-m_2 B_1 + m_1 B_2)/D},$$

and by (2.18) we conclude that $\zeta = 1$. ∎

In the following two sections we intend to prove that the conditions of Proposition 1 are fulfilled in our case.

3. In the usual way (hard work as it may be), by considering many ideals of small norms, we found with the aid of a microcomputer the following independent units (see [27]; for ζ_2 see also Section IV, Remark (ii) after Theorem 2):

$$\zeta_1 = 355967 - 726615\rho + 145323\rho^3 + 28974\eta - 59145\eta\rho + 11829\eta\rho^3$$

$$\zeta_2 = -355 + 685\rho - 137\rho^3 - 32\eta + 57\eta\rho + 16\eta\rho^2 - 19\eta\rho^3.$$

Next we have to choose a convenient prime for our p-adic argument. A reasonable choice would be a prime p that splits in $\mathbb{M}$ into eight distinct prime ideal factors, because the integer e_p for such a prime p is a divisor of $p - 1$, which is relatively small. Examples of such primes are 71 and 97. The

corresponding value of q for these two primes is $p-1$, so that in both cases $e_p = p-1$. All this was checked by computer.

In order to show that ζ_1 and ζ_2 can play the role as described in the previous section with $p=71$ (the prime $p=97$ also plays a part, be it a minor one), we need a sequence of lemmas.

LEMMA 1. *For any rational prime p, D is divisible by p iff there exists at least one $s \in \{0, 1, ..., p-1\}$ such that either $\zeta_1 \zeta_2^s$ or $\zeta_1^s \zeta_2$ is a pth power of some unit of $\mathcal{O}$.*

Proof. The determinant D satisfies $D \equiv 0 \pmod{p}$ iff a pair $(u, v) \in \{0, 1, ..., p-1\}^2$ exists with $(u, v) \neq (0, 0)$ and such that

$$\begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p}.$$

The latter condition is equivalent to: for some integer $s \in \{0, 1, ..., p-1\}$ either $(1, s)$ or $(s, 1)$ is a solution of

$$\begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p}$$

and this in turn can be phrased equivalently as: either $\zeta_1 \zeta_2^s$ $(= \lambda_1^{m_1 s + n_1} \lambda_2^{m_2 s + n_2})$ or $\zeta_1^s \zeta_2$ $(= \lambda_1^{m_1 + n_1 s} \lambda_2^{m_2 + n_2 s})$ is a pth power in $\mathcal{O}$. ∎

LEMMA 2. *D is relatively prime to p for $p = 2, 3, 5, 7,$ and 71.*

Proof. We only consider the most difficult case in detail, namely $p = 71$. Following Bremner [7], we search for a rational prime $\pi \equiv 1 \pmod{71}$ which has prime ideal divisors in $\mathbb{M}$ of degree 1. Such a prime is $\pi = 6959$. The defining polynomial of θ has the following eight roots mod π: $r_1 = 713$, $r_2 = 1647$, $r_3 = 3430$, $r_4 = 2208$, $r_5 = -r_1$, $r_6 = -r_2$, $r_7 = -r_3$, $r_8 = -r_4$. Therefore, $\theta \equiv r_i \pmod{\mathfrak{p}_i}$ for $i = 1, 2, ..., 8$, where the $\mathfrak{p}_i$'s are the eight different prime ideals into which (π) splits. Thus, every integral element in $\mathbb{M}$ is congruent mod $\mathfrak{p}_i$ to a *rational integer.*

Consider first the case $\theta \equiv 713 \pmod{\mathfrak{p}_1}$. Then, by the expressions of ρ and η in terms of θ (see Appendix A in [27]), we easily find $\rho \equiv 1232$ and $\eta \equiv 6192 \pmod{\mathfrak{p}_1}$. Then $\zeta_1 \equiv 4147$ and $\zeta_2 \equiv 2889 \pmod{\mathfrak{p}_1}$.

Next consider a relation

$$\zeta_1 \zeta_2^s = \lambda^{71}, \qquad 0 \leqslant s \leqslant 70, \qquad \text{for some} \quad \lambda \in \mathcal{O}. \tag{2.22}$$

Since $\lambda \equiv k \pmod{\mathfrak{p}_1}$ for some $k \in \mathbb{Z}$, (2.22) implies that $4147 \cdot 2889^s \equiv k^{71} \pmod{\mathfrak{p}_1}$ and consequently

$$4147 \cdot 2889^s \equiv k^{71} \pmod{6959}, \tag{2.23}$$

and this is an ordinary congruence in $\mathbb{Z}$. The number 7 is a primitive root mod 6959 and $\text{ind}(4147) = 5004$, $\text{ind}(2889) = 5$. Thus (2.23) is equivalent to $5004 + 5s \equiv 71 \cdot \text{ind}(k) \pmod{6958}$. In particular, $5004 + 5s \equiv 0 \pmod{71}$, from which we deduce that $s = 50$. Thus (2.22) implies that $s = 50$.

Next we consider the relation (2.22) mod $\mathfrak{p}_2$, with $s = 50$. From the congruences

$$\theta \equiv 1647,\ \rho \equiv 5727,\ \eta \equiv 971,\ \zeta_1 \equiv 4033,\ \zeta_2 \equiv 813 \pmod{\mathfrak{p}_2},$$

and

$$\text{ind}(4033) = 2081, \qquad \text{ind}(813) = 6090,$$

it follows that $2081 + 50 \cdot 6090 \equiv 0 \pmod{71}$, which is clearly contradictory. Therefore, (2.22) is impossible and in a completely analogous way it can be shown that its companion $\zeta_1^s \zeta_2 = \lambda^{71}$ is equally impossible. In view of Lemma 1 it follows that $(D, 71) = 1$.

For $p = 7, 5, 2$, and 3 we proceed in a similar fashion. We delete the details, but the necessary numerical information is incorporated in the table below.

p	π	prim. root mod p	$\theta \equiv$	$\rho \equiv$	$\eta \equiv$	$\zeta_1 \equiv$	$\zeta_2 \equiv$	$\text{ind}(\zeta_1)$	$\text{ind}(\zeta_2)$
2, 5, 7	71	7	8	39	57	20	46	40	21
			23	32	5	59	8	3	18
3	73	5	14	60	11	39	42	65	47
			27	28	11	39	40	65	25

Proceeding as in the case $p = 71$, it is not difficult to check with the assistance of this table that for each p-value a contradiction is reached, and this shows that D is prime to 2, 3, 5, and 7. ∎

In view of Lemmas 1 and 2 it follows that condition (2.16) is fulfilled if $p = 71$ and also that $(D, e_p) = 1$ if $p = 97$.

