ACTA ARITHMETICA
107.2 (2003)

Chowla's conjecture

by

András Biró (Budapest)

1. Introduction. Let $K = \mathbb{Q}(\sqrt{d})$, where $\mathbb{Q}$ is the rational field and d is a squarefree positive integer, and let $h(d)$ be the class number of this field. In [C-F], S. Chowla conjectured that $h(4p^2+1) > 1$ if $p > 13$ is an integer, which we will prove to be true in this paper. Our work here has its origins in our paper [B], in which we established a conjecture of Yokoi that $h(p^2+4) > 1$ for $p > 17$. In fact, essentially the same proof works with appropriate modifications. We note that Siegel's theorem tells us that the class number is greater than 1 once p is sufficiently large, in both cases; however, Siegel's theorem does not indicate what "sufficiently large" means. Here we determine that using a quite different method. Our main result is as follows.

Theorem. *If d is squarefree, $h(d) = 1$ and $d = 4p^2 + 1$ with some positive integer p, then d 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).*

Combining this with Fact B below (which implies that if $h(d) = 1$, then d is a quadratic nonresidue modulo any prime r with $2 < r < p$) we obtain:

Corollary. *If d is squarefree, and $d = 4p^2 + 1$ with some integer $p > 1861$, then $h(d) > 1$.*

What concerns the small solutions, in the same way as in [B], we can easily prove (see Section 2) that $h(4p^2+1) > 1$ if $13 < p \leq 1861$. Hence Chowla's conjecture follows. We search these final few cases to show that $h(4p^2+1) = 1$ only for $p = 1, 2, 3, 5, 7, 13$.

The main lines of the proof are the same as in [B], but some modifications are needed; the most significant modifications can be found in the

2000 *Mathematics Subject Classification*: 11R11, 11R29, 11R42.

Research partially supported by the Hungarian National Foundation for Scientific Research (OTKA) Grants No. T032236, T029759 and D34576.

statement and proof of Lemma 1. Throughout the paper, we focus on the new ingredients appearing here: we heavily refer to [B], and omit some arguments which are explained in detail in [B]. The present proof also requires computer work.

As in [B], in Section 2 we give the outline of the proof, and in Section 3 we prove Lemma 1 and Fact B. However, we use exactly the same parameters in the proof as in [B], therefore we will just quote Section 4 (titled "Fixing the parameters") of [B], we do not have here a corresponding section. In Section 4 of the present paper we give the necessary modifications of the computer program, and in Section 5 we prove the Theorem.

2. Outline of the proof. Let $K = \mathbb{Q}(\sqrt{d})$, where $d = 4p^2 + 1$ is squarefree and p is a positive integer. Let R be the ring of algebraic integers of K, $P(K)$ the set of nonzero principal ideals of R, and denote by $N(a)$ the norm of an $a \in P(K)$, i.e. its index in R. If χ is a Dirichlet character, for $\Re s > 1$ define

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

In the next section we will prove the following formula for the special value at 0 of this function:

Lemma 1. *If $d = 4p^2 + 1$ is squarefree, $q > 2$ is an odd integer with $(q,d) = 1$, and χ is a primitive character modulo q with $\chi(-1) = -1$, then $\zeta_{P(K)}(s,\chi)$ extends meromorphically in s to the whole complex plane and*

$$\zeta_{P(K)}(0,\chi) = \frac{1}{q}\, C_\chi(p),$$

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

$$C_\chi(a) = \sum_{(C,D) \in H(q)} \chi(D^2 - C^2 - 4aCD) \lceil (4aC - D)/q \rceil (C - q)$$

with

$$H(q) = \{(C,D) : 2C, 2D, C - D \text{ are integers, and } 0 \le C, D < q\}.$$

Observe that if $(C,D) \in H(q)$ and a is an integer, then $D^2 - C^2 - 4aCD$ is also an integer, so the definition of $C_\chi(a)$ is consistent.

Remark. You might compare the definition of $C_\chi(a)$ with the definition of the corresponding quantity $A_\chi(a)$ in Lemma 1 of [B]. On the one hand, the discriminant of the quadratic form inside $\chi(\cdot)$ here (in $C_\chi(a)$) is $(4a)^2 + 4$ (i.e. of the previous form), which equals 4 times $4a^2 + 1$, i.e. of the new form. On the other hand, note that we sum over different sets in the case of $C_\chi(a)$ and in the case of $A_\chi(a)$.

