ACTA ARITHMETICA
Online First version

The class number one problem for the real quadratic fields $\mathbb{Q}(\sqrt{(an)^2+4a})$

by

András Biró and Kostadinka Lapkova (Budapest)

1. Introduction. Let us consider the quadratic fields $K=\mathbb{Q}(\sqrt{d})$ with class group $Cl(d)$ and order of the class group denoted by $h(d)$. In this paper we determine all fields $K=\mathbb{Q}(\sqrt{d})$ where $d=(an)^2+4a$ is square-free and a and n are positive odd integers such that the class number $h(d)$ is 1. It follows from Siegel's Theorem that there are only finitely many such fields, but since Siegel's Theorem is ineffective, it cannot provide the specific fields with class number one. We apply the method developed by Biró [B1] and we use the result of Lapkova [La].

We remark that the class number one problem that we consider was already suggested by Biró [B3] as a possible generalization of his work. The discriminants of the form $d=(an)^2+ka$ for $\pm k\in\{1,2,4\}$ are called of *Richaud–Degert type*, so we consider here Richaud–Degert type discriminants with $k=4$. We expect that the same method will work for the other values of k as well.

The class number one problem for special cases of Richaud–Degert type was solved in [B1], [B2], proving the Yokoi and Chowla Conjectures. The method was subsequently applied e.g. in [BY] and [L], but in those papers the parameter a is fixed ($a=1$). However, already a subset of positive density of the discriminants of Richaud–Degert type with $k=4$ are covered in [La].

Under the assumption of the Generalized Riemann Hypothesis there is a list of principal quadratic fields of Richaud–Degert type (see [M]), and one can check there that the largest number in that list having the form $d=(an)^2+4a$ is 1253. Here, however, our main result is unconditional:

2010 *Mathematics Subject Classification*: Primary 11R11; Secondary 11R29, 11R42.
Key words and phrases: class number problem, real quadratic field.
Received 10 October 2014; revised 2 September 2015.
Published online *.

DOI: 10.4064/aa7957-12-2015

THEOREM 1.1. *If $d = (an)^2 + 4a$ is square-free for a and n odd positive integers and $d > 1253$, then $h(d) > 1$.*

2. Notation and structure of the paper. If χ is a Dirichlet character, then $L(s, \chi)$ denotes the usual Dirichlet L-function. If d is a square-free positive integer and $d \equiv 1 \pmod 4$, we denote by χ_d the real primitive Dirichlet character with conductor d, i.e. $\chi_d(m) = \left(\frac{m}{d}\right)$ (Jacobi symbol).

$\mathcal{O}_K$ denotes the ring of integers of the quadratic field K. The norm $N\mathfrak{a}$ of an integral ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is the index $[\mathcal{O}_K : \mathfrak{a}]$. The Dedekind zeta function is defined as

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s} \tag{2.1}$$

where the summation is over all integral ideals $\mathfrak{a}$ in $\mathcal{O}_K$. It is well-known (see e.g. [W, Theorems 4.3 and 3.11]) that

$$\zeta_K(s) = \zeta(s)L(s, \chi_d). \tag{2.2}$$

Throughout the paper by (a, b) we denote the greatest common divisor of the integers a and b, and $P^+(a)$ denotes the largest prime factor of a. As usual, $\mu(x)$ is the Möbius function.

If K is a real quadratic field, we denote the algebraic conjugate of $\beta \in K$ by $\overline{\beta}$. The element $\beta \in K$ is called *totally positive*, denoted by $\beta \gg 0$, if $\beta, \overline{\beta} > 0$.

The structure of the paper is the following: In §3 we state the main result of [BG] on the evaluation of a partial zeta function in a general real quadratic field K, then we apply it for our special fields in §4, and we derive our main tool, Lemma 4.3. In §5 we simplify some quantities appearing in Lemma 4.3. We prove our main theorem in §6.

Computer calculations play an important role in the proof of the main theorem. These are SAGE (see [ST]) and C++ computations. The main number-theoretic objects, characters, algebraic numbers and ideals in certain cyclotomic fields are introduced in SAGE. We then plug the data obtained in SAGE into programs (sieves) in C++ to speed up the calculations, and most of the time we return to SAGE to finish our sieving with much fewer cases to consider and hence not bothering about the speed. The time for performing all possible computations was about 57 hours, on an old personal laptop under Windows XP, with an AMD 64x2 mobile processor at 1.6 GHz speed, and 1 GB RAM. All files can be found at [HT], and more information about the implementation is provided in the file `READ ME.txt` there.

3. Biró–Granville's Theorem. In [BG] Biró and Granville give a finite formula for a partial zeta function at 0. They illustrate its efficiency by

successfully solving the class number one problem for some one-parameter R-D discriminants where $a = 1$. Here we restate their main theorem.

