Publ. Math. Debrecen
92/3-4 (2018), 293–315
DOI: 10.5486/PMD.2018.7848

Computing relative power integral bases in a family of quartic extensions of imaginary quadratic fields

By ZRINKA FRANUŠIĆ (Zagreb) and BORKA JADRIJEVIĆ (Split)

Abstract. Let $M = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with the ring of integers $\mathbb{Z}_M$, and let ξ be a root of the polynomial $f(x) = x^4 - 2cx^3 + 2x^2 + 2cx + 1$, where $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3. We consider an infinite family of octic fields $K_c = M(\xi)$ with the ring of integers $\mathbb{Z}_{K_c}$. Our goal is to determine all generators of a relative power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$. We show that our problem reduces to solving the system of relative Pellian equations $cV^2 - (c+2)U^2 = -2\mu$, $cZ^2 - (c-2)U^2 = 2\mu$, where μ is a unit in $\mathbb{Z}_M$. We solve the system completely and find that all non-equivalent generators of power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$ are given by $\alpha = \xi$, $2\xi - 2c\xi^2 + \xi^3$ for $|c| \geq 159108$ and $|c| \leq 1000$, $c \notin S_c$ (where S_c is a set of exceptional cases, $|S_c| = 28$). Also, we find that, in all the above cases, $\mathcal{O}$ admits no absolute power integral basis if $-D \equiv 2, 3 (\mathrm{mod}\, 4)$.

1. Introduction

Let K be an algebraic number field of degree n, $\mathbb{Z}_K$ its ring of integers, and $\{1, \omega_2, \ldots, \omega_n\}$ an integral basis of K. It is a classical problem in algebraic number theory to decide if there exists an element $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \in \mathbb{Z}_K$ such that powers of α constitute a *power integral basis*, i.e., an integral basis of the form $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$. It has been shown that if such an α exists, then

$$I(x_2, \ldots, x_n) = \pm 1, \tag{1}$$

Mathematics Subject Classification: 11D57, 11R04, 11J86, 11J68, 11Y50.
Key words and phrases: index form equations, relative power integral basis, system of relative Pellian equations.
This paper is supported by the Croatian Science Foundation under the project No. 6422.

where $I(X_2, \ldots, X_n)$ is a homogenous polynomial of degree $\frac{n(n-1)}{2}$ with rational integer coefficients called *index form.* Hence, solving (1) in rational integers yields all generators of the power integral basis and the Diophantine equation (1) is called an *index form equation.*

Index form equations are mostly very complicated Diophantine equations. In some particular types of fields, by studying the structure of index form, a correspondence between the index form equation and simpler types of equations has been found (for a survey, see [4]). In [6], [7], I. Gaál, A. Pethő and M. Pohst showed that a resolution of index form equations in any quartic field can be reduced to the resolution of cubic and several corresponding Thue equations. In [5], I. Gaál and M. Pohst extended some basic ideas and developed a method of determining generators of a power integral basis to relative quartic extension fields K over base fields M.

Algorithms for solving index form equations have been applied to several infinite parametric families of certain fields. In particular, I. Gaál and T. Szabó in [8] applied the method described in [5] to three infinite parametric families of octic fields that are quartic extensions of imaginary quadratic fields. By using results on infinite parametric families of relative Thue equations given in [11] and [10], they found all non-equivalent generators of a relative power integral basis for infinite values of parameter.

In this paper, we consider an infinite family of octic fields $K_c = M(\xi)$ with the ring of integers $\mathbb{Z}_{K_c}$, where M is an imaginary quadratic field with the ring of integers $\mathbb{Z}_M$, and ξ is a root of the polynomial

$$f(t) = t^4 - 2ct^3 + 2t^2 + 2ct + 1, \tag{2}$$

where $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3. Since an integral basis of K_c is not known in a parametric form, our goal is to determine all generators of a relative power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ (instead of $\mathbb{Z}_{K_c}$ over $\mathbb{Z}_M$). The elements of $\mathcal{O}$ that differ by a unit factor or a translation by an element of $\mathbb{Z}_M$ have the same relative indices, and are called *equivalent.* Therefore, it is enough to find all non-equivalent generators of a relative power integral basis, and it has been shown that there are only finitely many such generators.

The paper is organized as follows. In Section 2, we briefly describe the method of I. Gaál and M. Pohst given in [5]. In Section 3, we apply that method to the problem described above. We show that our problem reduces to solving a system of relative Pellian equations over M, and we apply some results given in [10]. In Section 4, by combining the *congruence method* with an extension of Bennett's theorem given in [10], we solve the system completely and find all

non-equivalent generators of a power integral basis of $\mathcal{O}$ over $\mathbb{Z}_M$ if the absolute value of the parameter c is large enough ($|c| \geq 159108$). In Section 5, we assume that $|c| < 159108$ and apply a theorem of Baker and Wüstholz, and a version of the reduction procedure due to Baker and Davenport. Without proving that the corresponding linear form $\Lambda \neq 0$, we cannot apply Baker's theory. The proof of it given in 5.1 is long and rather complicated. We were not able to perform reduction procedure for all values of $|c| < 159108$, because we estimated that it would last more than 10^{10} sec. (in *Mathematica* on a simple PC). So, we have performed reduction procedure for $|c| \leq 1000$. Section 6 is devoted to the exceptional cases $c \in S_c$. In the last section, we examine whether the order $\mathcal{O} = \mathbb{Z}_M[\xi]$ admits an absolute power integral basis. Our main result is the following theorem.

Theorem 1. *Assume that D is a square-free positive integer, $M = \mathbb{Q}(\sqrt{-D})$ is an imaginary quadratic field with the ring of integers $\mathbb{Z}_M$, and ξ is a root of the polynomial* (2)*, where $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3. Then $K_c = M(\xi)$ is an octic field and all non-equivalent generators of a power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ are given by*

$$\alpha = \xi, \quad 2\xi - 2c\xi^2 + \xi^3, \tag{3}$$

in each of the following cases:

(i) *for all D and $|c| \geq 159108$,*

(ii) *for all D, $c \notin S_c$ and $|c| \leq 1000$ or $\mathrm{Re}(c) = 0$, where*

$$S_c = \Big\{\pm 1, \pm\sqrt{-1}, \pm 1 \pm \sqrt{-1}, \pm 2 \pm \sqrt{-1}, \pm 1 \pm \sqrt{-2}, \pm 1 \pm \sqrt{-3}, \frac{\pm 1 \pm \sqrt{-3}}{2}, \frac{\pm 3 \pm \sqrt{-3}}{2}\Big\}, \tag{4}$$

with mixed signs.

Proof of Theorem 1. Immediate from Corollary 5, Propositions 15, 21 and Corollary 20. □

The current work supports the following conjecture.

Conjecture 2. *All non-equivalent generators of a power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ are given by* (3)*, for all D and $c \notin S_c \cup \{0, \pm 2\}$.*

Also, we prove the following theorem.

Theorem 3. *If $D \equiv 2, 3 \pmod 4$, then $\mathcal{O}$ admits no absolute power integral basis consisting of elements of the form $A + \varepsilon\alpha$, where $\varepsilon \in M$ is a unit, $A \in \mathbb{Z}_M$, and α is given by* (3)*. In particular, in cases* (i) *and* (ii) *of Theorem 1, $\mathcal{O}$ admits no absolute power integral basis.*

2. Preliminaries

Since we are going to apply the method of I. Gaál and M. Pohst given in [5], we begin with a brief description of it. Let M be a field of degree m, and $K = M(\xi)$ its quartic extension generated by an algebraic integer ξ with relative minimal polynomial

$$f(t) = t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 \in \mathbb{Z}_M[t].$$

Let $\mathbb{Z}_K$ and $\mathbb{Z}_M$ denote the ring of integers of K and M, respectively. Also, assume that d is the smallest natural number with the property $d\mathbb{Z}_K \subseteq \mathbb{Z}_M[\xi]$ and $i_0 = \left[\mathbb{Z}_K^+ : \mathbb{Z}_M[\xi]^+\right]$. Then each $\alpha \in \mathbb{Z}_K$ can be represented in the form

$$\alpha = \frac{1}{d}\left(a + x\xi + y\xi^2 + z\xi^3\right), \quad a, x, y, z \in \mathbb{Z}_M. \tag{5}$$

The (absolute) index of α can be factorized in the form $I(\alpha) = [\mathbb{Z}_K^+ : \mathbb{Z}_M[\alpha]^+] \cdot [\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+]$. An element α generates a relative power integral basis of K over M if and only if the relative index $I_{K/M}(\alpha) = \left[\mathbb{Z}_K^+ : \mathbb{Z}_M[\alpha]^+\right]$ of α is equal to 1. Let

$$F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 \tag{6}$$

be a binary cubic form over $\mathbb{Z}_M$, and

$$Q_1(x, y, z) = x^2 - xya_1 + y^2a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1a_2) + z^2(a_2^2 + a_4 - a_1a_3), \tag{7}$$

$$Q_2(x, y, z) = y^2 - xz - yza_1 + a_2z^2 \tag{8}$$

be ternary quadratic forms over $\mathbb{Z}_M$. If $\alpha \in \mathbb{Z}_K$ given by (5) generates a relative power integral basis of $\mathbb{Z}_K$ over $\mathbb{Z}_M$, then there is a solution $(u, v) \in \mathbb{Z}_M^2$ of

$$F(u, v) = \delta\varepsilon, \tag{9}$$

where

$$u = Q_1(x, y, z), \quad v = Q_2(x, y, z), \tag{10}$$

δ is an integer in M of the norm $\pm d^{6m}/i_0$, and ε is a unit in M. Hence, in (9), the full set of nonassociated elements δ of the norm $\pm d^{6m}/i_0$ has to be considered.