LEMMA 3. *Let* $(D, e_p) = 1$. *Then for every* mod p *acceptable unit* $\zeta = \lambda_1^{b_1} \lambda_2^{b_2}$, *there exists a* mod p *acceptable unit* $\zeta_0 = \zeta_1^{\beta_1} \zeta_2^{\beta_2}$ *with* $(\beta_1, \beta_2) \in \{0, 1, \ldots, q-1\}^2$, *where the* b_i's *and* β_i's *are related by*

$$\begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \pmod{q}. \tag{2.24}$$

Proof. We want to specify the β_i's so that $G(\zeta_0) \equiv G(\zeta) \pmod{p}$. In

view of the definition of G (see the end of Section 1), it suffices to specify the β_i's so that $\zeta_0 \equiv \zeta \pmod{p}$, and this is equivalent to

$$\lambda_1^{m_1\beta_1 + n_1\beta_2} \lambda_2^{m_2\beta_1 + n_2\beta_2} \equiv \lambda_1^{b_1} \lambda_2^{b_2} \pmod{p}. \tag{2.25}$$

Since, by hypothesis, D and q are co-prime, it follows that, given (b_1, b_2), we can find $(\beta_1, \beta_2) \in \{0, 1, ..., q-1\}^2$ satisfying (2.24). But then, in view of (2.19), (2.25) is true, as we set out to prove. ∎

LEMMA 4. *If the unit $\zeta = \lambda_1^{b_1} \lambda_2^{b_2}$ is acceptable, then $b_1 \equiv b_2 \equiv 0 \pmod{70}$.*

Proof. Since ζ is acceptable mod 97 and also mod 71, it follows, in view of Lemmas 3 and 2, that there exist pairs $(\beta_1, \beta_2) \in \{0, 1, ..., 95\}^2$ and $(\gamma_1, \gamma_2) \in \{0, 1, ..., 69\}^2$ satisfying

$$\begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \pmod{96}, \tag{2.26}$$

and

$$\begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \pmod{70}, \tag{2.27}$$

where the units $\zeta_1^{\beta_1} \zeta_2^{\beta_2}$ and $\zeta_1^{\gamma_1} \zeta_2^{\gamma_2}$ are acceptable modulo 97 and 71, respectively. With the aid of a computer we found that the unit $\zeta_1^{\beta_1} \zeta_2^{\beta_2}$ is acceptable modulo 97 only if $(\beta_1, \beta_2) = (0, 0)$, (0, 48), (24, 24), (24, 72), (48, 0), (48, 48), (72, 24), or (72, 72). In particular, (2.26) then implies that both b_1 and b_2 are even. But then, in view of (2.27) and Lemma 2, both γ_1 and γ_2 are even too. The same computer program also found that, if the unit $\zeta_1^{\gamma_1} \zeta_2^{\gamma_2}$ is acceptable mod 71, then $(\gamma_1, \gamma_2) \in \{(0, 0), (0, 35), (11, 14), (40, 43), (63, 29)\}$. Since both γ_1 and γ_2 are even, this leaves only $(\gamma_1, \gamma_2) = (0, 0)$ and hence, by (2.27), we obtain $(b_1, b_2) \equiv (0, 0) \pmod{70}$. ∎

Lemma 4 proves that, if $p = 71$, then condition (2.17) is satisfied also. Thus, working with $p = 71$, only condition (2.18) remains to be proven. This will be done in the following section.

4. We apply Skolem's p-adic method to prove that (2.18) is satisfied. We have $\alpha + \theta = -3 + 6\rho + 3\rho^2 - 2\rho^3 + \eta + \eta\rho$ and for a typical unit $\zeta \in \mathcal{U}_0$, we put

$$\zeta = A_0 + A_1\rho + A_2\rho^2 + A_3\rho^3 + B_0\eta + B_1\eta\rho + B_2\eta\rho^2 + B_3\eta\rho^3$$

and (2.28)

$$(\alpha + \theta)\zeta = x_0 + x_1\rho + x_2\rho^2 + x_3\rho^3 + y_0\eta + y_1\eta\rho + y_2\eta\rho^2 + y_3\eta\rho^3.$$

Hence

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} -3 & 2 & -3 & 2 & 44 & -31 & 31 & -44 \\ 6 & -3 & 2 & -3 & -80 & 44 & -31 & 31 \\ 3 & -2 & 9 & -6 & -31 & 44 & -80 & 145 \\ -2 & 3 & -2 & 9 & 31 & -31 & 44 & -80 \\ 1 & 0 & 0 & -1 & -3 & 2 & -3 & 2 \\ 1 & 1 & 0 & 0 & 6 & -3 & 2 & -3 \\ 0 & 1 & 1 & 4 & 3 & -2 & 9 & -6 \\ 0 & 0 & 1 & 1 & -2 & 3 & -2 & 9 \end{pmatrix} \begin{pmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \\ B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} \tag{2.29}$$

On the other hand, in view of (2.12) and (2.28),

$$\alpha X = x_0 + x_1\rho + x_2\rho^2 + x_3\rho^3, \qquad (1+\rho)\, Y = y_0 + y_1\rho + y_2\rho^2 + y_3\rho^3,$$

so that (2.13) is equivalent to the system (recall the comments immediately following (2.13))

$$\begin{cases} \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x_0 + x_1\rho + x_2\rho^2 + x_3\rho^3) = -188, \\ \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(y_0 + y_1\rho + y_2\rho^2 + y_3\rho^3) = -2, \end{cases}$$

which, in turn, is equivalent to

$$\begin{vmatrix} c_{i0} & -c_{i1} & c_{i2} & c_{i3} \\ -c_{i3} & -c_{i0} & c_{i1} + 4c_{i3} & c_{i2} \\ -c_{i2} & -c_{i3} & c_{i0} + 4c_{i2} & c_{i1} + 4c_{i3} \\ -c_{i1} - 4c_{i3} & -c_{i2} & 4c_{i1} + 15c_{i3} & c_{i0} + 4c_{i2} \end{vmatrix} = c_i \tag{2.30}$$

($i = 1, 2$), where $c_{1j} = x_j$, $c_{2j} = y_j$ ($j = 0, ..., 3$), $c_1 = -188$, and $c_2 = -2$.

In view of (2.18), we need only consider units $\zeta \in \mathscr{U}_0$ that can take the shape

$$\zeta = (\zeta_1^q)^M (\zeta_2^q)^N, \qquad \text{where } M \text{ and } N \text{ are } p\text{-adic integers}$$

(in our case $p = 71$ and $q = 70$). Thus we expand $(\zeta_1^q)^M (\zeta_2^q)^N$ in a p-adic power series in order to obtain a p-adic power series expansion for the unit $\zeta \in \mathscr{U}_0$ of the said shape. Some computer calculations showed that

$$\zeta_1^{70} \equiv 1 + 71(13\eta - 28\eta\rho + 34\eta\rho^3) \pmod{p^2},$$
$$\zeta_2^{70} \equiv 1 + 71(-31\eta - 22\eta\rho - 20\eta\rho^2 + 31\eta\rho^3) \pmod{p^2},$$

and it is easy to show that the coefficients $A_0, ..., A_3, B_0, ..., B_3$ in the 71-adic expansion of $\zeta = (\zeta_1^{70})^M (\zeta_2^{70})^N$ are

$$\begin{aligned} A_0 &= 1 + 71^2( ) & B_0 &= 71(13M - 31N) + 71^2( ), \\ A_1 &= 71^2( ), & B_1 &= 71(-28M - 22N) + 71^2( ), \\ A_2 &= 71^2( ), & B_2 &= -71 \cdot 20N + 71^2( ), \\ A_3 &= 71^2( ), & B_3 &= 71(34M + 31N) + 71^2( ), \end{aligned}$$

where in expressions like $71( )$ and $71( )^2$ we write parentheses $( )$ to indicate 71-adic integers whose exact values are immaterial.

Formula (2.29) then provides the values for the x_i's and y_i's and consequently also for the c_{ij} of formula (2.30). Note that the expansion of the determinant on the left-hand side of (2.30) does not present any calculational difficulties, because the exact values of the coefficients of p^2 are irrelevant. In this way we find that the system (2.30) is equivalent to

$$\begin{cases} 26M - 18N + 71( ) = 0 \\ -15M - 35N + 71( ) = 0 \end{cases} \quad \text{and} \quad \begin{vmatrix} 26 & -18 \\ -15 & -35 \end{vmatrix} \not\equiv 0 \pmod{71}.$$

As a result (see [22] or the footnote on p. 152 of [31]), this means that both M and N must vanish, and the proof of Theorem 1 is complete.

III. Some Technical Lemmas

1. In Section II.1 we used certain, thus far unproven, properties of the number fields $\mathbb{K}$ and $\mathbb{M}$, in order to avoid unnecessary diversions from the main line of reasoning. In the lines to follow we shall supply the missing information in a sequence of lemmas. But first we recall the definitions of the number fields involved and their interdependencies.