Let K be a real quadratic field with discriminant d, let χ be a Dirichlet character of conductor q and let I be an integral ideal of K. Define

$$\zeta_I(s,\chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

where the summation is over all integral ideals $\mathfrak{a}$ equivalent to I in the ideal class group $Cl(d)$. For a quadratic form $f(x,y) \in \mathbb{Z}[x,y]$ set

$$G(f,\chi) := \sum_{1\le u,v\le q-1} \chi(f(u,v))\frac{u}{q}\frac{v}{q}. \tag{3.1}$$

According to the theory of cycles of reduced forms corresponding to a given ideal (see e.g. [H, §53]), the ideal I of K has a $\mathbb{Z}$-basis (ν_1,ν_2) for which $\nu_1 \gg 0$ and $\alpha = \nu_2/\nu_1$ satisfies $0 < \alpha < 1$. Moreover, the regular continued fraction expansion of α is purely periodic:

$$\alpha = [0, \overline{a_1,\dots,a_\ell}]$$

for some positive ℓ (which is the least period) and $a_1,\dots,a_\ell$. Here $a_{j+\ell} = a_j$ for every $j \ge 1$. Further for $n \ge 1$ denote

$$p_n/q_n = [0, a_1, \dots, a_n]$$

and write $\alpha_n := p_n - q_n\alpha$ with $\alpha_{-1} = 1$ and $\alpha_0 = -\alpha$. Define also, for $j = 1, 2, \dots,$

$$Q_j(x,y) = \frac{1}{NI}(\nu_1\alpha_{j-1}x + \nu_1\alpha_j y)(\overline{\nu_1}\,\overline{\alpha}_{j-1}x + \overline{\nu_1}\,\overline{\alpha}_j y),$$
$$f_j(x,y) = (-1)^j Q_j(x,y).$$

It is known that every f_j has integer coefficients. Using the usual notation

$$\tau(\chi) := \sum_{a(q)} \chi(a)e(a/q)$$

for the Gauss sum, we introduce the expression

$$\beta_\chi := \frac{1}{\pi^2}\chi(-1)\tau(\chi)^2 L(2,\overline{\chi}^2). \tag{3.2}$$

Also recall that a character χ is called *odd* if $\chi(-1) = -1$.

In [BG] the following main result is proven.

THEOREM 3.1 (Biró and Granville [BG]). *Suppose that χ is an odd primitive character with conductor $q > 1$ and $(q, 2d) = 1$. With the notation as above we have*

$$\frac{1}{2}\zeta_I(0,\chi) = \sum_{j=1}^{\ell} G(f_j,\chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi \sum_{j=1}^{\ell} a_j\overline{\chi}(f_j(1,0)).$$

4. Application of Theorem 3.1 for our special discriminant. Let $d=(an)^2+4a$ be square-free with odd positive integers a and n, and assume that $a>1$. We use the fact that $d\equiv 1 \pmod 4$, so the ring of integers of the field $K=\mathbb{Q}(\sqrt{d})$ is of $\mathcal{O}_K=\mathbb{Z}[1,(\sqrt{d}+1)/2]$. Let

$$\alpha=\frac{\sqrt{d}-an}{2}$$

and $I=\mathbb{Z}[1,\alpha]$. We note that $0<\alpha<1$ and $I=\mathcal{O}_K$. We apply Theorem 3.1 to compute the partial zeta function for the class of principal ideals.

However to apply the above formula for the function ζ_I we need the continued fraction expansion of α. Using [S] and the rules in [B, p. 78], in [LaT, §6.3] it is computed that

$$\alpha=[0,\overline{n,an}]. \tag{4.1}$$

Alternatively, given (4.1), it is easy to see that this periodic continued fraction equals α, and conclude by uniqueness of the expansion that this is indeed the answer.

Using the notation from §3 we have $\ell=2$, since we consider $a>1$, and

$$\frac{1}{2}\zeta_I(0,\chi)=\sum_{j=1}^{2}G(f_j,\chi)+\frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi\sum_{j=1}^{2}a_j\overline{\chi}(f_j(1,0)). \tag{4.2}$$

Here $p_1/q_1=[0;n]=1/n$, $p_2/q_2=1/(n+1/an)=an/(an^2+1)$ and $\alpha_1=1-n\alpha$, $\alpha_2=an-(an^2+1)\alpha$.

By the choice of the ideal $I=\mathcal{O}_K$ we have $NI=1$ and $\nu_1=1$, and so

$$Q_j(x,y)=\alpha_{j-1}\overline{\alpha}_{j-1}x^2+(\alpha_{j-1}\overline{\alpha}_j+\alpha_j\overline{\alpha}_{j-1})xy+\alpha_j\overline{\alpha}_j y^2. \tag{4.3}$$

Observe that α is the positive root of the equation $x^2+(an)x-a=0$. Then $\alpha+\bar{\alpha}=-an$ and $\alpha\bar{\alpha}=-a$. We use these to compute

$$\begin{aligned}Q_1(x,y)&=\alpha_0\bar{\alpha}_0x^2+(\alpha_0\bar{\alpha}_1+\alpha_1\bar{\alpha}_0)xy+\alpha_1\bar{\alpha}_1y^2\\&=\alpha\bar{\alpha}x^2+\big(-\alpha(1-n\bar{\alpha})-\bar{\alpha}(1-n\alpha)\big)xy+(1-n\alpha)(1-n\bar{\alpha})y^2\\&=-ax^2-anxy+y^2.\end{aligned}$$

