Class number one problem for a family of real quadratic fields

by András BIRÓ

A. Rényi Institute of Mathematics

1053 Budapest, Reáltanoda u. 13-15., Hungary; e-mail: biroand@renyi.hu

Abstract. We effectively solve the class number one problem for a certain family $\mathbf{Q}\left(\sqrt{D}\right)$ $(D \in \mathcal{F})$ of real quadratic fields, where $\mathcal{F}$ is an infinite subset of the set of odd positive fundamental discriminants. The set $\mathcal{F}$ contains the Yokoi discriminants n^2+4, so our result is a generalization of the solution of Yokoi's Conjecture. But this family may contain also infinitely many fields with comparatively larger fundamental units than the fields in the Yokoi family (it may be as large as $\log^2 D$ instead of $\log D$). The proof is also a generalization of the proof of Yokoi's Conjecture.

1. Introduction

For integers $b \geq 0$, $c > 0$, $n \geq 2$ write

$$D = D_{n,b,c} := \left(b\left(1+bc\right)^n + c\right)^2 + 4\left(1+bc\right)^n,$$

and assume that D is squarefree. Let $K = K_{n,b,c} = \mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$. These discriminants appear already in [5]. The fundamental unit ϵ_D of these fields can be computed explicitly and it is $\ll \log^2 D$ (see below). Then, using Dirichlet's class number formula

$$h(D)\log\epsilon_D = D^{1/2}L(1,\chi_D)$$

Research partially supported by NKFIH (National Research, Development and Innovation Office) grants K135885, K119528 and by the Rényi Intézet Lendület Automorphic Research Group

2020 Mathematics Subject Classification: 11R11, 11R29

(where $h(D)$ denotes the class number of K, $\chi_D(n) = \left(\frac{n}{D}\right)$ is a Jacobi symbol, $L\left(s, \chi_D\right)$ is the corresponding Dirichlet L-function) and Siegel's theorem (see [3])

$$L(1, \chi_D) \gg_\epsilon |D|^{-\epsilon}$$

(which is an ineffective estimate), we see that there are only finitely many fields in this family having class number 1.

But the effective (and unconditional) determination of every field of class number one in this family is not known. Partial results were proved in [7] and in [8] (the problem was solved there for some fixed values of the pair (b,c), in particular, for the so-called Shanks sequence $b = c = 1$), and also in [1] (for $b = 0$; this case was Yokoi's Conjecture). Assuming the Riemann Hypohesis, every field of class number one in this family was determined in [6], Theorem 5.2.

In the present paper we solve the problem under the condition that b is divisible by a certain fixed positive integer N_0.

THEOREM 1.1. *Let $b \geq 0$, $c > 0$, $n \geq 2$ be integers, assume that $D_{n,b,c}$ is squarefree and the field $K_{n,b,c} = \mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$ has class number one. Suppose that N_0* divides b, *where N_0 denotes the product of* 5^2, 7, 41, 61, *and* 1861. *Then $b = 0$, and $c \in \{1, 3, 5, 7, 13, 17\}$.*

It is possible that similar statements may be proved with other specific values of N_0. However, we cannot show it with $N_0 = 1$, i.e. the class number one problem for the entire family remains open.

The $b = 0$ case of the above theorem is exactly the statement of Yokoi's Conjecture (proved in [1]). The present theorem is proved by the method of [1]. During the proof an important tool is a formula proved in [2] for the special value at 0 of a certain zetafunction belonging to a real quadratic field, which is a generalization of a similar formula of [1] proved for the Yokoi family.