The same arguments as in Section 2 of [B] (but with $d = 4p^2 + 1$) then lead to Fact A below. We do not repeat these arguments, but we mention that they rely in an essential way on the assumption that $h(d) = 1$.

Fact A. *If $d = 4p^2 + 1$ is squarefree, $h(d) = 1$, q is an odd integer with $q > 2$, $(q, d) = 1$, and χ is a primitive character modulo q with $\chi(-1) = -1$, then, writing*

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

we have $m_\chi \neq 0$, and $C_\chi(p)m_\chi^{-1}$ is an algebraic integer.

As in [B], we will show that the Theorem is a consequence of Fact A.

Let U_m and $\mathcal{L}_\chi$ have the same meaning as in [B]: If m is an odd positive integer, we denote by U_m the set of rational integers a satisfying

$$\left(\frac{a^2 + 4}{r}\right) = -1$$

for every prime divisor r of m. Let $\mathcal{L}_\chi$ be the field generated over $\mathbb{Q}$ by the values $\chi(a)$ $(1 \le a \le q)$.

In the present case, we consider the residue of $4p$ modulo q, that is, we write (observe that it is not the same as equation (2.5) of [B]):

$$4p = Pq + p_0 \quad \text{with } 0 \le p_0 < q. \tag{2.1}$$

We show (see (2.6) below) that if q, p_0 and χ are fixed, then $C_\chi(p)$ depends linearly on P (or, what is the same, on p).

Indeed, since q is odd, P and p_0 have the same parity. It follows easily that for $(C, D) \in H(q)$ we have

$$\lceil (4pC - D)/q \rceil = PC + f(p_0, C, D, q), \tag{2.2}$$

where for any pair $(C, D) \in H(q)$ and for any integer a we write

$$f(a, C, D, q) = \begin{cases} \lceil (aC - D)/q \rceil & \text{if } 2Ca \text{ is even,} \\ -1/2 + \lceil 1/2 + (aC - D)/q \rceil & \text{if } 2Ca \text{ is odd.} \end{cases} \tag{2.3}$$

On the other hand, let j be an integer (existing for odd q) such that

$$4j \equiv 1 \pmod{q}. \tag{2.4}$$

One can easily verify that

$$D^2 - C^2 - 4pCD \equiv D^2 - C^2 - 4jp_0CD \pmod{q} \tag{2.5}$$

for every $(C, D) \in H(q)$. Formulas (2.1)–(2.5) imply that

$$C_\chi(p) = PD_\chi(p_0) + E_\chi(p_0), \tag{2.6}$$

where for any integer a we write (j is given by (2.4))

$$D_\chi(a)=\sum_{(C,D)\in H(q)}\chi(D^2-C^2-4jaCD)C(C-q) \tag{2.7}$$

and

$$E_\chi(a)=\sum_{(C,D)\in H(q)}\chi(D^2-C^2-4jaCD)f(a,C,D,q)(C-q). \tag{2.8}$$

It is worth to multiply $D_\chi(a)$ and $E_\chi(a)$ by 4, because (if we multiply each summand by 4) in this way every summand becomes an algebraic integer. If $a_1,a_2\in U_q$, then (this is the analogue of (2.9) of [B])

$$(4D_\chi(a_1))=(4D_\chi(a_2)), \tag{2.9}$$

i.e. they generate the same ideal in the ring of integers of $\mathcal{L}_\chi$. We prove (2.9) at the end of this section.

For positive integers q and r we introduce the following condition (we had an analogue of this condition in [B]).