Similarly

$$\begin{aligned}Q_2(x,y)&=\alpha_1\bar{\alpha}_1x^2+(\alpha_1\bar{\alpha}_2+\alpha_2\bar{\alpha}_1)xy+\alpha_2\bar{\alpha}_2y^2\\&=(1-n\alpha)(1-n\bar{\alpha})x^2\\&\quad+\big\{(1-n\alpha)\big(an-(an^2+1)\bar{\alpha}\big)+(1-n\bar{\alpha})\big(an-(an^2+1)\alpha\big)\big\}xy\\&\quad+\big(an-(an^2+1)\alpha\big)\big(an-(an^2+1)\bar{\alpha}\big)y^2\\&=x^2+anxy-ay^2.\end{aligned}$$

So

$$f_1(x,y) = ax^2 + anxy - y^2, \tag{4.4}$$

$$f_2(x,y) = x^2 + anxy - ay^2. \tag{4.5}$$

We see that $f_1(1,0) = a$ and $f_2(1,0) = 1$. Let

$$c_a := a + \overline{\chi}(a). \tag{4.6}$$

When we substitute in (4.2) we get

$$\frac{1}{2}\zeta_I(0,\chi) = G(f_1,\chi) + G(f_2,\chi) + \frac{n}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a. \tag{4.7}$$

Now assume that we are in a field K where $h(d) = 1$. Then all integral ideals are principal. So

$$\zeta_I(s,\chi) = \sum_{\mathfrak{a}\lhd\mathcal{O}_K} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s} =: \zeta_K(s,\chi). \tag{4.8}$$

By the same method used to prove (2.2) it follows that

$$\zeta_K(s,\chi) = L(s,\chi)L(s,\chi\chi_d). \tag{4.9}$$

Recall (see e.g. [W, Theorem 4.2]) the following equation for an odd primitive character χ:

$$L(0,\chi) = -\sum_{1\le a\le q} \chi(a)\frac{a}{q}. \tag{4.10}$$

Further denote

$$m_\chi := \sum_{1\le a<q} a\chi(a) = -qL(0,\chi). \tag{4.11}$$

Then from (4.8) and (4.9) we have

$$q\zeta_I(0,\chi) = qL(0,\chi)L(0,\chi\chi_d) = -m_\chi L(0,\chi\chi_d).$$

Combining the latter equality with (4.7) we get

$$-\frac{1}{2}m_\chi L(0,\chi\chi_d) = q\bigg(G(f_1,\chi) + G(f_2,\chi) + \frac{n}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a)\bigg). \tag{4.12}$$

Set

$$C_\chi(a,n) := q(G(f_1,\chi) + G(f_2,\chi)). \tag{4.13}$$

Then (4.12) transforms into

LEMMA 4.1. *With the above notation, if $h(d) = 1$, we have*

$$-m_\chi L(0,\chi\chi_d) = 2C_\chi(a,n) + nq\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a.$$

Let $\mathfrak{L}_\chi$ be the field formed by adjoining to $\mathbb{Q}$ all the values of the character χ, and $\mathcal{O}_{\mathfrak{L}_\chi}$ be its ring of integers. Note that $d \equiv 1 \pmod 4$, so $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2} = 1$ and χ_d is an even character. Now we can state

Claim 4.2. *For the odd character χ with conductor q and $d \equiv 1 \pmod 4$ such that $(q,d) = 1$ the quantity $L(0, \chi\chi_d)$ is an algebraic integer in the number field $\mathfrak{L}_\chi$.*

This can be shown in the same way as the corresponding statement preceding [B1, Fact A], using formula (4.10) for the odd primitive character $\chi\chi_d$ and the fact that q and d are coprime.

Take a prime ideal $\mathfrak{R}$ in $\mathcal{O}_{\mathfrak{L}_\chi}$ such that $m_\chi \in \mathfrak{R}$. By Claim 4.2 we have $L(0, \chi\chi_d) \in \mathcal{O}_{\mathfrak{L}_\chi}$, so $-m_\chi L(0, \chi\chi_d) \equiv 0 \pmod{\mathfrak{R}}$. Then by Lemma 4.1 we get the main result of this section:

Lemma 4.3. *Let $d = (an)^2 + 4a$ be square-free with odd positive integers a and n, and assume that $a > 1$ and $h(d) = 1$. Suppose that χ is an odd primitive character with conductor $q > 1$ and $(q, 2d) = 1$. Take a prime ideal $\mathfrak{R}$ in $\mathcal{O}_{\mathfrak{L}_\chi}$ such that $m_\chi \in \mathfrak{R}$. Then*

$$0 \equiv 2C_\chi(a,n) + n\chi(d)\left(\frac{d}{q}\right) q\beta_\chi c_a \pmod{\mathfrak{R}} \tag{4.14}$$

with the notation (3.1), (4.4), (4.5), (4.13), (3.2) *and* (4.6).

5. Further remarks on Lemma 4.3. First we find a more simple finite form for β_χ. Let

$$\gamma_\chi := \sum_{n=1}^{q-1} \chi^2(n) \frac{n^2}{q^2} \tag{5.1}$$

and consider the Jacobi sum

$$J_\chi := \sum_{\substack{a,b \,(\mathrm{mod}\, q) \\ a+b \equiv 1 \,(\mathrm{mod}\, q)}} \chi(a)\chi(b).$$

The following claim shows that β_χ is actually not only an algebraic number but also computable in finitely many steps, which is not at all evident from definition (3.2). The claim is stated in the Introduction of [BG], and it is proven in §6 of that paper.