In order to find all non-equivalent generators of a relative power integral basis of $\mathbb{Z}_K$, the first step consists of determining all (nonassociated) solutions $(u, v) \in$

$\mathbb{Z}_M^2$ of (9). In the next step, we have to find all $(x, y, z) \in \mathbb{Z}_M^3$ corresponding to a fixed solution (u, v). To this purpose, we solve the equation

$$Q_0(x, y, z) = uQ_2(x, y, z) - vQ_1(x, y, z) = 0. \tag{11}$$

It is possible to decide if (11) has nontrivial solutions, and if so, all solutions of (11) can be given in a parametric form (with two parameters p and q). By substituting these parametric representations of u and v into the original system (10), it can be shown that at least one of the equations in (10) is a quartic Thue equation over $\mathbb{Z}_M$. By solving that Thue equation, we are able to determine all parameters $(p, q) \in \mathbb{Z}_M^2$ up to unit factors in M. Hence, we can calculate all $(x, y, z) \in \mathbb{Z}_M^3$ up to a unit factor of M, as well. Then all generators of a power integral basis of $\mathbb{Z}_K$ over $\mathbb{Z}_M$ are of the form $\alpha = \frac{1}{d}(a + \eta(x\xi + y\xi^2 + z\xi^3))$, where $a \in \mathbb{Z}_M$, and the unit $\eta \in M$ is arbitrary. Consequently, all generators α of a power integral basis of $\mathbb{Z}_K$ over $\mathbb{Z}_M$ are determined up to equivalence (i.e., up to multiplication by units in M or translation by elements in $\mathbb{Z}_M$), so it is enough to look for those of the form $\alpha = \frac{1}{d}(x\xi + y\xi^2 + z\xi^3)$. Also, there are finitely many non-equivalent generators of a power integral basis of $\mathbb{Z}_K$ over $\mathbb{Z}_M$.

Our purpose is to describe the relative power integral bases of either $\mathcal{O} = \mathbb{Z}_K$ over $\mathbb{Z}_M$ (if the integer basis of K is known) or that of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$. Note that in the case $\mathcal{O} = \mathbb{Z}_M[\xi]$, ξ itself is a generator of a relative power integral basis, but we wonder if there exists any other non-equivalent generator of power integral bases. Also, we have $i_0 = d = 1$.

3. Simultaneous Pellian equations

Let D be a square-free positive integer, and let $M = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field with the ring of integers $\mathbb{Z}_M$. Let ξ be a root of the polynomial (2), where $c \in \mathbb{Z}_M$. The field $K_c = M(\xi)$ is an octic field if and only if the polynomial (2) is irreducible over $\mathbb{Z}_M$.

Lemma 4. *The polynomial $f(t)$ given in* (2) *is reducible over $\mathbb{Z}_M$ if and only if $c = 0, \pm 2$ or $c = \pm 1$ and $D = 1$ or 3.*

Proof. Let ξ be a root of the polynomial $f(t)$ given in (2), where $c \in \mathbb{Z}_M$. Since $f(t)$ is a monic polynomial with coefficients in $\mathbb{Z}_M$, ζ is an algebraic integer over M. Hence, if f is reducible over $\mathbb{Z}_M$, then f can be factorized as a product of at least two non-constant monic polynomials with coefficients in $\mathbb{Z}_M$. It is enough to observe the following cases: $f(t) = \left(t^2 + at + b\right)\left(t^2 + dt + h\right)$ and

$f(t) = (t+b)\left(t^3+at^2+dt+h\right)$, where $a,b,d,h \in \mathbb{Z}_M$. The first case leads to the system

$$a+d=-2c, \quad b+h+ad=2, \quad bd+ah=2c, \quad bh=1, \tag{12}$$

and the second to the system

$$a+b=-2c, \quad d+ab=2, \quad h+bd=2c, \quad bh=1. \tag{13}$$

Since in both cases we have $bh=1$, it follows that b,h are units in $\mathbb{Z}_M$ and (b,h), $(h,b) \in A \cap \mathbb{Z}_M^2$, where $A = \left\{(1,1),(-1,-1),(i,-i),\left(\omega,\omega^2\right),\left(-\omega,-\omega^2\right)\right\}$ and $\omega = \frac{-1+\sqrt{-3}}{2}$. By solving (12) and (13), we obtain that the polynomial f is reducible only if one of the following holds:

(1) $c=0$, $f(t) = \begin{cases} \left(t^2+1\right)^2, & \text{if } D \neq 1 \\ (t+i)^2(t-i)^2, & \text{if } D=1, \end{cases}$

(2) $c=\pm 2$, $f(t) = \left(t^2 \mp 2t - 1\right)^2$,

(3) $c=\pm 1$, $D=1,3$,

$$f(t) = \begin{cases} \left(t^2-(\sqrt{-3}\pm 1)t-1\right)\left(t^2+(\sqrt{-3}\mp 1)t-1\right), & \text{if } D=3 \\ \left(t^2+(\mp 1\pm i)\,t+i\right)\left(t^2+(\mp 1\mp i)\,t-i\right), & \text{if } D=1. \end{cases}$$ □

Corollary 5. *The field $K_c = M(\xi)$ is an octic field if and only if $c \in \mathbb{Z}_M \backslash \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3.*

Therefore, from now on, we assume that $c \in \mathbb{Z}_M \backslash \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3, and we consider an infinite family of octic fields $K_c = M(\xi)$ with the ring of integers $\mathbb{Z}_{K_c}$.

Since the integral basis of K_c is not known in a parametric form, our goal is to determine all non-equivalent generators α of a relative power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ (instead of $\mathbb{Z}_{K_c}$ over $\mathbb{Z}_M$). So, (9) is of the form

$$F(u,v) = (u+2v)\,(u-2\,(c+1)\,v)\,(u+2\,(c-1)\,v) = \varepsilon, \tag{14}$$

where ε is a unit in M, i.e., $\varepsilon \in \{\pm 1, \pm i, \pm\omega, \pm\omega^2\} \cap \mathbb{Z}_M$, and (7), (8) can be rewritten as

$$\begin{aligned} Q_1(x,y,z) &= x^2 + 2cxy + 2y^2 + 4(c^2-1)xz + 6cyz + z^2(4c^2+5), \\ Q_2(x,y,z) &= y^2 - xz + 2cyz + 2z^2. \end{aligned}$$

According to (14), we conclude that $u-2v$, $u-2(c+1)v$, $u+2(c-1)v$ are units in $\mathbb{Z}_M$, and that implies $v=0$. Therefore, all solutions of (14) are given by $(u,v)=(\eta,0)$, where η is a unit in $\mathbb{Z}_M$. Since $v=0$, equation (11) implies

$$Q_2(x,y,z)=y^2-xz+2cyz+2z^2=0, \tag{15}$$

and $(x,y,z)=(2,0,1)$ is one nontrivial solution of (15). Therefore, all solutions can be parameterized by

$$x=2r+p, \quad y=q, \quad z=r, \tag{16}$$

where $p,q,r\in M$ and $r\neq 0$. By substituting (16) into (15), we obtain $q^2=r(p-2cq)$. Further, if we multiply (16) by $k=p-2cq$, we get

$$kx=2q^2+p^2-2cqp, \quad ky=qp-2cq^2, \quad kz=q^2. \tag{17}$$

We can assume that $k,p,q\in\mathbb{Z}_M$, and since the corresponding determinant equals 1, the parameter k must be a unit in $\mathbb{Z}_M$. Now, by substituting kx,ky,kz given by (17) into the equation $Q_1(x,y,z)=\eta$ (η is a unit in $\mathbb{Z}_M$), we obtain

$$p^4-2cp^3q+2p^2q^2+2cpq^3+q^4=\mu, \tag{18}$$

where $\mu=k^2\eta$ is a unit in $\mathbb{Z}_M$. This is a relative Thue equation over $\mathbb{Z}_M$, and it can be transformed into a system of Pellian equations

$$cV^2-(c+2)U^2=-2\mu, \quad (c-2)U^2-cZ^2=-2\mu, \tag{19}$$

by putting

$$U=p^2+q^2, \quad V=p^2+2pq-q^2, \quad Z=-p^2+2pq+q^2. \tag{20}$$

Both equations in (19) are of the same form as the equation already studied in [10], i.e., of the form

$$(k-1)x^2-(k+1)y^2=-2\mu. \tag{21}$$

Proposition 6 ([10, Proposition 5.2])**.** *Let $k\in\mathbb{Z}_M$, and let $\mu\in\mathbb{Z}_M$ be a unit. Suppose $|k|\geq 2$ or k is not an element of the set*

$$S=\{0,\pm 1,\pm\sqrt{-1},\pm 1\pm\sqrt{-1},\pm\sqrt{-2},\pm\sqrt{-3},\pm\omega,\pm\omega^2\},$$

with mixed signs, where $\omega=\frac{-1+\sqrt{-3}}{2}$. If equation (21) is solvable, then $\mu\in\{1,-1,\omega,\omega^2\}$. All solutions are of the form $(x,y)=(\pm x_m,\pm y_m)$, with mixed signs, where the sequences (x_m) and (y_m) are given by the recurrence relations

$$\begin{aligned} &x_0=\varepsilon, && x_1=\varepsilon(2k+1), && x_{m+2}=2kx_{m+1}-x_m, && m\geq 0,\\ &y_0=\varepsilon, && y_1=\varepsilon(2k-1), && y_{m+2}=2ky_{m+1}-y_m, && m\geq 0, \end{aligned}$$

where $\varepsilon=1,\sqrt{-1},\omega^2,\omega$ corresponds to $\mu=1,-1,\omega,\omega^2$, respectively.