Condition (∗). *The integer q is odd, r is an odd prime, and there is an odd primitive character χ with conductor q and a prime ideal I of $\mathcal{L}_\chi$ lying above r such that $m_\chi\in I$, but I does not divide the ideal generated by $4D_\chi(a)$ in the ring of integers of $\mathcal{L}_\chi$, where a is any rational integer with $a\in U_q$.*

Reducing everything modulo I, by (2.1), (2.6) and Fact A we can derive the following

Statement. *If $h(d)=1$, q and r satisfy Condition (∗) with a character χ and ideal I, and $4p\in U_q$ (equivalently, $p_0\in U_q$, where p_0 is defined by (2.1)), then*

$$4p\equiv p_0-q\,\frac{4E_\chi(p_0)}{4D_\chi(p_0)}\ (\mathrm{mod}\,I), \tag{2.10}$$

where we divide in R/I.

Hence, under the conditions of the Statement, the residue of $4p$ modulo q determines its residue modulo r (since I lies above r).

The proof of the Theorem then runs very similarly to the proof in [B], but here $4p$ plays the role what p played in [B].

Now, denote by $q\to r$ that q and r satisfy the present Condition (∗). It will turn out that we have the arrows

$$175\to 61,\qquad 175\to 1861,\qquad 61\to 1861,\qquad 61\to 41$$

also in the present case.

Since

$$\left(\frac{d}{r}\right) = \left(\frac{4p^2+1}{r}\right) = \left(\frac{(4p)^2+4}{r}\right)$$

for every odd prime r, for the proof of the Theorem we may assume that

$$4p \in U_q$$

for $q = 175, 61, 1861, 41$.

There are 40 residue classes modulo 175 contained in U_{175}; we may assume that $4p$ belongs to one of them. For 18 of these classes, the arrow $175 \to 61$ forces $4p$ (through the Statement) into a residue class modulo 61 which is not contained in U_{61}. The arrow $175 \to 1861$ similarly eliminates 12 of the remaining residue classes, so 10 possible residue classes remain for $4p$ modulo 175.

Just as in [B], applying the arrow $61 \to 1861$, we find that for eight of the remaining residue classes modulo 175, different residue classes modulo 1861 are prescribed for $4p$ by consecutive application of the two arrows

$$175 \to 61, \qquad 61 \to 1861,$$

and by the arrow $175 \to 1861$. We are left with

$$4p \equiv \pm 52 \pmod{175 \cdot 61 \cdot 1861}.$$

The arrow $61 \to 41$ then forces $4p$ into residue classes modulo 41 which are not contained in U_{41}. This will complete the proof.

The Corollary follows at once from the following fact, which will be proved in the next section.

Fact B. *If $d = 4p^2 + 1$ is squarefree and $h(d) = 1$, then d is a prime, and if $2 < r < 2p$ is also a prime, $r \neq p$, then*

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

(Legendre symbol).

It can be checked that if $1 \le p \le 1861$ and $p \neq 1, 2, 3, 5, 7, 13$, then there is a prime $3 \le r \le 41$ such that $r < 2p$, $r \neq p$, and

$$\left(\frac{4p^2+1}{r}\right) \neq -1,$$

and this proves Chowla's conjecture.

Finally, we prove (2.9). By (2.4) and (2.7), and since $2C$ and $2D$ are integers for $(C, D) \in H(q)$, for $a \in U_q$ we have

$$(2.11)\qquad \frac{\chi(16)}{\chi(a^2+4)}\,4D_\chi(a) = \sum_{(C,D)\in H(q)} \chi\biggl(\frac{(4D-a(2C))^2}{a^2+4}-(2C)^2\biggr)4C(C-q).$$

For every fixed C, $4D-a(2C)$ runs over a complete residue system modulo q, hence the right-hand side of (2.11) is independent of $a\in U_q$, so (2.9) is proved.

3. Proof of Lemma 1 and Fact B. First we have to introduce the notations α and $Q(C,D)$. Notice that they have a slightly different meaning than in [B]. (They are obtained by writing $4p$ in place of p in the definition of the corresponding quantities of [B].)

Let α be the positive root of the equation $x^2+4px=1$. This time $1,(1+\alpha^{-1})/2$ is an integral basis of R, but it is also true in this case that α^{-1} is the fundamental unit of K; thus the units of R are $\pm\alpha^j$ with integer j. For $\beta\in R$, denote by $\overline{\beta}$ the algebraic conjugate of β. Any $\beta\in R$ is of the form

$$\beta = C + D\alpha^{-1}$$

with C, D such that $2C, 2D$ and $C-D$ are integers; and for this β one has

$$\beta\overline{\beta} = -Q(C,D),$$

where

$$Q(C,D) = D^2 - C^2 - 4pCD.$$

In particular, $Q(C,D)$ is an integer for such numbers C and D (this can be also seen directly).