Lemma 5.1. *Let χ be a primitive character of order greater than 2. For the unique way to write $\chi = \chi_+\chi_-$ where χ_+, χ_- are primitive characters of coprime conductors q_+, q_- respectively, such that χ_- has order 2, and χ_+^2*

is also primitive, we have

$$\beta_\chi = \chi_+(-1)J_{\chi_+}\gamma_\chi\mu(q_-)\prod_{p|q_-}\frac{p^2\chi_+^2(p)-1}{p\chi_+^2(p)-1}.$$

The following statement is proved in [BG, §9]. As the exposition in [BG] is somewhat sketchy, we give here a detailed proof.

LEMMA 5.2. *For an odd complex character χ with conductor $q>2$ such that $(q,2d)=1$ we have*

$$G(f_1,\chi)=G(f_2,\chi).$$

Proof. In (3.1) we change the summation via $u\to v$, $v\to q-u$. Then for the new variables again $1\le v, q-u\le q-1$. Now

$$\begin{aligned}
G(f_1,\chi) &= \sum_{1\le u,v\le q-1}\chi\big(av^2+anv(q-u)-u^2\big)\frac{v}{q}\frac{q-u}{q}\\
&= \sum_{1\le u,v\le q-1}\chi(av^2-anvu-u^2)\frac{v}{q}\frac{-u}{q}+\sum_{1\le u,v\le q-1}\chi(av^2-anvu-u^2)\frac{v}{q}\\
&= \sum_{1\le u,v\le q-1}\chi(-1)\chi(-av^2+anvu+u^2)\frac{v}{q}\frac{-u}{q}-\sum_{1\le u,v\le q-1}\chi(f_2(u,v))\frac{v}{q}\\
&= \sum_{1\le u,v\le q-1}\chi(f_2(u,v))\frac{u}{q}\frac{v}{q}-\sum_{1\le u,v\le q-1}\chi(f_2(u,v))\frac{v}{q}.
\end{aligned}$$

We use the notation

$$g(\chi,f,h):=\sum_{1\le m,n\le q-1}\chi(f(m,n))h\left(\frac{n}{q}\right) \tag{5.2}$$

for the quadratic form $f(x,y)=Ax^2+Bxy+Cy^2$ with square-free discriminant $\Delta=B^2-4AC$ and $h(x)\in\mathbb{Z}[x]$.

Therefore we have

$$G(f_1,\chi)=G(f_2,\chi)-g(\chi,f_2,t).$$

We will prove that

$$g(\chi,f_2,t)=0. \tag{5.3}$$

We will do so by showing that $g(\chi,f_2,1)=0$ and $g(\chi,f_2,t-1/2)=0$.

First notice that there is a δ with $(\delta,q)=1$ such that $\chi(\delta)\ne 0,1$, and one can find r,s for which $\delta\equiv r^2-\Delta s^2 \pmod q$. The argument that follows is for square-free q, and the one for general q follows easily. The existence of such r and s follows from the theory of norm residues modulo q in $\mathbb{Q}(\sqrt{\Delta})$ for $(q,\Delta)=1$ (see [H, §47, Theorem 138 and Lemma]). Basically we use the fact that the group of norm residues modulo q is big, take an element δ_1 from it, and then choose δ to be δ_1 or $4\delta_1$ depending on the residue of the

discriminant of the field modulo 4. In this case $r^2 - \Delta s^2$ is the norm, or four times the norm, of an algebraic integer in $\mathbb{Q}(\sqrt{\Delta})$.

Now if we choose M and N satisfying

$$(2AM + BN) + \sqrt{\Delta}\, N = \big((2Am + Bn) + \sqrt{\Delta}\, n\big)(r + \sqrt{\Delta}\, s)$$

we get

$$\begin{aligned}\big((2AM + BN) + \sqrt{\Delta}\, N\big)\big((2AM + BN) - \sqrt{\Delta}\, N\big)\\ = 4Af(M, N) = 4Af(m, n)(r^2 - \Delta s^2).\end{aligned}$$

From definition (4.5) the coefficient A of f_2 equals 1, i.e. $(A, q) = 1$, so we get $f_2(M, N) \equiv f_2(m, n)\delta \pmod q$. One checks that

$$\begin{pmatrix} M \\ N \end{pmatrix} = \begin{pmatrix} r - Bs & -2Cs \\ 2As & r + Bs \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

with determinant of the upper matrix $\mathfrak{T} := r^2 - \Delta s^2 \neq 0$. Since $\mathfrak{T}$ is invertible and m and n are linear forms of M and N, if some of the latter do not take each residue modulo q exactly q times, then some of the residues m or n will not either. Therefore when $0 \leq m, n \leq q-1$, also $0 \leq M, N \pmod q \leq q-1$. Notice as well that

$$g(\chi, f, 1) = \sum_{0 \leq m,n \leq q-1} \chi(f(m, n))$$

because χ is not a real character and

$$\sum_{0 \leq m \leq q-1} \chi(Am^2) = \sum_{0 \leq n \leq q-1} \chi(Cn^2) = 0.$$