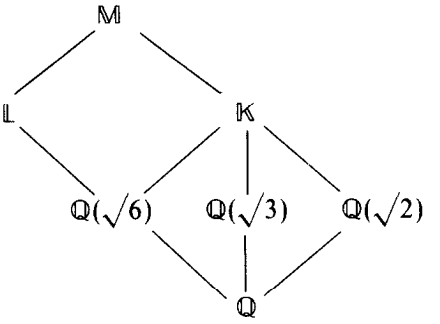
The number field $\mathbb{K} = \mathbb{Q}(\rho)$ has defining equation $\rho^4 - 4\rho^2 + 1 = 0$ and we choose $\rho = (1 + \sqrt{3})/\sqrt{2}$. The field $\mathbb{K}$ is a Galois field with automorphisms characterized by

$$\rho \mapsto \rho, \ \rho \mapsto -\rho, \ \rho \mapsto \rho^{-1}, \quad \text{and} \quad \rho \mapsto -\rho^{-1}.$$

Further, by definition, $\mathbb{L} = \mathbb{Q}(\eta)$ and $\mathbb{M} = \mathbb{Q}(\rho, \eta)$, where

$$\eta = \sqrt{75 - 31\sqrt{6}}.$$

The following diagram results:



2. We continue with a lemma on certain algebraic integers of $\mathbb{K}$. As stated before, the set $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ with $\varepsilon_1 = \rho$, $\varepsilon_2 = -2 - 3\rho + \rho^2 + \rho^3$, $\varepsilon_3 = 3 + 4\rho - \rho^2 - \rho^3$ is a set of fundamental units of $\mathbb{K}$ (see [20]).

LEMMA 5. *If for some rational integers* x, y, a_1, a_2, a_3 *the relation*

$$x + y\rho = \varepsilon_1^{a_1}\varepsilon_2^{a_2}(\varepsilon_1\varepsilon_3)^{a_3}(2 + 3\rho) \tag{3.1}$$

holds, then $a_1 \equiv a_2 \equiv a_3 \pmod 2$.

Proof. Write $A_1 = \varepsilon_1^{2a_1+1}(-1)^{a_1+a_3}$, $A_2 = \varepsilon_2^{2a_2}(-1)^{a_2+a_3}$, and $A_3 = (\varepsilon_1\varepsilon_3)^{2a_3}(-1)^{a_1+a_2}$. Elimination of $|x$ and $\|y$ from the four conjugate relations of (3.1) leads to the following identities (see (2.5) and (2.6)):

$$A_1A_2A_3(2 + 3\rho) = A_1(-2 + 3\rho) + A_2(3 + 2\rho) + A_3(-3 + 2\rho), \tag{3.2}$$

$$A_1A_2A_3(2 + 3\rho) = A_1(2 - 3\rho) + A_2\rho^2(3 + 2\rho) + A_3\rho^2(3 - 2\rho). \tag{3.3}$$

Since $\varepsilon_1 = \rho > 0$ and $A_1A_2A_3/\varepsilon_1$ is a real square, it follows that

$$A_1A_2A_3 > 0. \tag{3.4}$$

Multiplying (3.2) by ρ^2 and adding (3.3) to the result we get

$$(\rho^2 - 1)(3\rho - 2)A_1 + 2\rho^2(3 + 2\rho)A_2 = (\rho^2 + 1)(2 + 3\rho)A_1A_2A_3 > 0.$$

The coefficients of A_1 and A_2 are positive ($\rho \approx 1.93$), therefore,

$$\text{if } A_1 < 0 \text{ then } A_2 > 0 \text{ and hence } A_3 < 0, \tag{3.5}$$

in view of (3.4).

Multiplying (3.2) by ρ^2 and subtracting (3.3) leads to

$$(\rho^2 + 1)(3\rho - 2)A_1 + 2\rho^2(2\rho - 3)A_3 = (\rho^2 - 1)(2 + 3\rho)A_1A_2A_3 > 0$$

which shows that

$$\text{if } A_1 < 0 \text{ then } A_3 > 0.$$

Compare this with (3.5) to get a contradiction. Therefore A_1 is positive and by (3.4) also $A_2 A_3$ is positive. So A_2 and A_3 have the same sign. We will show that both A_2 and A_3 can only be positive.

Subtracting (3.2) from (3.3) gives

$$2(3\rho - 2)\frac{A_1}{A_2} + (2\rho - 3)(\rho^2 + 1)\frac{A_3}{A_2} = (2\rho + 3)(\rho^2 - 1). \tag{3.6}$$

Let $\pi := 2\rho - 3$; π is a prime divisor of 47 so that from $2\rho \equiv 3 \pmod{\pi}$ it follows that

$$\rho \equiv -22 \pmod{\pi}. \tag{3.7}$$

Now (3.6) implies the relation

$$2(3\rho - 2)\frac{A_1}{A_2} \equiv (2\rho + 3)(\rho^2 - 1) \pmod{\pi}. \tag{3.8}$$

Recall that $A_1/A_2 = \rho(-1)^{a_1 + a_2}(\varepsilon_1^{a_1}\varepsilon_2^{-a_2})^2$. From the assumption that A_3 is negative, it follows that $a_1 + a_2$ is odd and hence $A_1/A_2 = -\rho\varepsilon^2$, for some unit ε of $\mathbb{K}$. Consequently, by (3.8),

$$-2\rho(3\rho - 2)\varepsilon^2 \equiv (2\rho + 3)(\rho^2 - 1) \pmod{\pi}.$$

In view of (3.7), we deduce that $16\varepsilon^2 \equiv -16 \pmod{\pi}$, and thus $\varepsilon^2 \equiv -1 \pmod{\pi}$. But also, because of (3.7), ε is congruent to a rational integer modulo π, say $\varepsilon \equiv z \pmod{\pi}$ with $z \in \mathbb{Z}$. Hence $z^2 \equiv -1 \pmod{\pi}$ and this implies $z^2 \equiv -1 \pmod{47}$, which is false. This contradiction proves that both A_2 and A_3 are positive. Hence $A_i > 0$ for $i = 1, 2, 3$, and this is equivalent to $a_1 \equiv a_2 \equiv a_3 \pmod{2}$. ∎

3. Next we prove a lemma on the field $\mathbb{M}$ and its subfield $\mathbb{L}$.

LEMMA 6. (a) $\mathbb{M} = \mathbb{Q}(\rho, \eta)$ *is a quadratic extension of* $\mathbb{L} = \mathbb{Q}(\eta)$,

(b) $\mathbb{M} = \mathbb{Q}(\theta)$, *where* $\theta := \eta(1 + \rho)$,

(c) $\mathbb{M}$ *has four real embeddings and two pairs of complex conjugate embeddings.*

Proof. (a) From the definition of η, it is easily seen that $31\rho^2 + (\eta^2 - 75)\rho + 31 = 0$. Now $31t^2 + (\eta^2 - 75)t + 31 \in \mathbb{L}[t]$ is irreducible.

Because, if this were not the case then, $\rho \in \mathbb{L}$ so that $\mathbb{K} \subseteq \mathbb{L}$. It would follow that $\mathbb{K} = \mathbb{L}$, since both $\mathbb{K}$ and $\mathbb{L}$ are extensions of $\mathbb{Q}$ of degree 4. This is clearly false, because $\mathbb{K}$ is totally real and $\mathbb{L}$ is not.

(b) It is a straightforward exercise to check that the powers θ^2, θ^4, and θ^6 belong to the order $\mathbb{Z}[1, \rho, \rho^2, \rho^3]$. This means that ρ can be rationally expressed in terms of powers of θ, and the same is true for η. Thus $\rho, \eta \in \mathbb{Q}(\theta)$, so that $\mathbb{M} \subseteq \mathbb{Q}(\theta)$. On the other hand, by definition, $\mathbb{Q}(\theta) \subseteq \mathbb{M}$.