We remark that the notation (2.4) is not valid in this section (we do not need that multiplicative inverse here); we will use the notation j to parametrize the elements of the set $R(C,D)$ below.

Proof of Lemma 1. The proof of formula (3.3) of [B] applies literally here (noting that $C+D\alpha^{-1}$ with integers $0\le C,D\le q-1$ form a complete set of representatives of R/qR for odd q also in the present case), and gives the following formula (which is a special case of a formula on p. 595 of [S2]):

$$\zeta_{P(K)}(s,\chi) = \frac{-1}{q^{2s}}\sum_{C,D=0}^{q-1}\chi(Q(C,D))\sum_{(x,y)\in R(C,D)}\zeta\biggl(s,\begin{pmatrix}1 & \alpha^{-2}\\ 1 & \alpha^2\end{pmatrix},(x,y)\biggr)$$

with the following notations: $R(C,D)$ denotes the set

$$\biggl\{(x,y)\in\mathbb{Q}^2 : 0<x\le 1,\, 0\le y<1,\, x+y\alpha^{-2}-\frac{C+D\alpha^{-1}}{q}\in R\biggr\},$$

and for a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with positive entries and $x > 0$, $y \geq 0$ we write

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x, y)\right)$$

for the function

$$\sum_{n_1, n_2 = 0}^{\infty} (a(n_1 + x) + b(n_2 + y))^{-s} (c(n_1 + x) + d(n_2 + y))^{-s}.$$

Just as in [B], we then deduce by the Corollary to Proposition 1 of [S1] (quoted as the Proposition in Section 3 of [B]) that

$$\zeta_{P(K)}(0, \chi) = -\sum_{0 \leq C, D \leq q-1} \chi(Q(C, D)) \Sigma_{C,D}, \tag{3.1}$$

where $\Sigma_{C,D}$ denotes the sum

$$\sum_{(x,y) \in R(C,D)} \left(-8p^2 xy - (4p^2 + 1)(x + y) + \frac{8p^2 + 1}{2}(x + y)^2 + \frac{16p^2 + 5}{12}\right).$$

For any m, n we have

$$\frac{m\alpha^{-1} + n}{q} = \frac{\left(n - \frac{m}{4p}\right) + \frac{m}{4p}\alpha^{-2}}{q},$$

and so fixing a pair $0 \leq C, D \leq q - 1$, the conditions for (m, n) having $(x, y) \in R(C, D)$ with

$$(x, y) = \left(\frac{1}{q}\left(n - \frac{m}{4p}\right), \frac{m}{4qp}\right) \tag{3.2}$$

(using that q is odd) are:

$$2m, 2n, m - n \text{ are integers,}$$
$$2m \equiv 2D \pmod{q}, \qquad 2n \equiv 2C \pmod{q}$$

and

$$0 \leq 2m < 8qp, \tag{3.3}$$

$$0 < 2n - \frac{m}{2p} \leq 2q. \tag{3.4}$$

Then

$$2m = 2D + jq, \tag{3.5}$$

where

$$j = 0, 1, \ldots, 8p - 1 \qquad \text{if } 0 \leq 2D < q; \tag{3.6}$$

$$j = -1, 0, \ldots, 8p - 2 \qquad \text{if } q < 2D \leq 2q - 2. \tag{3.7}$$

If j is fixed, then $2n \equiv 2C + jq \pmod{2q}$, because this is true modulo q, and also modulo 2, since $2n \equiv 2m \equiv jq \pmod 2$. Hence

$$2n = 2C + jq + 2Lq \tag{3.8}$$

with some integer L, and together with (3.4), this implies

$$L = \left[\frac{m}{4pq} - \frac{2C + jq}{2q} + 1\right],$$

so

$$L = \begin{cases} \left[\dfrac{m}{4pq} - \dfrac{C}{q} + 1\right] - \dfrac{j}{2} & \text{if } j \text{ is even,} \\ \left[\dfrac{m}{4pq} - \dfrac{C}{q} + \dfrac{1}{2}\right] - \dfrac{j-1}{2} & \text{if } j \text{ is odd.} \end{cases}$$