That is why we can replace m and n with M and N in the sum $g(\chi, f_2, 1)$. We get $g(\chi, f_2, 1) = \chi(\delta) g(\chi, f_2, 1)$. Hence

$$g(\chi, f_2, 1) = \sum_{1 \leq m,n \leq q-1} \chi(f(m, n)) = 0. \tag{5.4}$$

Further, consider the Bernoulli polynomial $B_1(x) := x - 1/2$. We notice that $B_1(1 - x) = 1/2 - x = -B_1(x)$. Therefore

$$\chi(f(m, n)) B_1\left(\frac{n}{q}\right) = -\chi(f(q - m, q - n)) B_1\left(\frac{q - n}{q}\right)$$

and

$$\begin{aligned} g(\chi, f, B_1) &= \sum_{1 \leq m,n \leq q-1} \chi(f(m, n)) B_1\left(\frac{n}{q}\right) \\ &= -\sum_{1 \leq m,n \leq q-1} \chi(f(q - m, q - n)) B_1\left(\frac{q - n}{q}\right) \\ &= -g(\chi, f, B_1). \end{aligned}$$

Hence $g(\chi, f, B_1) = 0$. This together with (5.4) yields (5.3) and completes the proof. ∎

LEMMA 5.3. *For any odd character χ with conductor $q > 2$,*

$$C_\chi(a, q-n) = -C_\chi(a, n).$$

Proof. To show this we substitute $n \to q-n$ in the definition of $G(f_1, \chi)$:

$$\begin{aligned} G(f_1,\chi)_{q-n} &= \sum_{1\le x,y\le q-1} \chi(ax^2 + a(q-n)xy - y^2)\frac{x}{q}\,\frac{y}{q} \\ &= \sum_{1\le x,y\le q-1} \chi(ax^2 - anxy - y^2)\frac{x}{q}\,\frac{y}{q} \\ &= \sum_{1\le x,y\le q-1} \chi(-1)\chi(-ax^2 + anxy + y^2)\frac{x}{q}\,\frac{y}{q} \\ &= -G(f_2,\chi)_n. \end{aligned}$$

Thus

$$\begin{aligned} \frac{1}{q}C_\chi(a, q-n) &= G(f_1,\chi)_{q-n} + G(f_2,\chi)_{q-n} = -G(f_2,\chi)_n - G(f_1,\chi)_n \\ &= -\frac{1}{q}C_\chi(a,n). \ ∎ \end{aligned}$$

Since $C_\chi(a,0) = C_\chi(a, q-0) = -C_\chi(a,0)$, we obtain

LEMMA 5.4. *For any odd character χ with conductor $q > 2$ and for any integer a,*

$$C_\chi(a, 0) = 0.$$

This also means that under the conditions of Lemma 5.2 for any n divisible by q we have $C_\chi(a,n) = 0$, and therefore $G(f_1,\chi) = 0$ as well.

6. Proof of Theorem 1.1. Let d be as in Theorem 1.1. We assume $a > 1$, since the case $a = 1$ follows from Yokoi's Conjecture proved in [B1].

Suppose now that χ is an odd primitive character modulo $q > 1$ and $(q, 2d) = 1$. Assume in addition that χ is a complex character, i.e. $\chi^2 \ne 1$.

We will use Lemmas 4.3, 5.2 and 5.1. By (4.13) and (4.14) we get

$$\begin{aligned} (6.1)\qquad & 4q^2\Big(\prod_{p\mid q^-}(p\chi_+^2(p) - 1)\Big)G(f_1,\chi) \\ & + n\chi(d)\left(\frac{d}{q}\right)c_a q^2 J_{\chi_+}\gamma_\chi\mu(q_-)\chi_+(-1)\Big(\prod_{p\mid q^-}(p^2\chi_+^2(p) - 1)\Big) \equiv 0 \ (\mathrm{mod}\ \mathfrak{R}), \end{aligned}$$

where the prime ideal $\mathfrak{R}$ of $\mathfrak{L}_\chi$ lies above the rational prime r and we suppose $m_\chi \in \mathfrak{R}$ and $(r, q) = 1$. Then it is clear, using (3.1) and the definition of

f_1 and c_a in (4.4) and (4.6), that the truth of (6.1) depends only on the residues of a and n modulo qr.

Let us now define a directed graph in a way similar to but slightly different from that in [B1]. Let

$$q \to r$$

mean the following: $q > 1$ is an odd integer, there is an odd primitive character χ modulo q such that $\chi^2 \neq 1$, and there is a prime ideal $\mathfrak{R}$ of $\mathfrak{L}_\chi$ such that $\mathfrak{R}$ lies above the odd rational prime r which satisfies $(r, q) = 1$ and $m_\chi \in \mathfrak{R}$. The latter condition can arise for example for an odd character if $r \mid h_q^-$, where h_q^- is the relative class number of the cyclotomic field $\mathbb{Q}(\zeta_q)$ for $\zeta_q = e^{2\pi i/q}$ [W, Theorem 4.17].

We will use the following claim proved in [La, Claim 5.1] as a generalization of [B1, Fact B].