(c) The isomorphic embeddings $\sigma_i : \mathbb{M} \to \sigma_i(\mathbb{M}) \subseteq \mathbb{C}$ $(i = 1, ..., 8)$ are characterized by their action on ρ and η as follows:

$$\begin{aligned}
&\sigma_1(\rho) = \rho, && \sigma_1(\eta) = \eta; && \sigma_2(\rho) = \rho, && \sigma_2(\eta) = -\eta,\\
&\sigma_3(\rho) = -\rho, && \sigma_3(\eta) = \eta'; && \sigma_4(\rho) = -\rho, && \sigma_4(\eta) = -\eta',\\
&\sigma_5(\rho) = \rho^{-1}, && \sigma_5(\eta) = \eta; && \sigma_6(\rho) = \rho^{-1}, && \sigma_6(\eta) = -\eta,\\
&\sigma_7(\rho) = -\rho^{-1}, && \sigma_7(\eta) = \eta'; && \sigma_8(\rho) = -\rho^{-1}, && \sigma_8(\eta) = -\eta',
\end{aligned}$$

where $\eta' := \sqrt{75 + 31\sqrt{6}}$. From this the result is immediate. ∎

4. The final lemma of Section III gives information on the unitgroup of $\mathbb{M}$.

LEMMA 7. (a) *The unit group $\mathcal{U}$ of $\mathbb{M}$ has five fundamental units and the only roots of unity belonging to $\mathbb{M}$ (and hence to $\mathbb{K}$ also) are ± 1.*

(b) *The subgroup $\mathcal{U}_0$ of $\mathcal{U}$, defined by*

$$\mathcal{U}_0 = \{\varepsilon \in \mathcal{U} \cap \mathcal{O} \mid \mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\varepsilon) = +1\},$$

has two generators of infinite order and -1 is its only generator of finite order.

Proof. (a) The first assertion is a direct consequence of Lemma 6(c) and Dirichlet's unit theorem. The second assertion follows immediately from the fact that $\mathbb{M}$ has a real conjugate field.

(b) Here we are dealing with a special case of the following proposition.

PROPOSITION 2. *Let $\mathbb{K} \subseteq \mathbb{M}$ be finite extensions of $\mathbb{Q}$ with k and m fundamental units, respectively. Further let $\mathcal{O}$ be an order of $\mathbb{M}$ containing a set of $[\mathbb{K}:\mathbb{Q}]$ $\mathbb{Q}$-independent elements of $\mathbb{K}$. Then the group $\mathcal{U}_0$ of those units ε of $\mathcal{O}$ for which $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\varepsilon)$ is a root of unity has $m - k$ generators of infinite order.*

Proof. Let $\{\lambda_1, ..., \lambda_m\}$ be a set of fundamental units of the order $\mathcal{O}$ and

let $\mathcal{U}_{\mathcal{O}} := \langle \lambda_1, ..., \lambda_m \rangle$ be the group generated by these fundamental units. Consider the subgroup $\mathcal{U}_1$ of $\mathcal{U}_{\mathcal{O}}$ consisting of those units $\lambda \in \mathcal{U}_{\mathcal{O}}$ for which $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\lambda)$ is a root of unity. Then clearly, every $u \in \mathcal{U}_0$ is of the form $u = \zeta \cdot u_1$, where $u_1 \in \mathcal{U}_1$ and ζ is a root of unity belonging to $\mathbb{M}$. Thus we have to show that $\mathcal{U}_1$ has rank $m-k$ as a free abelian group.

Let $\{\varepsilon_1, ..., \varepsilon_k\}$ be a set of fundamental units for $\mathbb{K}$ and put $\mathcal{U}_{\mathbb{K}} := \langle \varepsilon_1, ..., \varepsilon_k \rangle$. We define a homomorphism $\phi: \mathcal{U}_{\mathcal{O}} \to \mathcal{U}_{\mathbb{K}}$ as follows: if $\lambda \in \mathcal{U}_{\mathcal{O}}$ and $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\lambda) = \zeta \cdot \varepsilon$ with $\varepsilon \in \mathcal{U}_{\mathbb{K}}$ and root of unity ζ belonging to $\mathbb{K}$, then $\phi(\lambda) := \varepsilon$. Clearly, $\mathrm{Ker}\, \phi = \mathcal{U}_1$. Since $\phi(\mathcal{U}_{\mathcal{O}})$ is a subgroup of $\mathcal{U}_{\mathbb{K}}$, it is a free abelian group of rank $\leqslant k$.

On the other hand, by hypothesis, $\mathcal{O} \cap \mathbb{K}$ is a full module of $\mathbb{K}$ and consequently it is an order of $\mathbb{K}$. Therefore, it contains a set of k fundamental units $\{\varepsilon_1', ..., \varepsilon_k'\} \subseteq \mathcal{U}_{\mathcal{O}}$. If $d = [\mathbb{M}:\mathbb{K}]$, then $\phi(\varepsilon_1') = \varepsilon_i'^d$ $(i = 1, ..., k)$ and therefore the subgroup $\phi(\langle \varepsilon_1', ..., \varepsilon_k' \rangle)$ of $\phi(\mathcal{U}_{\mathcal{O}})$ has rank k. We conclude that $\phi(\mathcal{U}_{\mathcal{O}}) \cong \mathbb{Z}^k$. Recall that $\mathcal{U}_{\mathcal{O}} \cong \mathbb{Z}^m$ and $\mathrm{Ker}\, \phi = \mathcal{U}_1$. Hence (see [12, lemma on p. 44]), $\mathcal{U}_{\mathcal{O}} = \mathcal{U}' \oplus \mathcal{U}_1$, where $\mathcal{U}'$ is a subgroup of $\mathcal{U}_{\mathcal{O}}$, isomorphic to $\phi(\mathcal{U}_{\mathcal{O}})$. Hence, $\mathbb{Z}^m \cong \mathbb{Z}^k \oplus \mathcal{U}_1$ so that $\mathcal{U}_1$ is of rank $m-k$, as claimed. ∎

Part (b) of Lemma 7 follows immediately from this proposition. To see this, note that in our particular case $\mathbb{M}$ and $\mathbb{K}$ have 5 and 3 fundamental units, respectively, while the only possible roots of unity are ± 1. On the other hand, there are no units $\varepsilon \in \mathbb{M}$ with $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\varepsilon) = -1$. Indeed, every $\varepsilon \in \mathbb{M}$ has the form $\alpha + \beta\eta$ with $\alpha, \beta \in \mathbb{Q}(\rho)$, so that $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\varepsilon) = \alpha^2 - \beta^2\eta^2 = |\alpha + \beta\eta|^2 \geqslant 0$. Thus the group $\mathcal{U}_0$ defined in the statement of Proposition 2 coincides in our particular case with the $\mathcal{U}_0$ of Lemma 7(b). Also $\mathcal{O} \cap \mathbb{K}$ contains $4 = [\mathbb{K}:\mathbb{Q}]$ $\mathbb{Q}$-independent elements, namely $1, \rho, \rho^2$, and ρ^3, so that Proposition 2 applies to show that $\mathcal{U}_0$ has two generators of infinite order. Also the generators of finite order are the roots of unity and hence by (a), -1 is the only such possibility.

This completes the proof of the lemma. ∎

IV. Discussion

1. In this section it is our aim to show that the method we used to solve Eq. (1.1) is worth trying on quartic Thue equations of a more general type. The successive stages of the method are labeled by capitals.