By Satz 1 of [4] we know that for the fundamental unit ϵ_D of K we have

$$\epsilon_D = \frac{b\left(1+bc\right)^n + c + \sqrt{D}}{2} \left(\frac{b^2\left(1+bc\right)^n + 2 + bc + b\sqrt{D}}{2\left(1+bc\right)}\right)^n.$$

One can then see easily that if $0 < bc = O(1)$, then

$$\log^2 D \ll \log \epsilon_D \ll \log^2 D$$

(as it is noted on p 158 of [4]). One also sees that if we assume only that bc is not too large in terms of n, precisely we assume $bc > 0$ and $\log(1 + bc) = n^{o(1)}$, then we have

$$\log \epsilon_D \gg \log^{2-o(1)} D.$$

In contrast, in the Yokoi family $D = n^2 + 4$ with squarefree D, we have

$$\log \epsilon_D \ll \log D.$$

Hence we see that the method of [1] can be applied for a family with comparatively larger fundamental units than the fields in the Yokoi family.

In Section 2 our main goal is to prove Lemma 2.8 below, which shows that under the conditions of Theorem 1.1 $D_{n,b,c}$ must be a square modulo at least one element of a fixed finite set of primes (this corresponds to the Theorem of [1]). The proof (just as in [1]) ultimately depends on some computer work. But the computations needed here are exactly the same which was carried out in [1], so here we can simply refer to them. Section 2 is the most important part of the proof. It would be possible to finish the proof from this point by using the theory of reduced ideals, as in [8]. But we prefer to give a direct proof in Section 3, similarly as we proved Fact B in [1], using here some well-known results from diophantine approximation.

2. The main reasoning

Let R be the ring of algebraic integers of K, denote by $I(K)$ the set of nonzero ideals of R and by $P(K)$ the set of nonzero principal ideals of R. Let $N(a)$ be the norm of an ideal $a \in I(K)$. For $\Re s > 1$ and a character χ define

$$\zeta_{P(K)}(s, \chi) = \zeta_{P(K_{n,b,c})}(s, \chi) = \sum_{a \in P(K)} \frac{\chi(N(a))}{N(a)^s}.$$

Our first main goal is to prove Lemma 2.4 below. The statement of that lemma will be the important property of $\zeta_{P(K)}(0,\chi)$ needed in our class number problem.

LEMMA 2.1. *Let*

$$D = D_{n,b,c} := \left(b\left(1+bc\right)^n + c\right)^2 + 4\left(1+bc\right)^n$$

with integers $b \geq 0$, $c > 0$, $n \geq 2$, *and let* D *be squarefree. Let* χ *be an odd primitive character modulo* $q > 1$ *with* $(q, 2D) = 1$, *and assume that the order of* χ *is greater than* 2. *Assume that* $q|b$. *Then* $\zeta_{P(K)}(s,\chi)$ *extends meromorphically in* s *to the whole complex plane and* $\zeta_{P(K)}(0,\chi)$ *equals the sum of*

$$\frac{2}{q^2}\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right)$$

and

$$\frac{\tau\left(\chi\right)^2 L\left(2,\overline{\chi}^2\right)}{\pi^2}\chi\left(-D\right)\left(\frac{D}{q}\right)\left(b\left(1+bc\right)^n + c + 2\frac{\left(1+bc\right)^n - 1}{c}\right),$$

where $\left(\frac{D}{q}\right)$ *is the Jacobi symbol,* $\tau\left(\chi\right) = \sum_{a=1}^{q-1}\chi\left(a\right)e^{2\pi i a/q}$ *is the Gauss sum, and if* ψ *is a character, then* $L\left(s,\psi\right)$ *denotes the corresponding Dirichlet L-function.*

Proof. First let $b = 0$. Then the result is proved on p 1825 of [2] (see p 1809 there for the definition of β_χ).