Now, by (3.3) and the conditions for C, one has

$$-1 < \frac{m}{4pq} - \frac{C}{q} < 1,$$

and by (3.5) one has

$$\frac{m}{4pq} - \frac{C}{q} = \frac{j/2 - (4pC - D)/q}{4p}.$$

It is then clear by (3.5), (3.8) and these last conditions that the possibilities for (m, n) having $(x, y) \in R(C, D)$ with (3.2) are (m_j, n_j), where the conditions for j are (3.6) and (3.7), and

$$m_j = D + jq/2;$$

for even j we have

$$n_j = \begin{cases} C & \text{if } j/2 < (4pC - D)/q, \\ C + q & \text{if } j/2 \geq (4pC - D)/q, \end{cases}$$

for odd j we have

$$n_j = \begin{cases} C - q/2 & \text{if } j/2 < (4pC - D)/q - 2p, \\ C + q/2 & \text{if } (4pC - D)/q - 2p \leq j/2 < (4pC - D)/q + 2p, \\ C + 3q/2 & \text{if } j/2 \geq (4pC - D)/q + 2p. \end{cases}$$

This means that

$$\Sigma_{C,D} = \sum_j \left(-\frac{2pm_j}{q^2}\left(n_j - \frac{m_j}{4p}\right) - \frac{4p^2+1}{q} n_j + \frac{8p^2+1}{2q^2} n_j^2 + \frac{16p^2+5}{12} \right) \tag{3.9}$$

where the summation is over the integers j satisfying (3.6) and (3.7). Let

$$\Sigma_{C,D} = \Sigma^{(\mathrm{e})}_{C,D} + \Sigma^{(\mathrm{o})}_{C,D}, \tag{3.10}$$

where $\Sigma^{(\mathrm{e})}_{C,D}$ is the sum over the even numbers j in (3.9), and $\Sigma^{(\mathrm{o})}_{C,D}$ is the sum over the odd numbers. If $0 \le A \le 4p$ is an integer, let us introduce the notation $F(\delta,\gamma,A)$ for the sum

$$\sum_{j=0}^{4p-1}\biggl(-\frac{2p\mu_j}{q^2}\biggl(\nu_j-\frac{\mu_j}{4p}\biggr)-\frac{4p^2+1}{q}\,\nu_j+\frac{8p^2+1}{2q^2}\,\nu_j^2+\frac{16p^2+5}{12}\biggr) \tag{3.11}$$

with

$$\mu_j=\delta+jq,\qquad \nu_j=\begin{cases}\gamma & \text{if } 0\le j<A,\\ \gamma+q & \text{if } A\le j<4p.\end{cases}$$

It is then clear that

$$\Sigma^{(\mathrm{e})}_{C,D}=F(D,C,\lceil(4pC-D)/q\rceil). \tag{3.12}$$

For the computation of $\Sigma^{(\mathrm{o})}_{C,D}$, observe that for every fixed C and D in the definition of n_j for odd j we have in fact only two (and not three) cases, because taking into account (3.6) and (3.7), we see that if $2C<q$, then $j/2<(4pC-D)/q-2p$ is impossible; on the other hand, if $2C>q$, then $j/2\ge(4pC-D)/q+2p$ is impossible. By this remark and (3.6) and (3.7), examining a few cases, we see that

$$\Sigma^{(\mathrm{o})}_{C,D}=F(\delta(C,D),\gamma(C,D),A(C,D)),$$

where we put

$$\delta(C,D)=\begin{cases}D+q/2 & \text{if } 2D<q,\\ D-q/2 & \text{if } 2D>q,\end{cases}\qquad \gamma(C,D)=\begin{cases}C+q/2 & \text{if } 2C<q,\\ C-q/2 & \text{if } 2C>q,\end{cases}$$

$$A(C,D)=\begin{cases}\lceil(4pC-D)/q-1/2\rceil+2p & \text{if } 2D<q,\ 2C<q,\\ \lceil(4pC-D)/q+1/2\rceil+2p & \text{if } 2D>q,\ 2C<q,\\ \lceil(4pC-D)/q-1/2\rceil-2p & \text{if } 2D<q,\ 2C>q,\\ \lceil(4pC-D)/q+1/2\rceil-2p & \text{if } 2D>q,\ 2C>q.\end{cases}$$