We consider the quartic Thue equation

$$f(x, y) = c \tag{4.1}$$

under the following assumptions:

(1) *The root ρ of the equation $f(x, 1) = 0$ is an algebraic integer, and the number field $\mathbb{K} = \mathbb{Q}(\rho)$ is a totally real normal field.*

(2) *A finite set $S := \{(u_i, v_i),\ i = 1, ..., m\}$ of solutions to* (4.1) *is known (we aim to prove that this solution set is complete).*

Clearly (4.1) is equivalent to

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x - y\rho) = c.$$

STAGE A. *Prove that for every solution (x, y) of Eq.* (4.1) *a pair $(u, v) \in S$ exists for which the ideal relation*

$$(x - y\rho) = (u - v\rho) \tag{4.2}$$

can be verified.

This is accomplished using factorization in $\mathbb{K}$ and possibly a few more or less standard tricks.

STAGE B. *Find a set of fundamental units for $\mathbb{K}$.*

This task is rather more difficult. In fact, sometimes, a substantial computational effort is needed. For general methods that deal with the problem of constructing fundamental units, we refer the reader to [20] (in this paper one finds, among other things, a table of 20 totally real quartic fields with their corresponding sets of fundamental units), [8], and [3]. In an appendix of a forthcoming paper by B. M. M. de Weger and N. Tzanakis [32] the reader will find an adaptation of Billevič's algortihm [3] to the case of a totally real quartic field.

STAGE C. *For each $(u, v) \in S$, or at least for those (u, v) representing the different ideals $(u - v\rho)$, reduce ideal Eq.* (4.2) *in the unknown rational integers x and y to an equation of the form*

$$\alpha X^2 + \beta Y^2 = \alpha + \beta, \text{ where } \alpha, \beta \text{ are known elements of } \mathbb{K} \text{ with } \alpha\beta > 0 \text{ and } X, Y \text{ are unknown units of } \mathbb{K}. \tag{4.3}$$

For $\alpha \in \mathbb{K}$, we shall denote the algebraic conjugates of α by $\alpha^{(i)}$, $i = 1, ..., 4$. Let ε_j, $j = 1, 2, 3$, be a triad of positive fundamental units of $\mathbb{K}$ (i.e., of the maximal order of $\mathbb{K}$; we can, however, work with any order of $\mathbb{K}$ containing ρ). Now (4.2) is equivalent to

$$x - y\rho = \nu \cdot \mu, \qquad \text{with } \mu := u - v\rho \text{ and } \mathbb{K}\text{-unit } \nu \tag{4.4}$$

and we would like to prove that $v = \pm 1$ is the only possibility. Since we expect v to be ± 1, we hope to be able to prove at this stage at least that for $i \neq j$, $v^{(i)}/v^{(j)}$ is a square in $\mathbb{K}$. In the case of Eq. (1.1), this is implied by Lemma 5, Section III.1. We suppose in the sequel that we have established this fact.

For distinct $i, j, k \in \{1, 2, 3, 4\}$, set $\tau_{ijk} := (\rho^{(i)} - \rho^{(j)})\,\mu^{(k)}$. Combining the three i, j, k-conjugate relations of (4.4), we get on eliminating x and y

$$\tau_{ijk} v^{(k)} + \tau_{jki} v^{(i)} + \tau_{kij} v^{(j)} = 0. \tag{4.5}$$

From the definition of τ_{ijk} it also follows that

$$\tau_{ijk} + \tau_{jki} + \tau_{kij} = 0,$$

which shows that i, j, k can be chosen such that

$$\operatorname{sign}(\tau_{jki}) = \operatorname{sign}(\tau_{kij}) = -\operatorname{sign}(\tau_{ijk}).$$

For this choice, setting

$$v^{(i)}/v^{(k)} =: X^2,\ v^{(j)}/v^{(k)} =: Y^2,\ \tau_{jki} =: \alpha,\ \tau_{kij} =: \beta$$

in (4.5), we see that Eq. (4.3) is obtained.

From our discussion it is clear that v in (4.4) can attain no other values than ± 1, if it can be shown that (4.3) can have no solutions but those given by $(|X|, |Y|) = (1, 1)$. Thus, from here on we direct our efforts to proving that the only solutions of (4.3) are given by $|X| = |Y| = 1$.

STAGE D. *Reduce* (4.3) *to a system of equations to which Skolem's p-adic method can be applied.*

This reduction can be achieved by working in a certain quadratic extension of $\mathbb{K}$. Write (4.3) as

$$(\alpha X)^2 - (\theta Y)^2 = \alpha(\alpha + \beta), \tag{4.6}$$

where $\theta^2 := -\alpha\beta$, so that $\theta \in i\mathbb{R}$. Therefore, $\mathbb{M} := \mathbb{K}(\theta)$ is a quadratic extension of $\mathbb{K}$ and an octic extension of $\mathbb{Q}$. The Galois group of the extension $\mathbb{M}:\mathbb{K}$ is generated by the automorphism characterized by $\theta \mapsto -\theta$. For elements of $\mathbb{M}$ we shall use the dash ($'$) to indicate conjugation under this automorphism.

Since we expect to prove that the only solutions to (4.6) are given by $|X| = |Y| = 1$, and because $(\alpha+\theta)(\alpha-\theta) = \alpha^2 - \theta^2 = \alpha(\alpha+\beta)$, it seems reasonable to expect that for suitable choices of the signs of X and Y, we can prove the ideal relation $(\alpha X + \theta Y) = (\alpha+\theta)$, using ideal factorization in the extension $\mathbb{M}:\mathbb{K}$. This, in turn, implies

$$\alpha X + \theta Y = \zeta(\alpha+\theta), \qquad \text{for some unit } \zeta \text{ of } \mathbb{M}. \tag{4.7}$$

Its conjugate relation is $\alpha X - \theta Y = \zeta'(\alpha-\theta)$, which gives on multiplication by (4.7)

$$\alpha(\alpha+\beta) = (\alpha X)^2 - (\theta Y)^2 = (\alpha X + \theta Y)(\alpha X - \theta Y) = \zeta\zeta'(\alpha^2 - \theta^2) = \zeta\zeta'\alpha(\alpha+\beta),$$

so that $\zeta\zeta' = 1$. Therefore the unknown unit $\zeta \in \mathbb{M}$ has the special property that

$$\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\zeta) = +1. \tag{4.8}$$

So our problem reduces to the task of finding all units $\zeta \in \mathbb{M}$ with relative norm $+1$ (see (4.8)), and with the property that the corresponding X and Y are units of $\mathbb{K}$.

Solving (4.7) and its conjugate equation for X and Y, we obtain the following expressions

$$X = \frac{\zeta(\alpha+\theta) + \zeta^{-1}(\alpha-\theta)}{2\alpha}, \qquad Y = \frac{\zeta(\alpha+\theta) - \zeta^{-1}(\alpha-\theta)}{2\theta} \tag{4.9}$$

for which

$$\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(X) = \pm 1 \qquad \text{and} \qquad \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(Y) = \pm 1. \tag{4.10}$$

Our work environment is an order $\mathcal{O} = \mathbb{Z}[1, \rho, \rho^2, \rho^3, \eta, \eta\rho, \eta\rho^2, \eta\rho^3]$ of $\mathbb{M}$, where η is some conveniently chosen algebraic integer of $\mathbb{M}$ such that $\theta/\eta \in \mathbb{K}$, not belonging to $\mathbb{K}$. Let $\mathcal{U}$ be the unit group of $\mathcal{O}$ and $\mathcal{U}_0$ its subgroup consisting of those units of $\mathcal{U}$ with norm relative to $\mathbb{K}$ equal to ± 1. In view of Proposition 2, (Section III.3), $\mathcal{U}_0$ has $m-3$ generators of infinite order, where m is the number of corresponding generators of $\mathcal{U}$. The number m depends on the number r of real embeddings of $\mathbb{M}$ and, since $\theta \in i\mathbb{R}$, $r = 0, 2, 4,$ or 6 with $m = 3, 4, 5,$ or 6, respectively. Assuming that the infinite generators for $\mathcal{U}_0$ can be constructed, our unit ζ may be expressed in terms of at most three unknown rational integral exponents. As we have

only two equations (4.10), we must exclude the case $r = 6$. This leaves us with two equations in at most two unknowns.