Now assume that $b > 0$. Let

$$\omega_D = \frac{1+\sqrt{D}}{2}. \tag{2.1}$$

Then the regular continued fraction expansion

$$\omega_D = \left[a_0, \overline{a_1, a_2, \ldots, a_l}\right],$$

where l is the least period of the expansion can be explicitly described as follows, see Satz 1 and p 161 of [4]. We have $l = 2n+1$,

$$a_0 = \frac{1}{2}\left(b\left(1+bc\right)^n + c + 1\right), \tag{2.2}$$

for $0 \leq i \leq n-1$ we have

$$a_{2i+1} = b\left(1+bc\right)^i, \tag{2.3}$$

$$a_{2i+2} = b\left(1+bc\right)^{n-1-i}, \tag{2.4}$$

finally

$$a_{2n+1} = b\left(1+bc\right)^{n} + c. \tag{2.5}$$

Let

$$\alpha := \omega_D - a_0. \tag{2.6}$$

As in [2], for $1 \leq j \leq 2n+1$ define the relatively prime positive integers p_j and q_j by

$$\frac{p_j}{q_j} = \left[0, a_1, a_2, \ldots, a_j\right],$$

and write

$$\alpha_j := p_j - q_j \alpha.$$

Define also $\alpha_0 = -\alpha$. For $1 \leq j \leq 2n+1$ introduce the quadratic forms

$$Q_j\left(x,y\right) = \left(\alpha_{j-1}x + \alpha_j y\right)\left(\overline{\alpha_{j-1}}x + \overline{\alpha_j}y\right),$$

where $\overline{\beta}$ denotes the algebraic conjugate of $\beta \in K$. Since every α_j $(0 \leq j \leq 2n+1)$ is an algebraic integer, so for every $1 \leq j \leq 2n+1$ we have

$$Q_j\left(x,y\right) = A_j x^2 + B_j xy + C_j y^2 \tag{2.7}$$

with rational integer coefficients A_j, B_j, C_j. For these coefficients we clearly have the following formulae:

$$A_j = \alpha_{j-1}\overline{\alpha_{j-1}} = p_{j-1}^2 - p_{j-1}q_{j-1}\left(\alpha + \overline{\alpha}\right) + q_{j-1}^2\alpha\overline{\alpha}$$

for $2 \leq j \leq 2n+1$,

$$A_1 = \alpha\overline{\alpha},$$

$$B_j = \alpha_{j-1}\overline{\alpha_j} + \alpha_j\overline{\alpha_{j-1}} = 2p_{j-1}p_j + 2q_{j-1}q_j\alpha\overline{\alpha} - \left(p_{j-1}q_j + p_j q_{j-1}\right)\left(\alpha + \overline{\alpha}\right)$$

for $2 \leq j \leq 2n+1$,

$$B_1 = -\alpha\overline{\alpha_1} - \alpha_1\overline{\alpha} = 2q_1\alpha\overline{\alpha} - p_1\left(\alpha + \overline{\alpha}\right),$$

$$C_j = \alpha_j\overline{\alpha_j} = p_j^2 - p_j q_j\left(\alpha + \overline{\alpha}\right) + q_j^2\alpha\overline{\alpha}$$

for $1 \leq j \leq 2n+1$.

It is easy to check by direct computation that

$$p_1 = 1, \qquad q_1 = b,$$

$$p_2 = b\left(1+bc\right)^{n-1}, \qquad q_2 = 1 + b^2\left(1+bc\right)^{n-1}.$$

On the other hand, we have well-known recursions (see e.g. Lemma 3A of [9])

$$p_j = a_j p_{j-1} + p_{j-2}, \qquad q_j = a_j q_{j-1} + q_{j-2}$$

for $3 \leq j \leq 2n+1$. Since by the condition $q|b$ and by formulas (2.3) and (2.4) we have $q|a_j$ for $1 \leq j \leq 2n$, so we get that