Proposition 6 implies that if $c \notin S_c$, where S_c is given in (4), and if the system (19) is solvable, then $\mu \in \{1, -1, \omega, \omega^2\}$. Furthermore, if (U, V, Z) is a solution of (19), then

$$U = \pm u_m = \pm u'_n,$$

for some $n, m \in \mathbb{N}_0$, with mixed signs, where u_m, u'_n are given by

$$u_0 = \varepsilon, \qquad u_1 = \varepsilon(2c+1), \qquad u_{m+2} = (2c+2)u_{m+1} - u_m, \tag{22}$$

$$u'_0 = \varepsilon, \qquad u'_1 = \varepsilon(2c-1), \qquad u'_{n+2} = (2c-2)u'_{n+1} - u'_n, \tag{23}$$

and $\varepsilon = 1, \sqrt{-1}, \omega^2, \omega$ corresponds to $\mu = 1, -1, \omega, \omega^2$, respectively. Evidently, $U = \pm u_0 = \pm u'_0 = \pm\varepsilon$. So, the next step consists of determining eventual intersections of sequences $(\pm u_m)$ and $(\pm u'_n)$ for $m, n \geq 1$.

4. Proof of the main theorem for $|c| \geq 159\,108$

In this section, we apply the *congruence method* introduced in [2] to obtain a lower bound for $|U|$. Combining that result with a generalization of *Bennett's theorem*, we are able to solve the system (19) for large values of $|c|$.

Lemma 7. *Let $|c| \geq 2$. Sequences (u_m) and (u'_n) given by* (22) *and* (23) *satisfy the following inequalities:*

$$(2|c|-3)^m \leq |u_m| \leq (2|c|+3)^m, \quad (2|c|-3)^n \leq |u'_n| \leq (2|c|+3)^n, \tag{24}$$

for $m, n \geq 0$.

Proof. The inequality for $|u'_n|$ is given in [10, Lemma 5.5]. In a similar way, we prove the other one. □

Lemma 8. *Sequences $(\pm u_m)$ and $(\pm u'_n)$ given by* (22) *and* (23) *satisfy the following congruences:*

$$u_m \equiv \varepsilon(1 + m(m+1)c) \pmod{4c^2}, \tag{25}$$

$$u'_n \equiv (-1)^n \varepsilon(1 - n(n+1)c) \pmod{4c^2}, \tag{26}$$

for $m, n \geq 0$.

Proof. The congruence relation for u'_n has already been proved in [10, Lemma 6.2]. The other relation can easily be shown by induction. □

Proposition 9. *Let $c \notin S_c$. If $u_m = \pm u'_n$, then*

$$m \geq \sqrt{2|c| + 0.25} - 0.5 \quad \text{or} \quad n \geq \sqrt{2|c| + 0.25} - 0.5 \quad \text{or} \quad m = n = 0. \tag{27}$$

Proof. If $u_m = \pm u'_n$, then Lemma 8 implies that

$$\varepsilon(1 + m(m+1)c) \equiv \pm(-1)^n \varepsilon(1 - n(n+1)c) \pmod{4c^2}.$$

Therefore, we have the congruence relation $\varepsilon(1 \mp (-1)^n) \equiv 0 \pmod{2c}$. If $\varepsilon(1 \mp (-1)^n) \neq 0$, then $|\varepsilon(1 \mp (-1)^n)| = 2$ and $|c| = 1$, which is not possible. So, we conclude that $\mp(-1)^n = -1$ and $\varepsilon(1 + m(m+1)c) \equiv \varepsilon(1 - n(n+1)c) \pmod{4c^2}$. Furthermore,

$$\varepsilon\left(\frac{m(m+1)}{2} + \frac{n(n+1)}{2}\right) \equiv 0 \pmod{2c}. \tag{28}$$

Consider the algebraic integer $A = \frac{\varepsilon}{2}(m(m+1) + n(n+1))$. It is clear that $A \neq 0$ for $m > 0$ or $n > 0$. So, (28) implies that $|A| \geq 2|c|$. Hence, $m(m+1) \geq 2|c|$ or $n(n+1) \geq 2|c|$ imply the inequalities in (27). □

Finally, the previous proposition yields a lower bound for a nontrivial solution of equations in (19). Directly from Lemma 7 and Proposition 9, we get:

Corollary 10. *Let $c \notin S_c$, and let (U, V, Z) be a solution of the system* (19). *If $U \in \mathbb{Z}_M \backslash \{\pm\varepsilon\}$, then*

$$|U| \geq (2|c| - 3)^{\sqrt{2|c|+0.25}-0.5}.$$

Now, we will find an upper bound for $|U|$ by using a generalization of Bennett's theorem for imaginary quadratic fields stated and proved in [10]:

Theorem 11 ([10, Theorem 7.1])**.** *Let $\theta_i = \sqrt{1 + \frac{a_i}{T}}$ for $1 \leq i \leq m$, with a_i pairwise distinct imaginary quadratic integers in $K := \mathbb{Q}(\sqrt{-D})$ with $0 < D \in \mathbb{Z}$ for $i = 0, \ldots, m$, and let T be an algebraic integer of K. Furthermore, let $A := \max |a_i|$, $|T| > A$ and $a_0 = 0$, and*

$$l = c_m \frac{(m+1)^{m+1}}{m^m} \cdot \frac{|T|}{|T| - A}, \quad L = |T|^m \frac{(m+1)^{m+1}}{4m^m \prod_{0 \leq i < j \leq m} |a_j - a_i|^2} \cdot \left(\frac{|T| - A}{|T|}\right)^m,$$

$$p = \sqrt{\frac{2|T| + 3A}{2|T| - 2A}}, \quad P = |T| \cdot 2^{m+3} \frac{\prod_{0 \leq i < j \leq m} |a_i - a_j|^2}{\min_{i \neq j} |a_i - a_j|^{m+1}} \cdot \frac{2|T| + 3A}{2|T|},$$

where $c_m = \frac{3\Gamma\left(m-\frac{1}{2}\right)}{4\sqrt{\pi}\Gamma(m+1)}$, *such that* $L > 1$, *then*

$$\max\left(\left|\theta_1 - \frac{p_1}{q}\right|, \ldots, \left|\theta_m - \frac{p_m}{q}\right|\right) > cq^{-\lambda},$$

for all algebraic integers $p_1, \ldots, p_m, q \in K$, *where*

$$\lambda = 1 + \frac{\log P}{\log L} \quad \textit{and} \quad C^{-1} = 2mpP\left(\max\{1, 2l\}\right)^{\lambda-1}.$$

The first step in the application of Theorem 11 consists of choosing suitable values for θ_1 and θ_2. Let $(U, V, Z) \in \mathbb{Z}_M^3$ be a solution of the system of Pellian equations in (19). The candidates for θ_1 and θ_2 are

$$\theta_1^{(1)} = \pm\sqrt{\frac{c+2}{c}}, \quad \theta_2^{(1)} = \pm\sqrt{\frac{c-2}{c}}, \quad \theta_1^{(2)} = -\theta_1^{(1)}, \quad \theta_2^{(2)} = -\theta_2^{(1)}, \tag{29}$$

where the signs are chosen such that $|V - \theta_1^{(1)}U| < |V - \theta_1^{(2)}U|$ and $|Z - \theta_2^{(1)}U| < |V - \theta_2^{(2)}U|$. The next lemma shows that $\frac{V}{U}$ and $\frac{Z}{U}$ are good approximations to the algebraic numbers $\theta_1^{(1)}$ and $\theta_2^{(1)}$.

Lemma 12. *Let* $|c| > 2$. *If* $(U, V, Z) \in \mathbb{Z}_M^3$ *is a solution of* (19), *then*

$$\max\left\{\left|\theta_1^{(1)} - \frac{V}{U}\right|, \left|\theta_2^{(1)} - \frac{Z}{U}\right|\right\} \leq \frac{2}{\sqrt{|c|(|c|-2)}}|U|^{-2}.$$

Proof. The inequality for $\theta_2^{(1)}$ is proved in [10, Lemma 8.1]. In a similar way, we prove the other inequality for $\theta_2^{(1)}$. □

We apply Theorem 11 with $m = 2$, $\theta_1 = \theta_1^{(1)}$, $\theta_2 = \theta_2^{(1)}$, $a_1 = 2$, $a_2 = -2$, $A = 2$, $T = c$, with $|T| = |c| > 2$,

$$l = \frac{27}{64}\frac{|c|}{|c|-2}, \quad L = \frac{27}{4096}(|c|-2)^2 > 1,$$

if $|c| \geq 15, p = \sqrt{\frac{|c|+3}{|c|-2}}, \quad P = 1024(|c|+3)$, and

$$\lambda = 1 + \frac{\log 1024 + \log(|c|+3)}{\log 27 - \log 4096 + 2\log(|c|-2)}, \quad C^{-1} = 4096(|c|+3)\sqrt{\frac{|c|+3}{|c|-2}},$$

if $|c| \geq 13$.