For $\zeta \in \mathcal{U}_0$, we set

$$\zeta = A_0 + A_1\rho + A_2\rho^2 + A_3\rho^3 + B_0\eta + B_1\eta\rho + B_2\eta\rho^2 + B_3\eta\rho^3, \quad (4.11)$$

where the A_i's and B_i's are unknown rational integers. From (4.9) we find, after some tedious computations (recall that $X, Y \in \mathbb{K}$),

$$\alpha X = x_0 + x_1\rho + x_2\rho^2 + x_3\rho^3, \qquad \frac{\theta}{\eta} Y = y_0 + y_1\rho + y_2\rho^2 + y_3\rho^3, \quad (4.12)$$

where the x_i's and y_i's are linear expressions in the A_i's and B_i's with explicitly known rational coefficients. These resulting expressions for αX and $(\theta/\eta)Y$ in terms of the A_i's and B_i's will be used in the equations (4.10).

A method that is worth trying for solving these equations (4.10) is the p-adic method of Skolem. Although there is no theoretical guarantee, it is our experience that in each particular instance the chances that it will work are rather good.

STAGE E. *Try to apply Skolem's p-adic method to* (4.10) *for a suitable choice of the prime p.*

We only discuss the most difficult case, corresponding to $r = 4$, $m = 5$, in which $\mathcal{U}_0$ has two infinite generators; from this discussion it is easy to see how to deal with the simpler cases.

To start with, we construct a pair of independent units ζ_1, ζ_2 of $\mathcal{U}_0$. This requires much computational power. To get an idea of what is involved, we refer the reader to Section 4 of [27], where the case of Eq. (1.1) is considered.

Next we check the conditions of Proposition 1 (Section II.2). If condition (2.16) is not satisfied, then the algorithm of Theorem 2 of Subsection 2 below can be applied in order to find a new pair (ζ_1, ζ_2) that does satisfy (2.16). However, in that case non-trivial computations are needed. There is no theoretical guarantee that condition (2.17) can be satisfied. An appropriate choice of the prime p, however, makes this highly probable. Suppose therefore that conditions (2.16) and (2.17) are already fulfilled. In view of Proposition 1 it remains to show that (2.18) is also fulfilled. Thus we need to consider only those units $\zeta \in \mathcal{U}_0$ that can be written in the form

$$\zeta = (\zeta_1^q)^M (\zeta_2^q)^N, \qquad \text{where } M \text{ and } N \text{ are } p\text{-adic integers.} \quad (4.13)$$

Since ζ_1 and ζ_2 are explicitly known, we can compute ζ_1^q and ζ_2^q modulo p^2 and then expand $(\zeta_1^q)^M (\zeta_2^q)^N$ in a p-adic power series to obtain p-adic

power series expressions for the A_i's and B_i's appearing in (4.11). These expressions will have the form

$$\begin{aligned} A_0 &= 1 + p \cdot f_0(M, N) + p^2(\ ), \qquad A_i = p \cdot f_i(M, N) + p^2(\ ), \\ B_j &= p \cdot g_j(M, N) + p^2(\ ), \qquad\qquad i = 1, 2, 3,\ j = 0, 1, 2, 3, \end{aligned} \tag{4.14}$$

where the f_i's and g_j's are linear forms in M and N with p-adic integral coefficients. As before, in expressions like $p(\ )$ and $p^2(\ )$ we write parentheses $(\ )$ to indicate p-adic integers whose exact values are immaterial. By means of (4.14) we can find the p-adic power series expressions for the x_i's and y_i's appearing in (4.12). Inserting these in the equations (4.10), where X and Y are replaced by their expressions in terms of the x_i's and y_i's, and adopting only one of the four possible sign-combinations leads to a system of the form

$$\begin{aligned} c_{11}M + c_{12}N + p(\ ) &= 0 \\ c_{21}M + c_{22}N + p(\ ) &= 0, \end{aligned} \tag{4.15}$$

where the coefficients are explicitly known p-adic integers. If $\det(c_{ij}) \not\equiv 0 \pmod{p}$ (this is highly probable if p is not very small, say, if $p > 10$), then Skolem's result, mentioned at the end of Section II, implies that $(M, N) = (0, 0)$ is the only solution of (4.15) and, consequently, the only acceptable unit ζ of the form (4.13) is 1. This confirms condition (2.18), as required.

2. The study of the diophantine equations of the previous section gives cause for venturing some remarks of a more general nature.

The setting of the problem is provided by two algebraic number fields $\mathbb{K}$ and $\mathbb{M}$, where $\mathbb{M}$ is a finite extension of $\mathbb{K}$, and an order $\mathcal{O}$ of $\mathbb{M}$ such that $\mathcal{O} \cap \mathbb{K}$ is an order of $\mathbb{K}$ and such that the group $\mathcal{U}_0$ of units $\varepsilon \in \mathcal{O}$ with $\mathrm{Norm}_{\mathbb{M}/\mathbb{K}}(\varepsilon) = \pm 1$ has two generators of infinite order, while -1 is its only generator of finite order. We want to prove that the only units $\zeta \in \mathcal{U}_0$ having a certain property (such units are called *acceptable*) are ± 1. If $\mathcal{U}_0 = \langle -1, \lambda_1, \lambda_2 \rangle$ then, equivalently, we want to show that the only acceptable unit of the form $\lambda_1^{b_1}\lambda_2^{b_2}$ $(b_1, b_2 \in \mathbb{Z})$ is 1 and our aim is to construct a proof which uses Skolem's p-adic method, with a convenient choice for the prime p.

In order to apply this method it is not strictly necessary to construct a pair of generators λ_1, λ_2; a pair of independent units ζ_1, ζ_2 satisfying certain weaker conditions will usually do the trick. All this is explained in Stage E of the previous section and in Sections II.2 and II.3. One may observe that the arguments used in these sections are quite general: they can be applied in any extension $\mathbb{M}:\mathbb{K}$ as above (e.g., in case $\mathbb{K} = \mathbb{Q}$ and $\mathbb{M}$

is a semi-real quartic number field) and they do not depend on the particular fields $\mathbb{K}$ and $\mathbb{M}$ that were used for the purpose of solving Eq. (1.1). Even Lemmas 2 and 4 of Section II.3, although appearing to be very special, give a clear idea of some general arguments that may be successfully applied in different settings. An analogous remark can be made for the theorem that we prove below: although the notations and the phrasing of proof and algorithm clearly depend on the particular extension $\mathbb{M}:\mathbb{K}$, the reader is invited to agree that this does not play an essential role.

3. From here on we shall refer to the notations, etc., of Sections II.2 and II.3 without explicitly stating so.

In Proposition 1 we refered to certain conditions the independent units ζ_1 and ζ_2 must satisfy. The most important one, which enables the pair ζ_1, ζ_2 to "behave p-adically as a pair of generators of infinite order for $\mathcal{U}_0$," is the validity of the relation (2.16). In the particular example that we study in the present paper, the requirement mentioned above turns out to be $(D, 2\cdot 3\cdot 5\cdot 7\cdot 71)=1$, whose validity was proved in Lemma 2.

One may object, however, that in our particular example we were lucky in finding a pair ζ_1, ζ_2 for which the corresponding D *happened to be prime* to 2, 3, 5, 7, and 71, so that only verification of this fact was needed. But—and this is the point of the objection—how would we have acted upon finding a pair ζ_1, ζ_2 with corresponding D being divisible by some $p \in \{2, 3, 5, 7, 71\}$? A general answer is implicit in the following result.