$$p_1 \equiv p_3 \equiv p_5 \equiv \ldots \equiv p_{2n-1} \equiv 1 \pmod{q},$$

$$p_2 \equiv p_4 \equiv p_6 \equiv \ldots \equiv p_{2n} \equiv 0 \pmod{q},$$

$$q_1 \equiv q_3 \equiv q_5 \equiv \ldots \equiv q_{2n-1} \equiv 0 \pmod{q},$$

$$q_2 \equiv q_4 \equiv q_6 \equiv \ldots \equiv q_{2n} \equiv 1 \pmod{q}.$$

By (2.5) we have

$$a_{2n+1} \equiv c \pmod{q},$$

hence by the above relations we get

$$p_{2n+1} \equiv 1 \pmod{q}, \qquad q_{2n+1} \equiv c \pmod{q}.$$

By formulas (2.1), (2.2) and (2.6) we see that

$$\alpha = \frac{\sqrt{D}}{2} - \frac{1}{2}\left(b\left(1+bc\right)^n + c\right),$$

so

$$-\alpha - \overline{\alpha} = b\left(1+bc\right)^n + c \equiv c \pmod{q},$$

$$\alpha\overline{\alpha} = \frac{\left(b\left(1+bc\right)^n + c\right)^2 - D}{4} = -\left(1+bc\right)^n \equiv -1 \pmod{q}.$$

Then, using our expressions above for A_j, B_j, C_j and our congruences for p_j and q_j we get examining a few cases that

$$A_j \equiv (-1)^j \pmod q,$$

$$C_j \equiv (-1)^{j-1} \pmod q$$

for $1 \leq j \leq 2n+1$,

$$B_j \equiv c \pmod q$$

for $1 \leq j \leq 2n$,

$$B_{2n+1} \equiv -c \pmod q.$$

Now, applying Theorem 1 of [2] (taking into account (2.7) above and the well-know fact that $1, \frac{1+\sqrt{D}}{2}$ is an integral basis of K) we get that $\zeta_{P(K)}(0,\chi)/2$ equals the sum of

$$\frac{1}{q^2}\sum_{j=1}^{2n+1}\sum_{1\leq u,v\leq q-1} uv\chi\left((-1)^j\left(A_ju^2+B_juv+C_jv^2\right)\right) \tag{2.8}$$

and

$$\frac{\tau(\chi)^2 L\left(2,\overline{\chi}^2\right)}{2\pi^2}\chi(-D)\left(\frac{D}{q}\right)\sum_{j=1}^{2n+1} a_j\overline{\chi\left((-1)^j A_j\right)}, \tag{2.9}$$

Inserting the expressions above for the residues modulo q of A_j, B_j and C_j we get that (2.8) equals

$$\frac{1}{q^2}\sum_{j=1}^{2n}\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+(-1)^j cuv-v^2\right)+\frac{1}{q^2}\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right), \tag{2.10}$$

and (2.9) equals

$$\frac{\tau(\chi)^2 L\left(2,\overline{\chi}^2\right)}{2\pi^2}\chi(-D)\left(\frac{D}{q}\right)\sum_{j=1}^{2n+1} a_j. \tag{2.11}$$

Now,

$$\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right)+\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2-cuv-v^2\right) \tag{2.12}$$

equals (by interchanging the role of u and v in the second sum)

$$\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right)+\sum_{1\leq u,v\leq q-1} uv\chi\left(v^2-cuv-u^2\right),$$

and since χ is odd, we get that (2.12) equals zero, and hence (2.10), and so also (2.8) equals

$$\frac{1}{q^2}\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right).$$

Using (2.3), (2.4), (2.5) in (2.11) and summing the geometric series we obtain the lemma.

LEMMA 2.2. *Under the assumptions of Lemma 2.1 we have that*

$$\frac{\tau(\chi)^2 L\left(2,\overline{\chi}^2\right)}{\pi^2}\chi(-D)\left(\frac{D}{q}\right)=\sum_{0\leq u,v\leq q-1}\left(\frac{v^2}{q^2}-\frac{v}{q}\right)\chi\left(u^2+cuv-v^2\right). \qquad (2.13)$$