Finally, Lemma 12 and Theorem 11, for $p_1 = V$, $p_2 = Z$ and $q = U$, give us the inequality

$$\frac{2}{\sqrt{|c|(|c|-2)}} \geq \max\left\{\left|\theta_1 - \frac{V}{U}\right|, \left|\theta_2 - \frac{Z}{U}\right|\right\} \cdot |U|^2 > C|U|^{2-\lambda}.$$

So, if $2-\lambda > 0$, then the upper bound obtained for $\log|U|$ is

$$\log|U| < \frac{1}{2-\lambda} \cdot \log\left(\frac{2C^{-1}}{\sqrt{|c|(|c|-2)}}\right). \tag{30}$$

It can be shown that $2-\lambda > 0$, for $|c| \geq 155\,352$. Now, we use the lower bound for $|U|$ given in Corollary 10, and obtain

$$\log|U| \geq (\sqrt{2|c|+0.25} - 0.5)\log(2|c|-3), \quad |c| > 2. \tag{31}$$

Comparing (30) and (31), we get an inequality which does not hold for $|c| \geq 159\,108$. Therefore, we have proved the following assertion.

Proposition 13. *For $|c| \geq 159\,108$, the only solutions of the system* (19) *are $(U,V,Z) = (\pm\varepsilon, \pm\varepsilon, \pm\varepsilon)$, with mixed signs and $\varepsilon = 1$, i, ω, ω^2 corresponding to $\mu = 1, -1, \omega$, ω^2, respectively.*

Let $(p,q) \in \mathbb{Z}_M^2$ be a solution of (18), and let $|c| \geq 159\,108$. From Proposition 13 and equations in (20), we have

$$U = p^2 + q^2 = \pm\varepsilon, \quad V = p^2 + 2pq - q^2 = \pm\varepsilon, \quad Z = -p^2 + 2pq + q^2 = \pm\varepsilon,$$

where $\varepsilon = 1$, i, ω,ω^2. Adding V and Z yields $2pq = 0, \pm\varepsilon$. Since $|2pq| \geq 2$ or $|2pq| = 0$, we have $2pq = 0$. Hence, either p or q is equal to 0, which implies $p^4 = \mu$ and $q = 0$ or $q^4 = \mu$ and $p = 0$, where $\mu \in \{1, -1, \omega, \omega^2\}$. So the following theorem is obtained immediately.

Theorem 14. *Let $c \notin S_c$. If equation* (18) *is solvable in $(p,q) \in \mathbb{Z}_M^2$, then $\mu \in \{1, -1, \omega, \omega^2\}$, where $\omega = \frac{1}{2}(-1+\sqrt{-3})$. Furthermore, if $|c| \geq 159\,108$, then all solutions of* (18) *are given by*

(1) $(p,q) \in \{(0,\pm1), (\pm1,0), (0,\pm i), (\pm i, 0)\} \cap \mathbb{Z}_M^2$ *if $\mu = 1$;*
(2) $(p,q) \in \{(0,\pm\omega), (\pm\omega, 0)\} \cap \mathbb{Z}_M^2$ *if $\mu = \omega$;*
(3) $(p,q) \in \{(0,\pm\omega^2), (\pm\omega^2, 0)\} \cap \mathbb{Z}_M^2$ *if $\mu = \omega^2$.*

Note that if $\mu = -1$ and $|c| \geq 159\,108$, then there is no solution of (18). The equations in (5), (17) and Theorem 14 imply the following proposition directly.

Proposition 15. *If $|c| \geq 159\,108$, then all non-equivalent generators of a relative power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ are $\alpha = \xi$, $2\xi - 2c\xi^2 + \xi^3$.*

Remark 4.1. Note that $(U, V, Z) = (\pm\varepsilon, \pm\varepsilon, \pm\varepsilon)$ with mixed signs and $\varepsilon = 1$, i, ω, ω^2 corresponding to $\mu = 1, -1, \omega$, ω^2, respectively, are solutions of the system (19) for all $c \in \mathbb{Z}_M$. This implies that $\alpha = \xi$, $2\xi - 2c\xi^2 + \xi^3$ are non-equivalent generators of a power integral basis for all $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3.

5. Applying Baker's theory for $|c| < 159\,108$

In this section, we apply Baker's theory on linear forms in the logarithms of algebraic numbers. So, first let us show that $u_m = \pm u'_n$ leads to such a linear form.

Assume that $|c| < 159\,108$, $c \notin S_c$ and $\mathrm{Re}(c) \geq 0$. Indeed, if $\mathrm{Re}(c) < 0$, then by replacing c in the system (19) by $-c$, we obtain the system $(c-2)U^2 - cV^2 = -2\mu$, $cZ^2 - (c+2)U^2 = -2\mu$, which corresponds to the initial system (19) by switching places of Z and V. Therefore, it is enough to observe only c's with $\mathrm{Re}(c) \geq 0$. Let us agree that the square root of a complex number $z = re^{i\varphi}$, $-\pi < \varphi \leq \pi$ is given by $\sqrt{z} = \sqrt{r}e^{i\frac{\varphi}{2}}$, i.e., the one with a positive real part (or the principal square root).

Let (U, V, Z) be a solution of the system (19). In Section 3, we showed that there exists $m \geq 0$ such that $U = \pm u_m$, where the sequence (u_m) is given by (22). Solving the recursion in (22) yields an explicit expression for u_m:

$$u_m = \varepsilon \frac{(c+\sqrt{c(c+2)})(c+1+\sqrt{c(c+2)})^m - (c-\sqrt{c(c+2)})(c+1-\sqrt{c(c+2)})^m}{2\sqrt{c(c+2)}}. \quad (32)$$

Since $\mathrm{Re}(c) \geq 0$, $|c+1+\sqrt{c(c+2)}| \cdot |c+1-\sqrt{c(c+2)}| = 1$ and $|c+1+\sqrt{c(c+2)}| \neq |c+1-\sqrt{c(c+2)}|$ for $c \neq 0, -1, -2$, we have $|c+1+\sqrt{c(c+2)}| > 1$ (and $|c+1-\sqrt{c(c+2)}| < 1$). So, we put

$$P = \frac{1}{\sqrt{c+2}}(c+\sqrt{c(c+2)})(c+1+\sqrt{c(c+2)})^m. \quad (33)$$

It is easy to show that

$$u_m = \frac{\varepsilon}{2\sqrt{c}}\left(P + \frac{2c}{c+1}P^{-1}\right), \quad (34)$$

since $\sqrt{c(c+2)} = \sqrt{c}\sqrt{(c+2)}$ if $\mathrm{Re}(c) \geq 0$ (because $\sqrt{z_1 z_2} = \sqrt{z_1}\sqrt{z_2}$ is not true in general), and

$$P^{-1} = \frac{\sqrt{c+2}}{2c}(\sqrt{c(c+2)} - c)(c+1-\sqrt{c(c+2)})^m.$$

Analogously, there exists $n \geq 0$ such that $U = \pm u'_n$, where the sequence (u'_n) is given by (23), and its explicit expression is

$$u'_n = \varepsilon \frac{(c+\sqrt{c(c-2)})(c-1+\sqrt{c(c-2)})^n - (c-\sqrt{c(c-2)})(c-1-\sqrt{c(c-2)})^n}{2\sqrt{c(c-2)}}. \quad (35)$$

Also, since $|c-1+\sqrt{c(c-2)}| \neq |c-1-\sqrt{c(c-2)}|$ for $c \neq 0, 1, 2$, and $|c-1+\sqrt{c(c-2)}| \cdot |c-1-\sqrt{c(c-2)}| = 1$, we put

$$Q = \frac{1}{\sqrt{c-2}}(c+\sqrt{c(c-2)})(c-1+\sqrt{c(c-2)})^n, \quad (36)$$

if $|c-1+\sqrt{c(c-2)}| > 1$. Alternatively, if $|c-1+\sqrt{c(c-2)}| < 1$, i.e., $|c-1-\sqrt{c(c-2)}| > 1$, we put

$$Q = \frac{1}{\sqrt{c-2}}(c-\sqrt{c(c-2)})(c-1-\sqrt{c(c-2)})^n. \quad (37)$$

To be more precise, if $\mathrm{Re}(c) > 1$ or $\mathrm{Re}(c) = 1$ and $\mathrm{Im}(c) > 0$, then Q is given by (36), and also $\sqrt{c(c-2)} = \sqrt{c}\sqrt{c-2}$. On the other hand, if $0 \leq \mathrm{Re}(c) < 1$ or $\mathrm{Re}(c) = 1$ and $\mathrm{Im}(c) < 0$, then $\sqrt{c(c-2)} = -\sqrt{c}\sqrt{c-2}$, and Q is defined by (37). Note that, in both cases, Q can be given by

$$Q = \frac{1}{\sqrt{c-2}}(c+\sqrt{c}\sqrt{c-2})(c-1+\sqrt{c}\sqrt{c-2})^n. \quad (38)$$

Similarly to the previous case, we have

$$u'_n = \pm\frac{\varepsilon}{2\sqrt{c}}\left(Q - \frac{2c}{c-2}Q^{-1}\right), \quad (39)$$

where $Q^{-1} = \frac{\sqrt{c-2}}{2c}(c-\sqrt{c}\sqrt{c-2})(c-1-\sqrt{c}\sqrt{c-2})^n$. Assuming that $u_m = \pm u'_n$, relations (34) and (39) imply

$$P \pm Q = \pm\frac{2c}{c-2}Q^{-1} + \frac{2c}{c+2}P^{-1}. \quad (40)$$

We will apply the theorem of Baker and Wüstholz from [1] to the form $\Lambda = \log \frac{|Q|}{|P|}$. So, we have to estimate the upper bound for $|\Lambda|$. If $c \in \mathbb{Z}_M \backslash \{S_c\}$, then

$$|\Lambda| < 3^{-m}, \quad |\Lambda| < (1.55)^{-n},$$

for $m, n \geq 2$, and that is enough for our purposes, since there are no solutions of $u_m = \pm u'_n$ if $m = 1$ or $n = 1$. Indeed, for $c \in \mathbb{Z}_M$, $|c| \geq \sqrt{2}$ and $\mathrm{Re}(c) \geq 0$, we have

$$|u_1|, |u'_1| \leq 2|c| + 1, \quad |u_m| > (2\sqrt{1+|c|^2} - 1)^m,$$
$$|u'_n| > (2\sqrt{1+|c|^2} - 1)^{n-1}(2|c| - 1),$$

for $m, n \geq 2$ (where the last two inequalities are obtained similarly to those in Lemma 7). Hence, $|u_1| \leq 2|c| + 1 < (2\sqrt{1+|c|^2} - 1)(2|c| - 1) \leq |u'_n|$, $|u'_1| \leq 2|c| + 1 < (2\sqrt{1+|c|^2} - 1)^2 \leq |u_m|$ for $m, n \geq 2$, and the equations $u_1 = \pm u'_n$ and $u'_1 = \pm u_m$ have no solution for $m, n \geq 2$, i.e., for $m, n \geq 1$ (because $u_1 \neq \pm u'_1$).