Observe that writing $\gamma=\gamma(C,D)$, $\delta=\delta(C,D)$, we have $A(C,D)=\lceil(4p\gamma-\delta)/q\rceil$ (this implies in particular $0\le A(C,D)\le 4p$), so

$$\Sigma^{(\mathrm{o})}_{C,D}=F(\delta,\gamma,\lceil(4p\gamma-\delta)/q\rceil). \tag{3.13}$$

Since $Q(C,D)\equiv Q(\gamma,\delta) \pmod q$, we see by (3.1) and formulas (3.10)–(3.13) that

$$\zeta_{P(K)}(0,\chi)=-\sum_{(C,D)\in H(q)}\chi(Q(C,D))F(D,C,\lceil(4pC-D)/q\rceil), \tag{3.14}$$

since the pairs (C,D) and $(\gamma(C,D),\delta(C,D))$ form the set $H(q)$, if (C,D) runs over the integer pairs with $0\le C,D\le q-1$. We then proceed just as in [B]. The transformation T is defined on $H(q)$ by the formulas

$$T((C,D))=(\widehat{C},\widehat{D}),\qquad \widehat{C}=D-4pC-q[(D-4pC)/q],\qquad \widehat{D}=C.$$

This is a permutation of $H(q)$. We put

$$T^2((C,D)) = (\widehat{\widehat{C}}, \widehat{\widehat{D}})$$

($\widehat{C}$, $\widehat{\widehat{C}}$, $\widehat{D}$ and $\widehat{\widehat{D}}$ depend on the pair (C,D)), and using the notation

$$A = \lceil (4pC - D)/q \rceil,$$

we have the relations

$$qA = 4pC - D + \widehat{C}, \qquad C = \widehat{D}, \qquad \widehat{C} = \widehat{\widehat{D}}. \tag{3.15}$$

It is not hard to verify the identity (see (3.11), and remember that $0 \le A \le 4p$ is an integer)

$$F(D,C,A) = A\left(1 - \frac{C}{q}\right) + \frac{4p}{4q^2}\Sigma^{(1)}_{C,D} - \frac{1}{4q}\Sigma^{(2)}_{C,D}, \tag{3.16}$$

where

$$\Sigma^{(1)}_{C,D} = 2C^2 + D^2 + (D - 4pC + qA)^2,$$
$$\Sigma^{(2)}_{C,D} = 8pC + (4p-2)D + (4p+2)(D - 4pC + qA).$$

(Note that (3.16) is almost the same as (3.5) of [B].) By (3.15) we see that

$$\Sigma^{(1)}_{C,D} = (D^2 + (\widehat{D})^2) + ((\widehat{D})^2 + (\widehat{\widehat{D}})^2), \tag{3.17}$$

$$\Sigma^{(2)}_{C,D} = (4p-2)(D + \widehat{D}) + (4p+2)(\widehat{D} + \widehat{\widehat{D}}). \tag{3.18}$$

Since $Q(\widehat{C}, \widehat{D}) \equiv -Q(C,D) \pmod q$ is true also here, and χ is an odd character, using (3.14) and (3.16)–(3.18), we finish the proof as in the case of Lemma 1 of [B]: the terms $\Sigma^{(1)}_{C,D}$, $\Sigma^{(2)}_{C,D}$ give 0 on each orbit of T. So the present lemma is proved.

Fact B is a consequence of Lemma 2 below and basic properties of factorization of rational primes in quadratic fields. So we prove just Lemma 2, because assuming this lemma, the proof of Fact B is easy (and, in addition, the proof of Fact B from Lemma 2 is almost the same as the proof of the corresponding fact in Section 3 of [B]).