Proof. Note first that because of the condition $q|b$ we have

$$D=D_{n,b,c}\equiv c^2+4 \pmod q.$$

Hence Proposition 6.1 of [2] implies (writing $l=2$ there) that the left-hand side of (2.13) equals

$$\sum_{0\leq u,v\leq q-1} B_2\left(\frac{v}{q}\right)\chi\left(u^2+cuv-v^2\right),$$

where $B_2(x)=x^2-x+\frac{1}{6}$ is the second Bernoulli polynomial. Hence it is enough to show that

$$S:=\sum_{0\leq u,v\leq q-1}\chi\left(u^2+cuv-v^2\right)=0.$$

But by the substitution $(u,v)\to(-v,u)$ we see that

$$S=\sum_{0\leq u,v\leq q-1}\chi\left(v^2-cuv-u^2\right)=-S,$$

since χ is odd. The lemma is proved.

LEMMA 2.3. *Let c be an integer, let χ be an odd primitive character modulo $q>1$ with $\left(q,2\left(c^2+4\right)\right)=1$, and assume that the order of χ is greater than 2. Then*

$$\frac{2}{q^2}\sum_{1\leq u,v\leq q-1} uv\chi\left(u^2+cuv-v^2\right)+c\sum_{0\leq u,v\leq q-1}\left(\frac{v^2}{q^2}-\frac{v}{q}\right)\chi\left(u^2+cuv-v^2\right) \qquad (2.14)$$

equals

$$\frac{1}{q}A_\chi(c),$$

where for any integer a we write ($\lceil t \rceil$ is the least integer not smaller than t)

$$A_\chi(a) = \sum_{0 \le C,D \le q-1} \chi(D^2 - C^2 - aCD) \lceil (aC - D)/q \rceil (C - q).$$

Proof. Introduce the notation

$$A = A\,(C, D) = \lceil (cC - D)/q \rceil,$$

and recall from p 95 of [1] the transformation

$$T\,((C, D)) = (\hat{C}, \hat{D})$$

with

$$\hat{C} = D - cC - q\,[(D - cC)/q]\,, \quad \hat{D} = C$$

(where we use lower integer part) and the relation

$$qA = cC - D + \hat{C}.$$

Then it is easy to check that

$$\frac{1}{q} A(C - q) = \frac{1}{q^2} \left((C - q)\,(cC - D) + \hat{C}\hat{D} - q\hat{C} \right). \tag{2.15}$$

As it is noted on p 95 of [1], T is a permutation of the set of the pairs (C, D) with $0 \le C, D \le q - 1$, any orbit of T (where χ is not 0) has an even number of elements, and the value of $\chi\left(D^2 - C^2 - cCD\right)$ changes to its negative at each step by T. Then (2.15) and the definition of $A_\chi(c)$ imply that

$$\frac{1}{q} A_\chi(c) = \frac{1}{q^2} \sum_{0 \le C,D \le q-1} \chi(D^2 - C^2 - cCD)\,((C - q)\,(cC - D) - CD + qC)\,,$$

and so (writing D in place of u, $q - C$ in place of v in (2.14)) the difference of (2.14) and $\frac{1}{q} A_\chi(c)$ equals

$$-\frac{2}{q} \sum_{D=1}^{q-1} \chi\left(D^2\right) D + \frac{1}{q} \sum_{0 \le C,D \le q-1} \chi(D^2 - C^2 - cCD) D - \frac{1}{q} \sum_{0 \le C,D \le q-1} \chi(D^2 - C^2 - cCD) C. \tag{2.16}$$

It is enough to show that this is zero. Note first that

$$2\sum_{D=1}^{q-1}\chi\left(D^2\right)D=\sum_{D=1}^{q-1}\chi\left(D^2\right)D+\sum_{D=1}^{q-1}\chi\left(D^2\right)(q-D)=q\sum_{D=1}^{q-1}\chi\left(D^2\right)=0,$$

since the order of χ is greater than 2. Using again that the order of χ is greater than 2, we see that (2.16) equals

$$\frac{1}{q}\sum_{D=0}^{q}D\sum_{C \bmod q}\chi(D^2-C^2-cCD)-\frac{1}{q}\sum_{C=0}^{q}C\sum_{D \bmod q}\chi(D^2-C^2-cCD). \qquad (2.17)$$