5.1. The condition $\Lambda \neq 0$. Without proving that $\Lambda \neq 0$, i.e., $|P| \neq |Q|$, we cannot use the theorem of Baker and Wüstholz. This proof is rather complicated and involves several cases.

First, we show that $P \neq \pm Q$. Let us assume that $P = \pm Q$. According to (40), the following cases occur:

$$\frac{c}{c^2 - 4} = 0 \quad \text{or} \quad P^2 = \frac{2c}{c^2 - 4}.$$

Neither the first one is possible, since $c \neq 0, \pm 2$, nor the other, because $|P|^2 \geq 16^2$ and $\left|\frac{2c}{c^2-4}\right| < 5$ for $|c| \geq \sqrt{2}$ and $c \neq \pm 2$.

Before presenting other cases, let us take a closer look at $|P|$ and $|Q|$ from an algebraic point of view. According to (33), we have

$$\frac{P}{\sqrt{c}} = \frac{c + \sqrt{c(c+2)}}{\sqrt{c(c+2)}}(c + 1 + \sqrt{c(c+2)})^m = a + b\alpha = a + \frac{b_1}{c+2}\alpha, \tag{41}$$

where $\alpha = \sqrt{c(c+2)}$ and $a, b_1 \in \mathbb{Z}_M$. Similarly, (36) and (37) imply that

$$\frac{Q}{\sqrt{c}} = d + e\beta = d + \frac{e_1}{c-2}\beta, \tag{42}$$

where $\beta = \sqrt{c(c-2)}$ and $d, e_1 \in \mathbb{Z}_M$. It follows straight away that

$$u_m = \frac{\varepsilon}{2}(a + b\alpha + a - b\alpha) = \varepsilon a, \quad u'_n = \frac{\varepsilon}{2}(d + e\beta + d - e\beta) = \varepsilon d,$$

where we used the explicit expressions (32) and (35) for u_m and u'_n. Since $u_m = \pm u'_n$, we get $a = \pm d$. Note that $a \neq 0$, $d \neq 0$, because $|u_m|, |u'_n| > 0$ for $m, n \geq 2$. Also,

$$\left|\frac{P}{\sqrt{c}}\right|^2 = |a|^2 + (\overline{a}b)\alpha + (a\overline{b})\overline{\alpha} + |b|^2|\alpha|^2, \quad \left|\frac{Q}{\sqrt{c}}\right|^2 = |d|^2 + (\overline{d}e)\beta + (d\overline{e})\overline{\beta} + |e|^2|\beta|^2$$

can be understood as the elements of the vector subspaces $\mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$ and $\mathrm{span}(1, \beta, \overline{\beta}, |\beta|^2)$, respectively, since the algebraic extension $\mathbb{Q}(\sqrt{-D})(\alpha, \overline{\alpha}, \beta, \overline{\beta})$ can be considered as a vector space over $\mathbb{Q}(\sqrt{-D})$ generated by the set $\{1, \alpha, \overline{\alpha}, |\alpha|^2, \beta, \overline{\beta}, |\beta|^2\}$. Before continuing with the proof, we establish the following useful claims.

Lemma 16. *If $c \notin \{0, \pm 1, \pm 2\}$, then $\alpha, \beta \notin \mathbb{Q}(\sqrt{-D})$.*

Proof. Indeed, we can show that $\alpha \in \mathbb{Q}(\sqrt{-D})$ if and only if $c = 0, -1, -2$. Note that $\alpha \in \mathbb{Q}(\sqrt{-D})$ if and only if $c(c+2) = t^2$ for some $t \in \mathbb{Z}_M$, or equivalently, if there exist $t, s \in \mathbb{Z}_M$ such that $t \pm s$ are units in $\mathbb{Z}_M$, since $c = -1 \pm \sqrt{t^2 + 1}$. It is easy to check that the only possibilities are $c = 0, -1, -2$. It can be proved similarly that $\beta \in \mathbb{Q}(\sqrt{-D})$ if and only if $c = 0, 1, 2$. □

Lemma 17. *If B_1 is a basis of the subspace $\mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$, then $B_1 = \{1, \alpha, \overline{\alpha}, |\alpha|^2\}$ or $B_1 = \{1, \alpha\}$. The set $\{1, \alpha\}$ is a basis of $\mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$ if and only if $\overline{\alpha} = A\alpha$, $A \in \mathbb{Q}(\sqrt{-D})$. The analogous statement is true for a basis of $\mathrm{span}(1, \beta, \overline{\beta}, |\beta|^2)$.*

Proof. According to Lemma 16, it is obvious that $\{1, \alpha\}$ is a linearly independent set. Let $\overline{\alpha} = A\alpha + C$, for $A, C \in \mathbb{Q}(\sqrt{-D})$. By squaring it, we obtain $2AC\alpha = \overline{\alpha}^2 - C^2 - \alpha^2 A^2 \in \mathbb{Q}(\sqrt{-D})$. Since $\alpha \notin \mathbb{Q}(\sqrt{-D})$, we have that $AC = 0$. If $A = 0$, then $\overline{\alpha} = C \in \mathbb{Q}(\sqrt{-D})$, a contradiction. If $C = 0$, then $\overline{\alpha} = A\alpha$ and $|\alpha|^2 = A\alpha^2 \in \mathbb{Q}(\sqrt{-D})$, which imply $B_1 = \{1, \alpha\}$.

The assumption that $\{1, \alpha, \overline{\alpha}\}$ is a linearly independent set leads to several contradictions (obtained similarly, but more complicated than in the previous cases). □

Lemma 18. *Let $c \notin \{0, \pm 1, \pm 2\}$. If $\beta \in \mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$, then $B_1 = \{1, \alpha, \overline{\alpha}, |\alpha|^2\}$ is a basis of the subspace $\mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$ and $\beta = A\overline{\alpha}$ or $\beta = A|\alpha|^2$, for some $A \in \mathbb{Q}(\sqrt{-D})$. The analogous statement is true if $\alpha \in \mathrm{span}(1, \beta, \overline{\beta}, |\beta|^2)$.*

Proof. Let $\beta \in \mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$. Obviously, this implies $\overline{\beta}, |\beta|^2 \in \mathrm{span}(1, \alpha, \overline{\alpha}, |\alpha|^2)$, too. If we assume that $\beta = A\alpha$ for some $A \in \mathbb{Q}(\sqrt{-D})$, then $A =$

$\pm\frac{\sqrt{c^2-4}}{c-2}$. Therefore, $c^2-4=r^2$ for some $r\in\mathbb{Z}_M$. Since $c,r\in\mathbb{Z}_M$ and $|c\pm r|\leq 4$, by checking all possibilities, we find $c=0,\pm 1,-2$. (Similarly, if $\alpha=A\beta$ for $A\in\mathbb{Q}(\sqrt{-D})$, then $c=0,\pm 1,2$).

If $B_1=\{1,\alpha\}$ is a basis of $\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2)$, then $\beta=A\alpha+C$ for some $A,C\in\mathbb{Q}(\sqrt{-D})$. Then, by squaring it, it is easy to see $\beta=C\in\mathbb{Q}(\sqrt{-D})$ or $\beta=A\alpha$, which is impossible.

If $B_1=\{1,\alpha,\overline{\alpha},|\alpha|^2\}$ is a basis of $\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2)$, then $\beta=C+A\alpha+A'\overline{\alpha}+A''\,|\alpha|^2$ for $C,A,A',A''\in\mathbb{Q}(\sqrt{-D})$. Similarly as before, we prove that one of the following possibilities occurs:

$$(1)\ \beta=C\in\mathbb{Q}(\sqrt{-D});\quad (2)\ \beta=A\alpha;\quad (3)\ \beta=A'\overline{\alpha};\quad (4)\ \beta=A''\,|\alpha|^2.$$

Therefore, we might have $\beta=A'\overline{\alpha}$ or $\beta=A''\,|\alpha|^2$, since the first two cases are impossible. □

Furthermore,

$$\left|\frac{P}{\sqrt{c}}\right|^2-\left|\frac{Q}{\sqrt{c}}\right|^2\in V=\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2,\beta,\overline{\beta},|\beta|^2).$$

There are several possibilities for choosing a basis B for V from $\{1,\alpha,\overline{\alpha},|\alpha|^2,\beta,\overline{\beta},|\beta|^2\}$:

(1) $B=\{1\}$. This happens if and only if $\alpha,\beta\in\mathbb{Q}(\sqrt{-D})$. So, this is not possible according to Lemma 16.