THEOREM 2. *Let p be any rational prime. Then, given a pair ζ_1, ζ_2 of independent units of $\mathcal{O}$, there exists an algorithm for deciding whether $D \not\equiv 0 \pmod p$ or $D \equiv 0 \pmod p$. In the latter case a new pair of independent units ζ_1^*, ζ_2^* of $\mathcal{O}$ can be explicitly constructed, such that $\langle \zeta_1, \zeta_2 \rangle$ is a proper subgroup of $\langle \zeta_1^*, \zeta_2^* \rangle$ and the corresponding D^* is not divisible by p.*

Remarks. (i) In view of this result, the validity of condition (2.16) can be effectively checked. If it is found that (2.16) is false, then, by Theorem 2, the pair ζ_1, ζ_2 can be replaced by a new, explicitly calculated pair, which satisfies condition (2.16).

(ii) As will be obvious from the proof (see Section 4 below), the algorithm mentioned in the theorem may involve a considerable amount of calculations, especially if p is large ($p > 100$, say). Therefore, it is recommended to first try the elementary method described in the proof of Lemma 2. There is a very good chance that this method will work in case D proves to be prime to p. The authors have worked out several numerical examples, not published here; see also various examples in [7]. However, if $D \equiv 0 \pmod p$, then for every choice of the rational prime $\pi \equiv 1 \pmod p$, this elementary method obviously must fail. In practice this means that, if

arguments analogous to those of Lemma 2 will not work for several choices of $\pi \equiv 1 \pmod{p}$, there is reason to suspect that D is divisible by p. One then may proceed to try the algorithm described in the proof of Theorem 2. This is exactly what happened with the initial value of ζ_2 we discovered when considering integral elements of $\mathbb{M}$ of small norm (see Section 4 of [27]). Indeed, we found the following ζ_2-value:

$$449677 - 917900\rho + 183580\rho^3 + 42264\eta - 77646\eta\rho - 21132\eta\rho^2 + 25882\eta\rho^3. \tag{4.16}$$

For $p = 2$, our attempts for various choices of $\pi \equiv 1 \pmod{p}$ failed, which made us suspect that the unit (4.16) is a perfect square of a unit of $\mathcal{O}$. Indeed, running the algorithm alluded to in Theorem 2 with $p = 2$ on a computer, we established the fact that the unit (4.16) is the square of the unit ζ_2 mentioned in the first few lines of Section II.3. Subsequently, the program, run with this new ζ_2-value, showed that this ζ_2 is not a perfect square of any unit of $\mathcal{O}$, a fact which is also proved in Lemma 2.

(iii) In view of Lemma 1, $D \equiv 0 \pmod{p}$ if either $\zeta_1\zeta_2^s$ or $\zeta_1^s\zeta_2$ is a perfect pth power in $\mathcal{O}$ for some $s \in \{0, 1, ..., p-1\}$. In general, it seems very unlikely that $\zeta_1\zeta_2^s$ or $\zeta_1^s\zeta_2$ is a pth power with p relatively large, say $p > 10$. This means that the values of p for which the method of Lemma 2 fails, i.e., the values of p dividing D, most likely are small, so that the algorithm described in the proof of Theorem 2 will not involve too many computations and hence may be applied without particular difficulties.

4. We now proceed to prove Theorem 2.

As already noted in Remark (iii) above, it suffices to describe an algorithm which does the following:

(1) Given any unit $\xi \in \mathcal{O}$, it decides whether ξ is a perfect pth power in $\mathcal{O}$, and

(2) if, using (1), it finds some $\zeta_1\zeta_2^s$ or $\zeta_1^s\zeta_2$ with $s \in \{0, 1, ..., p-1\}$ to be a pth power in $\mathcal{O}$, it replaces the pair (ζ_1, ζ_2) with a new pair (ζ_1^*, ζ_2^*) as in the statement of Theorem 2.

In the sequel we shall describe such an algorithm.

Suppose $\xi = \lambda^p$ for some $\lambda \in \mathcal{O}$ and put

$$\lambda = x_0 + x_1\rho + x_2\rho^2 + x_3\rho^3 + y_0\eta + y_1\eta\rho + y_2\eta\rho^2 + y_3\eta\rho^3. \tag{4.17}$$

Using the notation of Lemma 6 (see also Lemma 4 of [27]), we recall that

$\sigma_1, ..., \sigma_8$ are the isomorphic embeddings of $\mathbb{M}$, where $\sigma_3, \sigma_4, \sigma_7\ \sigma_8$ are real and $\sigma_1, \sigma_2, \sigma_5, \sigma_6$ are non-real with

$$\sigma_2(\alpha) = \overline{\sigma_1(\alpha)} \qquad \text{and} \qquad \sigma_6(\alpha) = \overline{\sigma_5(\alpha)}, \qquad \text{for every } \alpha \in \mathbb{M},$$

the bar denoting complex-conjugation.

Thus, the relation $\xi = \lambda^p$ implies

$$\sigma_i(\xi) = \sigma_i(\lambda)^p, \qquad \text{for} \quad i = 1, ..., 8. \tag{4.18}$$

In particular, $\sigma_i(\lambda) = \sigma_i(\xi)^{1/p}$, $i = 3, 4, 7, 8$ and since the left-hand side is a real number, it follows that the right-hand side can only have one possible value if $p > 2$ and two possible values if $p = 2$, for each $i \in \{3, 4, 7, 8\}$. On the other hand, from (4.18) it follows that $\sigma_i(\lambda) = \sigma_i(\xi)^{1/p}$ for $i = 1, 2$, and for these values of i the right-hand side represents p possible complex values. Further, since $\sigma_2(\lambda) = \overline{\sigma_1(\lambda)}$, also $\sigma_2(\xi)^{1/p}$ must be the complex-conjugate of $\sigma_1(\xi)^{1/p}$. Similarly, $\sigma_i(\lambda) = \sigma_i(\xi)^{1/p}$ for $i = 5, 6$ and $\sigma_5(\xi)^{1/p}$, $\sigma_6(\xi)^{1/p}$ are complex conjugates. Consequently,

$$\begin{pmatrix} \sigma_1(\lambda) \\ \vdots \\ \sigma_8(\lambda) \end{pmatrix} = \begin{pmatrix} \sigma_1(\xi)^{1/p} \\ \vdots \\ \sigma_8(\xi)^{1/p} \end{pmatrix} \tag{4.19}$$

and the number of possible values for the right-hand side column is p^2 if $p > 2$ and 64 if $p = 2$. These values can be explicitly calculated; the third, fourth, seventh, and eight elements are real numbers while the first and second, as well as the fifth and sixth, are complex conjugates. On the other hand, in view of (4.17) and the definition of the σ_i's, the left-hand side column of (4.19) has the form

$$\mathscr{D}\begin{pmatrix} x_0 \\ \vdots \\ x_3 \\ y_0 \\ \vdots \\ y_3 \end{pmatrix},$$

where $\mathscr{D}$ is an invertible 8×8 matrix. Then (4.19) implies

$$\begin{pmatrix} x_0 \\ \vdots \\ x_3 \\ y_0 \\ \vdots \\ y_3 \end{pmatrix} = \mathscr{D}^{-1} \begin{pmatrix} \sigma_1(\xi)^{1/p} \\ \vdots \\ \sigma_8(\xi)^{1/p} \end{pmatrix}. \tag{4.20}$$

The matrix $\mathscr{D}^{-1}$ is given explicitly on page 24 of [27] in the case of Eq. (1.1).