Writing $q-D$ in place of D and $-C$ in place of C in the first sum, and similarly, $q-C$ in place of C and $-D$ in place of D in the second sum, and averaging the old and new expressions we get that (2.17) equals

$$\frac{1}{2}\sum_{D=0}^{q}\sum_{C \bmod q}\chi(D^2-C^2-cCD)-\frac{1}{2}\sum_{C=0}^{q}\sum_{D \bmod q}\chi(D^2-C^2-cCD).$$

The $D\neq 0$ part of the first sum and the $C\neq 0$ part of the second sum cancels out, while the $D=0$ part of the first sum and the $C=0$ part of the second sum is zero since the order of χ is greater than 2. The lemma is proved.

LEMMA 2.4. *Under the assumptions of Lemma 2.1 we have that*

$$q\zeta_{P(K_{n,b,c})}(0,\chi)-A_\chi(c)$$

equals $\frac{b}{q}$ times an algebraic integer, where $A_\chi(c)$ is defined Lemma 2.3.

Proof. This follows at once from Lemmas 2.1, 2.2 and 2.3 above.

If χ is a character modulo q, denote by $\mathcal{L}_\chi$ the field generated over $\mathbf{Q}$ by the values $\chi(a)$ $(1\leq a\leq q)$, and write

$$m_\chi=\sum_{a=1}^{q}a\chi(a).$$

We start to apply the class number one condition from now on. The following lemma can be proved by the reasoning on pp 87-88 of [1].

LEMMA 2.5. *For some integers $b\geq 0$, $c>0$, $n\geq 2$ assume that $D_{n,b,c}$ is squarefree and $K_{n,b,c}=\mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$ has class number one. Then, if q is an integer with $q>2$,*

$(q, 2D_{n,b,c}) = 1$, *and* χ *is a primitive character modulo* q *with* $\chi(-1) = -1$, *then we have that* $m_\chi \neq 0$, *and*

$$q\zeta_{P(K_{n,b,c})}(0,\chi)m_\chi^{-1}$$

is an algebraic integer.

LEMMA 2.6. *We use the notations and assumptions of Lemma 2.5. Assume also that there is a prime ideal* I *of* $\mathcal{L}_\chi$ *and a rational prime* r *such that* $r \in I$, $m_\chi \in I$. *Suppose that* q *divides* b, *and* r *divides* $\frac{b}{q}$. *Then* $A_\chi(c) \in I$.

Proof. By Lemmas 2.1 and 2.2 we see that $\zeta_{P(K_{n,b,c})}(0,\chi) \in \mathcal{L}_\chi$. By Lemma 2.5 above and by the condition $m_\chi \in I$ we then get $q\zeta_{P(K_{n,b,c})}(0,\chi) \in I$. Then by Lemma 2.4 above, using the conditions $r \in I$, q divides b, and r divides $\frac{b}{q}$ we obtain the lemma.

In Section 4 of [1] three characters χ_1, χ_2, χ_3 and four prime ideals $I_{1,1}$, $I_{1,2}$, I_2 and I_3 are defined (we denote here by $I_{1,1}$ the ideal given in Example 1 of [1], by $I_{1,2}$ the ideal given in Example 2 of [1], by I_2 the ideal given in Example 3 of [1], finally by I_3 the ideal given in Example 4 of [1]). We do not need here the precise definitions, only the following properties, which are clear from [1]:

χ_1 is a character modulo 175, χ_2 and χ_3 are characters modulo 61,

$$I_{1,1} \text{ is a prime ideal of } \mathcal{L}_{\chi_1},\ m_{\chi_1} \in I_{1,1},\ I_{1,1} \text{ lies above the rational prime } 61,$$

$$I_{1,2} \text{ is a prime ideal of } \mathcal{L}_{\chi_1},\ m_{\chi_1} \in I_{1,2},\ I_{1,2} \text{ lies above the rational prime } 1861,$$

$$I_2 \text{ is a prime ideal of } \mathcal{L}_{\chi_2},\ m_{\chi_2} \in I_2,\ I_2 \text{ lies above the rational prime } 1861,$$

$$I_3 \text{ is a prime ideal of } \mathcal{L}_{\chi_3},\ m_{\chi_3} \in I_3,\ I_3 \text{ lies above the rational prime } 41.$$

The following lemma is proved in [1]. It is not stated explicitly there, but following the reasoning in Sections 4, 5 and 6 of [1] we see that it is actually proved there.

LEMMA 2.7. *Assume that* c *is an integer and*

$$A_{\chi_1}(c) \in I_{1,1},\ A_{\chi_1}(c) \in I_{1,2},\ A_{\chi_2}(c) \in I_2,\ A_{\chi_3}(c) \in I_3.$$

Then $d = c^2 + 4$ *is a square for at least one of the following moduli:* $q = 5, 7, 41, 61, 1861$ *(that is,* $(d/q) = 0$ *or* 1 *for at least one of the listed values of* q*).*

LEMMA 2.8. *For some integers $b \geq 0$, $c > 0$, $n \geq 2$ assume that $D_{n,b,c}$ is squarefree and $K_{n,b,c} = \mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$ has class number one. Suppose that the product of* 41, 61, 175 *and* 1861 *divides b. Then $D_{n,b,c}$ is a square for at least one of the following moduli:* $q = 5, 7, 41, 61, 1861$.

Proof. It follows easily by combining Lemmas 2.6 and 2.7 that $c^2 + 4$ is a square for at least one such q. Since every possible q divides b, hence $D_{n,b,c}$ is also a square modulo q. The lemma is proved.

3. The end of the proof

As it is noted in the Introduction, the $b = 0$ case is proved in [1]. So we may assume $b > 0$. Let $q \in \{5, 7, 41, 61, 1861\}$ be fixed such that $D_{n,b,c}$ is a square modulo q, we know by Lemma 2.8 that there is such a q. It is well-known that the ideal (q) is then a product of two prime ideals in R; both prime ideals must have norm q. Since the class number of $K_{n,b,c}$ is 1, it follows that there is a $\beta \in R$ such that $|\beta\overline{\beta}| = q$. We will show that this is impossible.

Since 1, $\frac{1+\sqrt{D}}{2}$ is an integral basis, so we have

$$\beta = A - B\frac{1+\sqrt{D}}{2}$$

with rational integers A and B. We have $|\beta\overline{\beta}| = q$ with a prime q, so B is nonzero, and $(A, B) = 1$. The expression $|\beta\overline{\beta}|$ is invariant under the transformations $(A, B) \to (-A, -B)$ and $(A, B) \to (B - A, B)$, so we may assume that $B > 0$ and $A \geq \frac{B}{2}$. We have

$$B\left|A - B\frac{1+\sqrt{D}}{2}\right| = \frac{Bq}{\left|A - \frac{B}{2} + B\frac{\sqrt{D}}{2}\right|} \leq \frac{2q}{\sqrt{D}} < \frac{1}{2}. \tag{3.1}$$

The last inequality easily follows from $b \geq N_0$. Hence the fraction $\frac{A}{B}$ approximates $\frac{1+\sqrt{D}}{2}$ so well that by Theorem 5C of [9] $\frac{A}{B}$ must be a convergent of $\frac{1+\sqrt{D}}{2}$, i.e. we must have

$$\frac{A}{B} = [a_0, a_1, a_2, \ldots, a_j]$$

with some $j \geq 0$, where

$$\frac{1+\sqrt{D}}{2} = [a_0, a_1, a_2, \ldots]$$

is the continued fraction expansion of $\frac{1+\sqrt{D}}{2}$. By the third displayed formula on p 17 of [9] we then have

$$\frac{1}{a_{j+1}+2} \leq B\left|A - B\frac{1+\sqrt{D}}{2}\right| \leq \frac{1}{a_{j+1}}. \tag{3.2}$$