(2) $B=\{1,\alpha\}$ (or $B=\{1,\beta\}$). This is also not possible. Indeed, in this case, $B_1=\{1,\alpha\}$ is basis of $\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2)$ and $\beta\in\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2)$, which contradicts Lemma 18.

(3) $B=\{1,\alpha,\overline{\alpha},|\alpha|^2\}$ (or $B=\{1,\beta,\overline{\beta},|\beta|^2\}$). In this case, $\beta\in\mathrm{span}(1,\alpha,\overline{\alpha},|\alpha|^2)$ or more precisely, $\beta=A\overline{\alpha}$ or $\beta=A|\alpha|^2$ for $A\in\mathbb{Q}(\sqrt{-D})$ according to Lemma 18.

(4) $B=\{1,\alpha,\beta\}$. This implies that $\overline{\alpha}=A\alpha$ and $\overline{\beta}=C\beta$, for $A,C\in\mathbb{Q}(\sqrt{-D})$ according to Lemma 17.

(5) $B=\{1,\alpha,\beta,\overline{\beta},|\beta|^2\}$ (or $B=\{1,\alpha,\overline{\alpha},|\alpha|^2,\beta\}$). Here, we have $\overline{\alpha}=A\alpha$ for $A\in\mathbb{Q}(\sqrt{-D})$ (or $\overline{\beta}=A\beta$ for $A\in\mathbb{Q}(\sqrt{-D})$).

(6) $B=\{1,\alpha,\overline{\alpha},|\alpha|^2,\beta,\overline{\beta},|\beta|^2\}$.

In what follows, we show that $|P|\neq|Q|$ in each of the possible cases (3) to (6), unless $\mathrm{Re}(c)=0$. Assume that $|P|=|Q|$, i.e.,

$$0=\left|\frac{P}{\sqrt{c}}\right|^2-\left|\frac{Q}{\sqrt{c}}\right|^2=(\overline{a}b)\alpha+(a\overline{b})\overline{\alpha}+|b|^2|\alpha|^2-(\overline{d}e)\beta-(d\overline{e})\overline{\beta}-|e|^2|\beta|^2.\quad(43)$$

Case (6). Let $B = \{1, \alpha, \overline{\alpha}, |\alpha|^2, \beta, \overline{\beta}, |\beta|^2\}$ be a basis B for V. Since the set $\{\alpha, \overline{\alpha}, |\alpha|^2, \beta, \overline{\beta}, |\beta|^2\}$ is linearly independent, all coefficients in (43) have to be zero: $\overline{a}b = a\overline{b} = |b|^2 = \overline{d}e = d\overline{e} = |e|^2 = 0$. This implies $b = e = 0$ and $P = a\sqrt{c} = \pm d\sqrt{c} = \pm Q$, which is not possible.

Case (5). The assumption is that the set $B = \{1, \alpha, \beta, \overline{\beta}, |\beta|^2\}$ forms a basis for V. In this case, we know that $\overline{\alpha} = A\alpha$ and $|\alpha|^2 = A\alpha^2$ for $A \in \mathbb{Q}(\sqrt{-D})$. Obviously, $A \neq 0$. So, (43) implies

$$(|b|^2 A\alpha^2)1 + (\overline{a}b + a\overline{b}A)\alpha - (\overline{d}e)\beta - (d\overline{e})\overline{\beta} - |e|^2|\beta|^2 = 0.$$

The coefficients must be zero: $|b|^2 A\alpha^2 = \overline{a}b + a\overline{b}A = \overline{d}e = d\overline{e} = |e|^2 = 0$. Since $A\alpha^2 \neq 0$, we have $b = e = 0$ and $P = a\sqrt{c} = \pm d\sqrt{c} = \pm Q$, which is not possible. Similarly, we obtain a contradiction if we assume that $B = \{1, \alpha, \overline{\alpha}, |\alpha|^2, \beta\}$ is a basis for V.

Case (4). The set $B = \{1, \alpha, \beta\}$ forms a basis for V. This is a situation when $\overline{\alpha} = A\alpha, |\alpha|^2 = A\alpha^2, \overline{\beta} = C\beta, |\beta|^2 = C\beta^2$, for $A, C \in \mathbb{Q}(\sqrt{-D})$ and $A, C \neq 0$. Substituting that into (43), we get $(|b|^2 A\alpha^2 - |e|^2 C\beta^2)1 + (\overline{a}b + a\overline{b}A)\alpha - (\overline{d}e + d\overline{e}C)\beta = 0$ and $|b|^2 A\alpha^2 = |e|^2 C\beta^2$, $\overline{a}b = -a\overline{b}A$, $\overline{d}e = -d\overline{e}C$. The assumption $b, e \neq 0$, after some calculations, leads to $(b\alpha - e\beta)(b\alpha + e\beta) = 0$, and that implies that α, β are linearly dependent, which they are not, according to Lemma 18. So, $b = e = 0$ implies $P = \pm Q$ again, a contradiction!

Case (3). Recall that $\{1, \alpha, \overline{\alpha}, |\alpha|^2\}$ forms a basis of V and $\beta = A\overline{\alpha}$ or $\beta = A|\alpha|^2$ for $A \in \mathbb{Q}(\sqrt{-D})$. If $\beta = A|\alpha|^2$, then $\overline{\beta} = \overline{A}|\alpha|^2$ and $|\beta|^2 = |A|^2|\alpha|^4 \in \mathbb{Q}(\sqrt{-D})$. So, (43) implies that

$$(-|e|^2|A|^2|\alpha|^4) \cdot 1 + (\overline{a}b)\alpha + (a\overline{b})\overline{\alpha} + (|b|^2 - \overline{d}eA - d\overline{e}\,\overline{A})|\alpha|^2 = 0.$$

Therefore, $|e|^2|A|^2|\alpha|^4 = 0$, $\overline{a}b = 0, |b|^2 - \overline{d}eA - d\overline{e}\,\overline{A} = 0$. Evidently, $e = b = 0$, which imply $P = \pm Q$, a contradiction.

If $\beta = A\overline{\alpha}$, then $\overline{\beta} = \overline{A}\alpha$ and $|\beta|^2 = |A|^2|\alpha|^2$. Notice that $\overline{\beta} \neq C\beta$ for all $C \in \mathbb{Q}(\sqrt{-D})$. (If $\overline{\beta} = C\beta$, then $\beta = C^{-1}A\alpha$, which is not possible by Lemma 18.) According to (43), we have $(\overline{a}b - d\overline{e}\,\overline{A})\alpha + (a\overline{b} - \overline{d}eA)\overline{\alpha} + (|b|^2 - |e|^2|A|^2)|\alpha|^2 = 0$, and $a\overline{b} - \overline{d}eA = 0, |b|^2 - |e|^2|A|^2 = 0$. Therefore,

$$A = \frac{a\overline{b}}{\overline{d}e} = \pm\frac{a\overline{b}}{\overline{a}e}. \tag{44}$$

From (41) and (42), we obtain

$$a^2 - b^2c(c+2) = \frac{2}{c+2}, \quad a^2 - e^2c(c-2) = -\frac{2}{c-2}, \tag{45}$$

and $cb_1^2-(c+2)a^2=-2$, $(c-2)a^2-ce_1^2=-2$, which again implies

$$e^2c(c-2)-b^2c(c+2)=\frac{4c}{c^2-4}\quad\text{and}\quad(c+2)e_1^2-(c-2)b_1^2=4. \tag{46}$$

Equation (44) gives us $|e\beta|=|b\alpha|$, which gives us $\left|e_1^2\,(c+2)\right|=\left|b_1^2\,(c-2)\right|$. Let $X=(c+2)\,e_1^2$ and $Y=(c-2)\,b_1^2$. Therefore, we have $X-Y=4$ and $|X|=|Y|$. Also, $\operatorname{Re}X=2$ and $\operatorname{Re}Y=-2$. On the other hand, from (44) and (46), we obtain

$$\frac{c^2-4}{c\cdot\overline{a}^2}(\overline{b}^2a^2\overline{\alpha}^2-\overline{a}^2b^2\alpha^2)=4. \tag{47}$$

Since $\overline{b}^2a^2\overline{\alpha}^2-\overline{a}^2b^2\alpha^2=2\operatorname{Im}\left(a\overline{b}\overline{\alpha}\right)^2i$, equation (47) implies $\operatorname{Re}(\frac{1}{c\overline{a}^2}(c^2-4))=0$, or equivalently, $\operatorname{Re}(\frac{a^2}{c}(c^2-4))=0$. By (45) and $\operatorname{Re}\left((c+2)\,e_1^2\right)=2$, it follows that $\operatorname{Re}c=0$, i.e., $c=vi$, $v\in\mathbb{Z}(\sqrt{D})$, $v\neq0,\pm1$. In general, we have $\overline{\sqrt{z}}=\sqrt{\overline{z}}$, if $z\in\mathbb{C}\backslash\mathbb{R}^-$ and $\overline{\sqrt{z}}=-\sqrt{\overline{z}}$, if $z\in\mathbb{R}^-$, where $\mathbb{R}^-=\{x\in\mathbb{R}:x<0\}$. So, since $\beta=\sqrt{vi\,(vi-2)}$, $\alpha=\sqrt{vi\,(vi+2)}$ and $\overline{(vi-2)\,vi}=vi\,(vi+2)\notin\mathbb{R}^-$, we have $\beta=\overline{\alpha}$, i.e., $A=1$. Also, from $\operatorname{Re}(\frac{1}{c\overline{a}^2}(c^2-4))=0$, we get $\operatorname{Re}(\frac{-iv}{v^2+4}(\overline{a})^2)=0$, which again implies $\overline{a}=-a$ or $\overline{a}=a$. Therefore, (44) gives $e=\pm\overline{b}$, and we can distinguish four cases:

(1) if $\overline{a}=a=d$, then $e=\frac{a\overline{b}}{\overline{d}}=\overline{b}$ and $\frac{P}{\sqrt{c}}=a+b\alpha$, $\frac{Q}{\sqrt{c}}=a+\overline{b}\overline{\alpha}$;

(2) if $\overline{a}=-a$, $a=d$, then $e=\frac{a\overline{b}}{\overline{d}}=-\overline{b}$ and $\frac{P}{\sqrt{c}}=a+b\alpha$, $\frac{Q}{\sqrt{c}}=a-\overline{b}\overline{\alpha}$;

(3) if $\overline{a}=a$, $a=-d$, then $e=\frac{a\overline{b}}{\overline{d}}=-\overline{b}$ and $\frac{P}{\sqrt{c}}=a+b\alpha$, $\frac{Q}{\sqrt{c}}=-a-\overline{b}\overline{\alpha}$;

(4) if $\overline{a}=-a$, $a=-d$, then $e=\frac{a\overline{b}}{\overline{d}}=\overline{b}$ and $\frac{P}{\sqrt{c}}=a+b\alpha$, $\frac{Q}{\sqrt{c}}=-a+\overline{b}\overline{\alpha}$.

Note that each of the above cases implies that $|P|=|Q|$, and hence $\Lambda=0$. In what follows, we show that in these cases, the equation $u_m=\pm u_n'$, $m,n>0$, has no solution. First we observe that $\overline{a}=\pm a$ implies $b\alpha\neq\pm\overline{b}\overline{\alpha}$. It is enough to show that $\operatorname{Im}(b\alpha)^2\neq0$. Suppose $\operatorname{Im}(b\alpha)^2=0$. Then, (45) gives us $(b\alpha)^2=b^2c(c+2)=a^2-2/(vi+2)$. Since $\operatorname{Im}(b\alpha)^2=\operatorname{Im}a^2=0$, we get $\operatorname{Im}\frac{2}{vi+2}=0$, which again implies $v=0$, a contradiction. From (40), we obtain

$$\frac{P}{\sqrt{c}}-\frac{Q}{\sqrt{c}}=-\frac{2}{c-2}\cdot\frac{\sqrt{c}}{Q}+\frac{2}{c+2}\cdot\frac{\sqrt{c}}{P},\quad\text{if } a=d, \tag{48}$$

$$\frac{P}{\sqrt{c}}+\frac{Q}{\sqrt{c}}=\frac{2}{c-2}\cdot\frac{\sqrt{c}}{Q}+\frac{2}{c+2}\cdot\frac{\sqrt{c}}{P},\quad\text{if } a=-d. \tag{49}$$

If $\overline{a}=a=d$, then (48) implies

$$b\alpha-\overline{b}\overline{\alpha}=\frac{2}{2-vi}\cdot\frac{1}{\overline{a}+\overline{b}\overline{\alpha}}+\frac{2}{2+vi}\cdot\frac{1}{a+b\alpha}.$$

Since $\mathrm{Re}(b\alpha - \overline{b}\overline{\alpha}) = 0$ and $\mathrm{Im}\left(\frac{2}{2-vi}\cdot\frac{1}{\overline{a}+\overline{b}\overline{\alpha}} + \frac{2}{2+vi}\cdot\frac{1}{a+b\alpha}\right) = 0$, we get $b\alpha = \overline{b}\overline{\alpha}$, a contradiction. Similarly, we have obtained a contradiction in the other three cases. If $B = \{1, \beta, \overline{\beta}, |\beta|^2\}$ is a basis for V, analogous results are verified.

Note that if $c = vi$, $v \in \mathbb{Z}[\sqrt{D}]$, $v \neq 0, \pm 1$, then $\beta = \overline{\alpha}$ and, according to Lemma 18, $\{1, \alpha, \overline{\alpha}, |\alpha|^2\}$ forms a basis of $V = \mathbb{Q}(\sqrt{-D})(\alpha, \overline{\alpha}, \beta, \overline{\beta})$, that is, Case (3). Hence, we have proved the following assertion.

Proposition 19. *Let $c \notin S_c$ and $\Lambda = \log\frac{|P|}{|Q|}$. Then*

(i) $\Lambda \neq 0$ *if and only if* $\mathrm{Re}(c) \neq 0$;

(ii) *if* $\mathrm{Re}(c) = 0$, *then the equation* $u_m = \pm u'_n$ *has no solutions for* $m, n > 0$.

Corollary 20. *If $c \neq \pm\sqrt{-1}$ and $\mathrm{Re}(c) = 0$, then all non-equivalent generators of a power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ are $\alpha = \xi$, $2\xi - 2c\xi^2 + \xi^3$.*

5.2. A reduction procedure. We are now ready to apply the theorem of Baker and Wüstholz to our linear form in logarithms of algebraic numbers

$$\Lambda = \log|Q| - \log|P| = n\log\eta - m\log\vartheta + \log\xi,$$

where $\eta = |c-1+\sqrt{c}\sqrt{c-2}|$, $\vartheta = |c+1+\sqrt{c(c+2)}|$, $\xi = \left|\dfrac{\sqrt{c+2}(\sqrt{c}+\sqrt{c-2})}{\sqrt{c-2}(\sqrt{c}+\sqrt{c+2})}\right|$.

First, we have to calculate the standard logarithmic Weil height of η, ϑ and ξ. The standard logarithmic Weil height $h(\alpha)$ can be bounded by

$$\frac{1}{k}\log\left(a_0\prod_{i=1}^{k}\max\{1, |\alpha^{(i)}|\}\right),$$

where the algebraic number α is a root of $a_0\prod_{i=1}^{k}(x-\alpha^{(i)})$. Since we are able to find explicit polynomials of which these algebraic integers are zeros, the following inequalities hold: $h(\eta), h(\vartheta) < 28.12$, $h(\xi) < 271.82$. Also $h'(\eta)$, $h'(\vartheta)$ and $h'(\xi)$ are less than the corresponding values given above. Since $d \leq 32\cdot 8\cdot 8$, we get

$$-\log|\Lambda| \leq 18\cdot 4!\cdot 3^4(32\cdot 2048)^5 28.12^2\cdot 271.82\cdot\log(2\cdot 3\cdot 2048)\log l < 8.6\cdot 10^{34}\log l,$$

where $l = \max\{m, n\}$. If $l = m$, applying $|\Lambda| < 3^{-m}$ to the previous inequality, we get $\frac{m}{\log m} < 7.8\cdot 10^{34}$, which does not hold for $m \geq 6.7\cdot 10^{36}$. Therefore, we solve

$$|m\theta - n + \gamma| < \delta\cdot 3^{-m} \tag{50}$$

for $m < 6.7\cdot 10^{36}$, where $\theta = \frac{\log\vartheta}{\log\eta}$, $\gamma = -\frac{\log\xi}{\log\eta}$ and $\delta = \frac{1}{|\log\eta|}$.

Similarly, if $l = n$, we have to solve

$$|n\theta' - n + \gamma'| < \delta' \cdot 1.55^{-n} \tag{51}$$

for $n < 1.715 \cdot 10^{37}$, where $\theta' = \frac{\log \eta}{\log \vartheta}$, $\gamma' = \frac{\log \xi}{\log \vartheta}$ and $\delta' = \frac{1}{|\log \vartheta|}$.

Now we will apply the reduction method described in [2, Lemma 5]. Since our bound for the absolute value of c is huge (almost 160 000), we carried out reductions only for $|c| \leq 1000$, $c \in \mathbb{Z}_M$, and obtained that (50) and (51) have no integer solutions for $m \geq n > 31$ and $n \geq m > 67$, respectively. The reason for not achieving a better bound for m and n is that θ and θ' are very close to 1, and hence their first convergent is too large, although for certain values of c, the reduction procedure is very efficient. To illustrate this, $c = 1 + 984\sqrt{-1}$ with related $\theta' \approx 1.000000272$ and $q_1 = 3\,672\,014$ (the denominator of the first convergent) represents a non-efficient example of reduction ($m \leq n \leq 67$), while on $c = 10 + \sqrt{-61}$ with related $\theta \approx 1.039$, the reduction works much better ($n \leq m \leq 2$). Finally, we showed that the equations $u_m = \pm u'_n$ for $1 \leq m, n \leq 67$ have no solutions in $\mathbb{Z}_M$ except $c = \pm 1, \pm 2$. (Note that according to (22) and (23), u_k and u'_k are k-th degree polynomials in the variable c. So, solving $u_m = \pm u'_n$ reduces to finding roots of certain polynomials in $\mathbb{Z}_M$.) Thus, we have proved:

Proposition 21. *If $|c| \leq 1000$ and $c \notin S_c$, then all non-equivalent generators of a power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ are $\alpha = \xi$, $2\xi - 2c\xi^2 + \xi^3$.*

Computational aspects. All reductions and calculations were performed in Wolfram Mathematica 9.0 with 150-digit precision. Since the algorithm for $|c| \leq 200$, $|c| \leq 400$ and $|c| \leq 1000$ took 1718 s, 9757 s and 99710 s, respectively, we estimated that the time required to do all computations for $|c| < 159108$ would be more then 10^{10} seconds.