Claim 6.1. *If $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$, then a and $an^2 + 4$ are primes, and for any prime $p \neq a$ such that $2 < p < an/2$ we have*

$$\left(\frac{d}{p}\right) = -1.$$

Also we recall the main result of [La].

Theorem 6.2 ([La, Theorem 1.1]). *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n such that $43 \cdot 181 \cdot 353 \mid n$, then $h(d) > 1$.*

Let $q \to r$ hold. Then by the considerations above and by Claim 6.1, we see that if $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$ satisfying $P^+(qr) < an/2$, and a is different from any prime factor of qr, then

$$\left(\frac{(an)^2 + 4a}{p}\right) = -1 \tag{6.2}$$

for every prime divisor p of qr, and (6.1) also holds. We see that (6.2), similarly to (6.1), depends only on the residues of a and n modulo qr.

Lemma 6.3. *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n with $an > 2 \cdot 127$,*

$$a \neq 1, 3, 5, 7, 13, 17, 19, 37, 73, 127, \tag{6.3}$$

and $h(d) = 1$, then

$$n \equiv 0 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37}.$$

Proof. We apply the arrows

$$\begin{aligned} &5 \times 19 \to 13, && 3 \times 37 \to 19, \\ &7 \times 19 \to 13, 37, 73, && 5 \times 37 \to 13, \\ &13 \times 19 \to 3, 7, 73, 127, && 3 \times 7 \times 13 \to 19, 37, \end{aligned}$$

$$\begin{aligned} &3\times 5\times 19\to 37,73, && 7\times 17\to 5,\\ &7\times 13\to 37, && 127\to 5,13,\\ &3\times 73\to 17, && 3\times 127\to 37. \end{aligned}$$

It is easy to check that the maximal prime factor of any q is at most 127 and the maximal value of r is 127, so our conditions guarantee that $P^+(qr) < an/2$, and a is different from any prime factor of qr in each case. One can check by concrete computations (finding a suitable character and a suitable prime ideal in each case) that these are indeed arrows.

Let $P := 3\cdot 5\cdot 7\cdot 13\cdot 19\cdot 37$, and let A be the set of those arrows from the above list where qr consists only of primes dividing P. Denote by B the set of those arrows from the list which are not in A, i.e. where qr is divisible by 17, 73 or 127.

In the first part of the proof we apply only the arrows from A. We fix the residue a_0 of a and n_0 of n modulo P; then the residues of a and n modulo qr are determined for every arrow from A. For every fixed pair $0\le a_0, n_0 < P$ we check (6.1) and (6.2) for every such arrow. We find that for most pairs (a_0, n_0) the implied conditions yield $n_0 = 0$. In the second part of the proof it is enough to deal with the exceptional (a_0, n_0) pairs, i.e. those for which $n_0 > 0$ and (6.1) and (6.2) are true for this pair and for every arrow from A.

In the second part of the proof we increase the modulus to $P\cdot 17\cdot 73\cdot 127$. We fix the residues A_0 of a and N_0 of n modulo $P\cdot 17\cdot 73\cdot 127$, but we consider only pairs $0\le A_0, N_0 < P\cdot 17\cdot 73\cdot 127$ for which there is an exceptional pair (a_0, n_0) in the above sense such that $A_0\equiv a_0 \pmod P$ and $N_0\equiv n_0 \pmod P$. For every such pair (A_0, N_0) and every arrow from B we check (6.1) and (6.2). This eventually leads only to cases $N_0 = 0$, which implies $n_0 = 0$. This proves the lemma.

In this way we explained the theoretical part of the proof, but the computer calculations are also important. To save space we do not present them here, but one can find them at [HT]. ∎

In what follows we will use cases when $q\to r$ holds, $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$ satisfying $P^+(qr) < an/2$, a is different from any prime factor of qr (just as above), and in addition either r divides n, or q divides n. If r divides n, then $n\in\mathfrak{R}$ (since $\mathfrak{R}$ lies above r), so (6.1) reduces to

$$4q^2\Big(\prod_{p\mid q^-}(p\chi_+^2(p)-1)\Big)G(f_1,\chi)\equiv 0 \pmod{\mathfrak{R}}, \tag{6.4}$$

so in this case (6.2) and (6.4) are valid.

If q divides n, from Lemma 5.4 we get $G(f_1,\chi) = 0$, so (6.1) transforms into

$$n\chi(d)\left(\frac{d}{q}\right)c_a q^2 J_{\chi_+}\gamma_\chi \mu(q_-)\chi_+(-1)\Big(\prod_{p\mid q^-}(p^2\chi_+^2(p)-1)\Big) \equiv 0 \pmod{\mathfrak{R}}. \tag{6.5}$$

We remark that most of the factors in this congruence are easily checked to be nonzero modulo $\mathfrak{R}$ (this can be computed for any particular parameters q and r), so in practice the only remaining condition will be

$$c_a \equiv 0 \pmod{\mathfrak{R}},$$

but we will check (6.5) itself in each case.

The proofs of the next three lemmas are very similar to each other. They are also similar to the proof of the previous lemma, but this time we will check (6.2) and (6.4), or (6.2) and (6.5).