Now, in view of (4.20), the matrix multiplication on the right-hand side of (4.20) must result in a *rational integral* column vector. Thus, once the (complex valued) elements of the right-hand side of (4.20) have been computed to a good precision (in our case double precision, i.e., 16 decimal digits, proved very satifactory), it is easy to check whether a particular choice of the complex column vector on the right-hand side of (4.19) gives rise to a rational integral column vector after being multiplied by $\mathscr{D}^{-1}$. If it does, then $\xi = \lambda^p$, with λ as in (4.17), where $x_0, ..., x_3, y_0, ..., y_3$ are the elements of the rational integral column vector. If, however, for every possible choice of the complex vector on the right-hand side of (4.19) the product on the right-hand side of (4.20) is *not* a rational integral column, then ξ is not a perfect pth power in $\mathscr{O}$.

Thus, the algorithm described above satisfies condition (1). Moreover, if ξ is in fact a pth power of an element of $\mathscr{O}$, it finds this element.

Next we check condition (2). Suppose, without loss of generality, that

$$\zeta_1 \zeta_2^s = \zeta_3^p. \tag{4.21}$$

Then

$$G_1 := \langle \zeta_1, \zeta_2 \rangle \subseteq \langle \zeta_2, \zeta_3 \rangle =: G_2.$$

Note that $\zeta_3 \notin G_1$, because in view of (4.21), a relation $\zeta_3 = \zeta_1^m \zeta_2^n$ implies that $mp = 1$, which is absurd. Hence $G_1 \neq G_2$.

If the determinant D corresponding to the pair ζ_2, ζ_3 satisfies $D \not\equiv 0 \pmod{p}$ then we put $\zeta_1^* := \zeta_2$, $\zeta_2^* := \zeta_3$ and we are done. Otherwise we repeat the process with ζ_2, ζ_3 instead of ζ_1, ζ_2, obtaining thus a new group of units G_3, whose two generators are explicitly known. Moreover, G_2 is a proper subgroup of G_3. Continuing in this way we obtain a chain (G_i) of distinct groups: $G_1 \subset G_2 \subset G_3 \subset \cdots \subset G_n \subset \cdots \subset G := \langle \lambda_1, \lambda_2 \rangle$. As the factor group G/G_1 is finite (in fact $\#(G/G_1) = |D|$), this chain has to be finite, which means that from some n onwards G_i $(i \geqslant n)$ remains constant. As a result, if $G_n = \langle \zeta_1^*, \zeta_2^* \rangle$, then the determinant corresponding to ζ_1^*, ζ_2^* does not vanish modulo p, as required.

ACKNOWLEDGMENT

The authors express their gratitude to a referee whose comments led to substantial improvements of the presentation.

REFERENCES

1. A, BAKER, Contributions to the Theory of Diophantine Equations I/II: On the representation of integers by binary forms/The Diophantine equation $y^2 = x^3 + k$, *Philos. Trans. Royal Soc. London Ser. A.* **263** (1967/1968), 173–208.
2. A. BAKER AND H. DAVENPORT, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* **20** (1969), 129–137.
3. K. K. BILLEVIČ, On the unit of algebraic fields of third and fourth degree, *Math. Sbornik* **40** (1956), 123–136.
4. J. BLASS *et al.*, On Mordell's equation $y^2 + k = x^3$, preprint.
5. J. BLASS *et al.*, "Practical Solutions to Thue Equations of Degree 4 over the Rational Integers," Preliminary Report, 1986.
6. Z. I. BOREVICH AND R. SHAFAREVICH, "Number Theory," (Chap. 4, Section 6), Academic Press, New York/London, 1973.
7. A. BREMNER, Integral generators in a certain quartic field and related diophantine equations, *Michigan Math. J.* **32** (1985), 295–319.
8. J. BUCHMANN, On the computation of units and class numbers by a generalization of Lagrange's algorithm, preprint.
9. F. B. COGHLAN AND N. M. STEPHENS, The Diophantine equation $y^2 - k = x^3$, *in* "Computers in Number Theory" (A. O. Atkin and B. J. Birch, Eds.), Academic Press, New York, 1971; Proceedings of the Atlas Symposium, No. 2, pp. 199–205, 1969.
10. W. J. ELLISON, "Recipes for Solving Diophantine Problems by Baker's Method," Sém. Th. Nombr. 1970–1971, Exp. No. 11, Lab. Théorie des Nombres, C.N.R.S., Talence, 1971.
11. W. J. ELLISON *et al.*, The Diophantine equation $y^2 + k = x^3$, *J. Number Theory* **4** (1972), 107–117.
12. S. LANG, "Algebra," Addison–Wesley, Reading, MA, 1970.
13. D. J. LEWIS, Diophantine equations: p-adic Methods, *in* "Studies in Number Theory" (W. J. LeVeque, Ed.), Vol. 6, MAA Studies in Mathematics, 1969.
14. W. LJUNGGREN, Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante, *Acta Math.* **75** (1942), 1–21.
15. W. LJUNGGREN, "Diophantine Equations: A p-adic Approach," Lectures given at the University of Nottingham in 1968. Notes prepared by R. R. Laxton.
16. W. LJUNGGREN, On the representation of integers by certain binary cubic and biquadratic forms, *Acta Arithm.* **XVII** (1971), 379–387.
17. L. J. MORDELL, "Diophantine Equations," Chap. 23, Academic Press, New York/London, 1969.
18. YU. V. MATIYASEVICH, Diophantine representation of enumerable predicates, *Izv. Akad. Nauk. SSSR Ser. Mat.* **35** (1971), 3–30.
19. A. PETHŐ AND R. SCHULENBERG, Effectives Lösen von Thue Gleichungen, *Publ. Math. Debrecen*, to appear.
20. M. POHST AND H. ZASSENHAUS, On effective computation of fundamental units I & II (with Peter Weiler), *Math. Comp.* **38** (1982), 275–291, 293–329.
21. R. J. RUDMAN AND R. P. STEINER, A generalization of Berwick's unit algorithm, *J. Number Theory* **10** (1978), 16–34.

22. T. SKOLEM, "Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen," pp. 163–188, 8de Skand. Mat. Kongr., Stockholm, 1934.
23. T. SKOLEM, The use of p-adic methods in the Theory of Diophantine Equations, *Bull. Soc. Math. Belg.* **7** (1955), 83–95.
24. R. P. STEINER, On the units in algebraic number fields, *in* "Proceedings, 6th Manitoba Conference in Num. Math., 1976," pp. 413–435.
25. R. P. STEINER, On Mordell's equation $y^2 - k = x^3$: A problem of Stolarsky, *Math. Comp.* **46** (1986), 703–714.
26. R. J. STROEKER, On the Diophantine equation $x^3 - Dy^2 = 1$, *Nieuw Arch. Wisk.* (3) **24** (1976), 231–255.
27. R. J. STROEKER AND N. TZANAKIS, "On Certain Norm Form Equations Associated with a Totally Real Biquadratic Field," Report 8607/B, Econometric Inst. Erasmus Un. Rotterdam, 1986.
28. A. THUE, Über Annäherungswerte algebraischer Zahlen, *J. Reine Angew. Math.* **135** (1909), 284–305.
29. N. TZANAKIS, The Diophantine equation $x^3 - 3xy^2 - y^3 = 1$ and related equations, *J. Number Theory* **18**, No. 2 (1984), 192–205; Corrigendum, *J. Number Theory* **19** (1984), 296.
30. N. TZANAKIS, On the Diophantine equation $x^2 - Dy^4 = k$, *Acta Arithm.* **46**, No. 3 (1986), 257–269.
31. N. TZANAKIS, On the Diophantine equation $2x^3 + 1 = py^2$, *Manuscripta Math.* **54** (1985), 145–164.
32. N. TZANAKIS AND B. M. M. DE WEGER, On the practical solution of Thue equations, in preparation.