6. On the case $c \in S_c$

So far, we have observed the case when the parameter $c \notin S_c$, where S_c is given in (4). Note that if $c \in S_c$, then for at least one of the equations in (19) we cannot apply Lemma 6. Indeed, if $c \in S_c$, there are additional classes of solutions of the equations in (19), or there exist only finitely many solutions of those equations. Also, according to the remark at the beginning of Section 5, it is enough to observe only c's from the set S_c with $\mathrm{Re}(c) \geq 0$. Furthermore, each $c \in S_c$ belongs to exactly one imaginary quadratic field, except for $c = \pm 1$ that belong to each field $M = \mathbb{Q}\left(\sqrt{-D}\right)$. Thus, for each $c \in S_c$, $c \neq \pm 1$, we have

to find additional classes of solutions of (at least one of) the equations in (19) (see [3]), and repeat the entire procedure from the previous sections. On the one hand, this situation is much simpler, because we handle a specific value of c in the exact field, but on the other hand, we need to find intersections of at least four recursive series.

For $c = 1$, Thue equation (18) has the form

$$p^4 - 2p^3q + 2p^2q^2 + 2pq^3 + q^4 = \mu, \tag{52}$$

and the related system is

$$V^2 - 3U^2 = -2\mu, \quad U^2 + Z^2 = 2\mu. \tag{53}$$

Note that Lemma 6 can be applied on the first equation in (53) to obtain $\mu \in \{1, \omega, \omega^2\} \cap \mathbb{Q}\left(\sqrt{-D}\right)$ if $D \neq 1$, and $\mu \in \{1, -1\}$ if $D = 1$.

It can be shown that the second equation in (53) has finitely many solutions if $D = 1$, but the cases $c = \pm 1$ when $D = 1$ or 3 are excluded. If $D \neq 1, 3$, the equation $U^2 + Z^2 = 2$ has infinitely many solutions in the ring of integers $\mathbb{Z}_M$ of the field $M = \mathbb{Q}(\sqrt{-D})$ (and the form of these solutions depends on D).

7. On elements with the absolute index 1

Let $\mathbb{Q} \subset M \subset K$ be number fields with $m = [M : \mathbb{Q}]$ and $k = [K : M]$. Let $\mathcal{O}$ be either the ring of integers $\mathbb{Z}_K$ of K or an order of $\mathbb{Z}_K$. Denote by $D_{\mathcal{O}}$ and D_M the discriminant of $\mathcal{O}$ and subfield M, respectively. Also, denote by $\gamma^{(i)}$ the conjugates of any $\gamma \in M$ $(i = 1, \ldots, m)$. Let $\delta^{(i,j)}$ be the images of $\delta \in K$ under the automorphisms of K leaving the conjugate field $M^{(i)}$ fixed elementwise $(j = 1, \ldots, k)$. According to [9] for any primitive $\alpha \in \mathcal{O}$, we have

$$I_{\mathcal{O}}(\alpha) = \left[\mathcal{O}^+ : \mathbb{Z}[\alpha]^+\right] = \left[\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+\right] \cdot \left[\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+\right]. \tag{54}$$

The first factor $I_{\mathcal{O}/M}(\alpha) = [\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+]$ we call the *relative index* of α, and for the second factor we have

$$\begin{aligned} J(\alpha) &= \left[\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+\right] \\ &= \frac{1}{\sqrt{|D_M|}^{[K:M]}} \cdot \prod_{1 \le i_1 < i_2 \le m} \prod_{j_1=1}^{k} \prod_{j_2=1}^{k} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|. \end{aligned} \tag{55}$$

Generators α_0 of a relative power integral bases of $\mathcal{O}$ over M have relative index $I_{\mathcal{O}/M}(\alpha_0) = 1$. The elements

$$\alpha = A + \varepsilon \cdot \alpha_0, \tag{56}$$

(where ε is a unit in M and $A \in \mathbb{Z}_M$) have the same relative index, and are called *equivalent* with α_0 over M. Equivalently, all elements $\alpha \in \mathcal{O}$ generating a power integral basis of $\mathcal{O}$ (over $\mathbb{Q}$), that is having $I_{\mathcal{O}}(\alpha) = 1$, must be of the form (56), where α_0 has relative index $I_{\mathcal{O}/M}(\alpha_0) = 1$. For α to generate a power integral basis of $\mathcal{O}$, we must also have $J(\alpha) = 1$. Therefore, for each $\alpha_0 \in \mathcal{O}$ with relative index $I_{\mathcal{O}/M}(\alpha_0) = 1$, we have to determine the unit $\varepsilon \in M$ and $A \in \mathbb{Z}_M$ such that $J(\alpha) = 1$.

We consider the octic field $K_c = \mathbb{Q}(\xi)$, where ξ is a root of the polynomial (2), where $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3, $M = \mathbb{Q}(\sqrt{-D})$, and D is a square-free positive integer. Therefore, $m = [M : \mathbb{Q}] = 2$, and K_c is an extension of M of degree $k = [K_c : M] = 4$. We have proved that all generators of a relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over M are given by $\alpha_1 = \xi, \alpha_2 = 2\xi - 2c\xi^2 + \xi^3$, in the cases given in Theorem 1. Also, according to Remark 4.1, α_1 and α_2 are the generators of a relative power integral bases for all $c \in \mathbb{Z}_M \setminus \{0, \pm 2\}$ and $c \neq \pm 1$ if $D = 1$ or 3.

Proof of Theorem 3. Taking $\alpha_0 = \alpha_1$, α_2, we calculate $J(\alpha)$ with the α in (56). For $-D \equiv 2, 3 \pmod 4$, an integral basis of M is given by $\{1, \vartheta\}$ with $\vartheta = \sqrt{-D}$. We have $\sqrt{|D_M|}^{[K:M]} = 16D^2$. We set $c = p + q\vartheta$ with integer parameters p, q. Let $A = a + b\vartheta$ with $a, b \in \mathbb{Z}$. Note that the product (55) in $J(\alpha)$ does not depend on a. We have $\varepsilon = \pm 1$, and for $-D = -1$ we also have $\varepsilon = \pm i$. The product

$$\prod_{j_1=1}^{4} \prod_{j_2=1}^{4} \left| \alpha^{(1,j_1)} - \alpha^{(2,j_2)} \right| \tag{57}$$

is of degree 16, depending on D, p, q and b. We calculated this product by Maple, using symmetric polynomials. The result is a very complicated polynomial with integer coefficients of the above variables. We found that in each case the product (57) was divisible by $4096D^2$. Therefore, dividing it by $16D^2$ would give that the $J(\alpha)$ is divisible by 256. This implies that we cannot have $J(\alpha) = 1$, therefore we cannot have $I_{\mathcal{O}}(\alpha) = 1$. □

Computational aspects. It was very difficult to perform the calculation of the product (57). We had to do it in several steps, making simplifications by using symmetric polynomials in each step. Even so, this calculation has reached the

limits of the capacities of Maple. We were not able to perform this calculation for $-D \equiv 1 \pmod 4$.

Remark. The extended version of this paper with all technical details can be found on arXiv:1607.03064.

Acknowledgements. The authors would like to thank Professor Andrej Dujella for helpful suggestions. The idea and the proof of Theorem 3 are due to Professor István Gaál.

References

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

[2] A. Dujella and A. Pethő, A generalization of a theorem of Baker and Davenport, *Quart. J. Math. Oxford Ser. (2)* **49** (1998), 291–306.

[3] L. Fjellstedt, On a class of Diophantine equations of the second degree in imaginary quadratic felds, *Ark. Mat.* **2** (1953), 435–461.

[4] I. Gaál, Diophantine Equations and Power Integral Bases, New Computational Methods, *Birkhäuser Boston, Boston, MA*, 2002.

[5] I. Gaál and M. Pohst, Computing power integral bases in quartic relative extensions, *J. Number Theory* **85** (2000), 201–219.

[6] I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations in quartic number fields, *J. Symbolic Comput.* **16** (1993), 563–584.

[7] I. Gaál, A. Pethő and M. Pohst, Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields, *J. Number Theory* **57** (1996), 90–104.

[8] I. Gaál and T. Szabó, Relative power integral bases in infinite families of quartic extensions of quadratic fields, *JP J. Algebra Number Theory Appl.* **29** (2013), 31–43.

[9] I. Gaál, L. Remete and T. Szabó, Calculating power integral bases by using relative power integral bases, *Funct. Approx. Comment. Math.* **54** (2016), 141–149.

[10] B. Jadrijević and V. Ziegler, A system of relative Pellian equations and a related family of relative Thue equations, *Int. J. Number Theory* **2** (2006), 569–590.

[11] V. Ziegler, On a family of relative quartic Thue inequalities, *J. Number Theory* **120** (2006), 303–325.

ZRINKA FRANUŠIĆ
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
UNIVERSITY OF ZAGREB
10000 ZAGREB
BIJENIČKA 30
CROATIA
E-mail: fran@math.hr
URL: https://web.math.pmf.unizg.hr/∼fran/

BORKA JADRIJEVIĆ
FACULTY OF SCIENCE
UNIVERSITY OF SPLIT
21000 SPLIT
R. BOŠKOVIĆA 33
CROATIA
E-mail: borka@pmfst.hr
URL: http://mapmf.pmfst.unist.hr/∼borka/

(Received October 10, 2016; revised May 26, 2017)