LEMMA 6.4. *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n with $an > 2 \cdot 43$,*

$$a \neq 1, 5, 7, 19, 37, 43, \tag{6.6}$$

$n \equiv 0 \pmod{5 \cdot 7 \cdot 19 \cdot 37}$ *and $h(d) = 1$, then*

$$n \equiv 0 \pmod{43}.$$

Proof. We apply the arrows

$$5 \times 43 \to 7, 19, 37.$$

One can check again by concrete computations (finding a suitable character and a suitable prime ideal in each case) that these are indeed arrows. By our considerations above we know that (6.2) and (6.4) must be valid because for these three arrows, r divides n.

We fix the residue a_0 of a and n_0 of n modulo $P := 5 \cdot 7 \cdot 19 \cdot 37 \cdot 43$, but we consider only cases when $n_0 \equiv 0 \pmod{5 \cdot 7 \cdot 19 \cdot 37}$. For every fixed pair $0 \le a_0, n_0 < P$ for which n_0 satisfies the above congruence we check (6.2) and (6.4) for each arrow listed above. We find that if (a_0, n_0) is such that $n_0 > 0$, then either (6.2) or (6.4) is false for at least one arrow. The necessary computer calculations can be found at [HT]. ∎

LEMMA 6.5. *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n with $an > 2 \cdot 181$,*

$$a \neq 1, 3, 5, 13, 19, 37, 181, \tag{6.7}$$

$n \equiv 0 \pmod{3 \cdot 5 \cdot 13 \cdot 19 \cdot 37}$ *and $h(d) = 1$, then*

$$n \equiv 0 \pmod{181}.$$

Proof. We apply the arrows

$$181 \to 5, 37, \qquad 13 \times 19 \to 181, \qquad 3 \times 5 \times 19 \to 181.$$

One can check again by concrete computations (finding a suitable character and a suitable prime ideal in each case) that these are indeed arrows.

We fix the residue a_0 of a and n_0 of n modulo $P := 3 \cdot 5 \cdot 13 \cdot 19 \cdot 37 \cdot 181$, but we consider only cases when $n_0 \equiv 0 \pmod{3 \cdot 5 \cdot 13 \cdot 19 \cdot 37}$. For every fixed pair $0 \le a_0, n_0 < P$ for which n_0 satisfies the above congruence we check (6.2) and (6.4) for the first two arrows $181 \to 5, 37$ (here r divides n). For the remaining pairs with $n_0 > 0$ we check (6.2) and (6.5) (q divides n). We find that if $n_0 > 0$, then either (6.2) or (6.5) is false for at least one arrow. The computer calculations can be found at [HT]. ∎

LEMMA 6.6. *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n with $an > 2 \cdot 353$ and*

$$a \neq 1, 3, 5, 13, 17, 353, \tag{6.8}$$

and if $n \equiv 0 \pmod{3 \cdot 5 \cdot 13 \cdot 17}$ and $h(d) = 1$, then

$$n \equiv 0 \pmod{353}.$$

Proof. We apply the arrows

$$3 \times 5 \times 17 \to 353, \qquad 3 \times 5 \times 13 \times 17 \to 353.$$

One can check again by concrete computations that these are indeed arrows. By our considerations above we know that (6.2) and (6.5) must be valid.

We fix the residue a_0 of a and n_0 of n modulo $P := 3 \cdot 5 \cdot 13 \cdot 17 \cdot 353$, but we consider only cases when $n_0 \equiv 0 \pmod{3 \cdot 5 \cdot 13 \cdot 17}$. For every fixed pair $0 \le a_0, n_0 < P$ for which n_0 satisfies the above congruence we check (6.2) and (6.5) for each arrow listed above. We find that if $n_0 > 0$, then either (6.2) or (6.5) is false for at least one arrow. The computer calculations are found at [HT]. ∎

We now prove the theorem assuming that $an > 2 \cdot 353$ and

$$a \neq 3, 5, 7, 13, 17, 19, 37, 43, 73, 127, 181, 353. \tag{6.9}$$

Assume $h(d) = 1$. Then $an > 2 \cdot 17$, and $a \neq 3, 5, 7, 13, 17$ follows from above. Much as before, for fixed residues a_0 of a and n_0 of n modulo $P := 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$ we check (6.2) and (6.4) for the arrows

$$7 \times 17 \to 3, 5, 13, \qquad 13 \times 17 \to 5.$$

We find that if $n_0 > 0$, then either (6.2) or (6.4) is false for at least one arrow. The computer calculations can be found at [HT]. In this way we find that 17 divides n.

Let us also apply Lemma 6.3. It follows that the conditions of Lemmas 6.4–6.6 are satisfied. Consequently, $n \equiv 0 \pmod{43 \cdot 181 \cdot 353}$. This contradicts Theorem 6.2. Hence our theorem is proved under the above two conditions. Since the finitely many cases $an \le 2 \cdot 353$ are easily checked (the computations can be found at [HT]), it is enough to prove the theorem if a equals one of the values

$$3, 5, 7, 13, 17, 19, 37, 43, 73, 127, 181, 353. \tag{6.10}$$

This means that we have almost finished the proof, since we have reduced our original two-parameter problem to finitely many one-parameter problems. To complete the proof we will prove the theorem for these finitely many values of a.