Returning to (3.1) we first get

$$\left|A - B\frac{1+\sqrt{D}}{2}\right| \leq \frac{2q}{B\sqrt{D}},$$

hence

$$\left|A - \frac{B}{2} + B\frac{\sqrt{D}}{2}\right| \leq B\sqrt{D} + \frac{2q}{B\sqrt{D}},$$

so, again by (3.1), we get

$$\frac{Bq}{B\sqrt{D} + \frac{2q}{B\sqrt{D}}} \leq B\left|A - B\frac{1+\sqrt{D}}{2}\right| \leq \frac{2q}{\sqrt{D}}. \tag{3.3}$$

So there must be an integer $j \geq 0$ such that the inequalities (3.3) and (3.2) simultaneously hold. By the description of the continued fraction expansion of ω_D (see (2.1) for this notation) during the proof of Lemma 2.1 we see that we may assume $0 \leq j \leq 2n$.

If $0 \leq j < 2n$, then by (2.3) and (2.4) we see that

$$1 \leq a_{j+1} \leq b\,(1+bc)^{n-1},$$

hence

$$\frac{1}{a_{j+1}+2} \geq \frac{1}{3b\,(1+bc)^{n-1}}.$$

By (3.3) and (3.2) we then must have

$$\frac{1}{3b\,(1+bc)^{n-1}} \leq \frac{2q}{\sqrt{D}},$$

so

$$\sqrt{D} \leq 6bq\,(1+bc)^{n-1}.$$

But $\sqrt{D} \geq b\,(1+bc)^n$, so we would get

$$1+bc \leq 6q,$$

but this is a contradiction by the conditions $b \geq N_0$, $q \leq 1861$.

We are left with the case $j = 2n$. Then by (2.5), (3.3) and (3.2) we have

$$\frac{Bq}{B\sqrt{D} + \frac{2q}{B\sqrt{D}}} \leq \frac{1}{b\,(1+bc)^n + c},$$

hence

$$b\,(1+bc)^n + c \leq \frac{\sqrt{D}}{q} + \frac{2}{B^2\sqrt{D}}.$$

But trivially

$$\sqrt{D} \leq b\,(1+bc)^n + c + 1.$$

Since $q \geq 5$, we get

$$4\frac{b\,(1+bc)^n + c + 1}{5} \leq 1 + \frac{2}{B^2\sqrt{D}}.$$

The right-hand side is clearly smaller than 3, so this is a contradiction. Theorem 1.1 is proved.

References

[1] A. Biró. Yokoi's conjecture. *Acta Arithmetica*, 106(1):85–104, 2003.

[2] A. Biró and A. Granville. Zeta functions for ideal classes in real quadratic fields, at s= 0. *Journal of Number Theory*, 132(8):1807–1829, 2012.

[3] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[4] F. Halter-Koch. Einige periodische kettenbruchentwicklungen und grundeinheiten quadratischer ordnungen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 59, pages 157–169. Springer, 1989.

[5] M.D. Hendy. Applications of a continued fraction algorithm to some class number problems. *Mathematics of Computation*, 28(125):267–277, 1974.

[6] S. Louboutin, R.A. Mollin, and H.C. Williams. Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers. *Canadian Journal of Mathematics*, 44(4):824–842, 1992.

[7] R.A. Mollin and H.C. Williams. Affirmative solution of a conjecture related to a sequence of shanks. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 67(3):70–72, 1991.

[8] R.A. Mollin and H.C. Williams. Quadratic residue covers for certain real quadratic fields. *Mathematics of Computation*, 62(206):885–897, 1994.

[9] W. M. Schmidt. Approximation to irrational numbers by rationals. In *Diophantine Approximation*, pages 1–26. Springer, 1980.