For most of the exceptional cases we can apply exactly the same arrows as in [B1] for Yokoi's Conjecture, i.e. for $a = 1$. Indeed, for

$$a = 3, 13, 17, 19, 37, 43, 73, 127, 181, 353 \tag{6.11}$$

we use the arrows

$$175 \to 1861, 61, \quad 61 \to 1861, \quad 61 \to 41.$$

We fix the residue n_0 of n modulo $P := 41 \cdot 61 \cdot 175 \cdot 1861$. For every fixed pair (a, n_0), where a is one of the values in (6.11) and $0 \le n_0 < P$, we check (6.1) and (6.2) for each arrow above. We find that for every such pair (a, n_0) we get a contradiction for at least one arrow. This proves the theorem for the values in (6.11) and $1861 < an/2$. For smaller values of n we can check the statement directly. The details of the computations can again be found at [HT].

It remains to consider the cases $a = 5$ and $a = 7$.

For $a = 5$ we use the arrows

$$61 \to 1861, \quad 61 \to 41, \quad 41 \to 11.$$

We fix the residue n_0 of n modulo $P := 11 \cdot 41 \cdot 61 \cdot 1861$. For $a = 5$ and for every fixed $0 \le n_0 < P$ we check (6.1) and (6.2) for each arrow above. We find that for every such n_0 we get a contradiction for at least one arrow. This proves the theorem for $a = 5$ and $1861 < 5n/2$. For smaller values of n we can check the statement directly. The details of the computations can be found at [HT].

For $a = 7$ we use the arrows

$$61 \to 1861, \quad 61 \to 41, \quad 41 \to 11, \quad 11, 19 \to 61, \quad 9 \to 11.$$

We fix the residue n_0 of n modulo $P := 9 \cdot 11 \cdot 19 \cdot 41 \cdot 61 \cdot 1861$. For $a = 7$ and every fixed $0 \le n_0 < P$ we check (6.1) and (6.2) for each arrow above. We find that for every such n_0 we get a contradiction for at least one arrow. This proves the theorem for $a = 7$ and $1861 < 7n/2$. For smaller values of n we can check the statement directly. The details of the computations can be found at [HT].

The theorem is proved.

Acknowledgements. The authors are deeply indebted to Katalin Gyarmati for her valuable help concerning the codes. We would like to thank L. Washington, R. Schoof and T. Metsänkylä for helpful correspondence which led to finding the arrow $3315 \to 353$. This is the only arrow which

was not suggested by the table for relative class numbers in Washington's book [W].

The first author is partially supported by the Hungarian National Foundation for Scientific Research (OTKA) Grants no. K100291, K104183, K109789 and ERC-AdG. Grant no. 321104. The second author is supported by Back-to-Research Grant of University of Vienna and partially supported by OTKA no. K104183.

References

[B] J. Beck, *Diophantine approximation and quadratic fields*, in: Number Theory, K. Győry et al. (eds.), de Gruyter, 1998, 55–93.

[B1] A. Biró, *Yokoi's conjecture*, Acta Arith. 106 (2003), 85–104.

[B2] A. Biró, *Chowla's conjecture*, Acta Arith. 107 (2003), 179–194.

[B3] A. Biró, *Yokoi–Chowla conjecture and related problems*, in: Proc. of the 2003 Nagoya Conference (Nagoya, 2003), S. Katayama et al. (eds.), Saga Univ., Saga, 2004.

[BG] A. Biró and A. Granville, *Zeta function for ideal classes in real quadratic fields, at $s = 0$*, J. Number Theory 132 (2012), 1807–1829.

[BY] D. Byeon, M. Kim and J. Lee, *Mollin's conjecture*, Acta Arith. 126 (2007), 99–114.

[H] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

[HT] http://www.renyi.hu/∼biroand/code/.

[La] K. Lapkova, *Class number one problem for real quadratic fields of certain type*, Acta Arith. 153 (2012), 281–298.

[LaT] K. Lapkova, *Class number problems for quadratic fields*, PhD Thesis, 2012.

[L] J. Lee, *The complete determination of wide Richaud–Degert types which are not 5 modulo 8 with class number one*, Acta Arith. 140 (2009), 1–29.

[M] R. A. Mollin and H. C. Williams, *Solution of the class number one problem for real quadratic fields of extended Richaud–Degert type (with one possible exception)*, in: Number Theory (Banff, 1988), de Gruyter, Berlin, 1990, 417–425.

[S] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1960/1961), 393–413.

[ST] W. A. Stein et al., *Sage Mathematics Software (Version 5.12)*, The Sage Development Team, 2013, http://sagemath.org.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1996.

András Biró, Kostadinka Lapkova
A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
Reáltanoda u. 13-15
1053 Budapest, Hungary
E-mail: biro.andras@renyi.mta.hu
lapkova.kostadinka@renyi.mta.hu

Abstract (will appear on the journal's web site only)

We solve unconditionally the class number one problem for the 2-parameter family of real quadratic fields $\mathbb{Q}(\sqrt{d})$ with square-free discriminant $d = (an)^2 + 4a$ for positive odd integers a and n.