LEMMA 2. *If $0 \neq \beta \in R$, and $|\beta\overline{\beta}| < 2p$, then $|\beta\overline{\beta}|$ is a square, or $|\beta\overline{\beta}| = p$.*

Proof. Let $\beta = c\alpha - d$, where $2c$, $2d$ and $c - d$ are integers. If one of the coefficients c and d is 0, then the other is an integer, and we are done. We may assume that $\alpha \le |\beta| \le 1$ and $c > 0$. Then

$$|\overline{\beta}| = \left| c\frac{1}{\alpha} + d \right| = \left| c\left(\alpha + \frac{1}{\alpha}\right) - \beta \right| \ge c\left(\alpha + \frac{1}{\alpha}\right) - 1,$$

hence

$$2p > |\beta\overline{\beta}| \geq c - \alpha.$$

The right-hand side is greater than $2p-1$ for $2c \geq 4p-1$, so we have $1 \leq 2c \leq 4p-2$. Then $0 < c\alpha < 1/2$, hence $d = \pm 1/2$ or $d = 1$, because $|\beta| \leq 1$, and $d = 0$ is already excluded. We know that

$$8p > 4|\beta\overline{\beta}| = |(2d)^2 - (2c)^2 + 4p(2c)(2d)|.$$

If $d = \pm 1/2$, then this gives

$$8p > 4|\beta\overline{\beta}| = |1 + C(4p - C)|$$

with the odd integer $C = \pm 2c$. For $C = \pm 1, 4p \pm 1$ the right-hand side is $4p$, otherwise it is greater than $8p$. So we can assume $d = 1$; then c is an integer and

$$2p > |\beta\overline{\beta}| = |1 + c(4p - c)|,$$

which implies that the right-hand side is 1. The lemma is proved.

4. The computer program. The aim of the program is to compute m_χ modulo I, and also $4E_\chi(p_0)$ modulo I and $4D_\chi(p_0)$ modulo I for every relevant residue class p_0 modulo q (we use the notations of Section 2). We compute these quantities with the concrete parameters of the four examples of Section 4 of [B], so we compute them in four separate cases. The program gives m_χ modulo I in the file result1.txt, $4E_\chi(p_0)$ modulo I in result2.txt, and $4D_\chi(p_0)$ modulo I in result3.txt for every interesting value of p_0.

We modify slightly the program given in [B]. This slight modification is needed only because the sums $A_\chi(p_0)$ and $B_\chi(p_0)$ of [B] are also modified: here $4E_\chi(p_0)$ plays the role of $A_\chi(p_0)$, and $4D_\chi(p_0)$ plays the role of $B_\chi(p_0)$.

Observe that in the definitions (2.7) and (2.8) of D_χ and E_χ we can simply omit $4j$ (j is defined by (2.4)) in the case of an integral pair $(C, D) \in H(q)$, so $4j$ is needed only for half-integral pairs (C, D). We replace the part of the program in [B] between

```
REM ======= WE COMPUTE $A_\chi(p_0)$ (AS s(2)) AND $B_\chi(p_0)$ (AS s(3))
```

and the next REM. Instead of that part we write (first we sum over the integral, then the half-integral pairs of $H(q)$; in the half-integral case, if $q = 175$, then we use $j = 44$, if $q = 61$, then $j = 46$):

```
REM ======= WE COMPUTE $4E_\chi(p_0)$ (AS s(2)) AND $4D_\chi(p_0)$ (AS s(3))
FOR c = 0 TO q - 1: FOR d = 0 TO q - 1
I = d * d - c * c - p(a) * c * d
g = 2 : Z = 4 * (q - c) * INT((d - p(a) * c)/q)
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
g = 3: Z = 4 * (c - q) * c
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
I = (d + 1/2) * (d + 1/2) - (c + 1/2) * (c + 1/2) - 44 * p(a) * (2 * c + 1) * (2 * d + 1)
IF q = 175 THEN GOTO 55
I = (d + 1/2) * (d + 1/2) - (c + 1/2) * (c + 1/2) - 46 * p(a) * (2 * c + 1) * (2 * d + 1)
55 g = 2: Z = 4 * (q - (c + 1/2)) * INT((d + 1/2 - p(a) * (c + 1/2))/q)
IF p(a) = 2 * INT(p(a)/2) THEN GOTO 56
Z = 4 * (q - (c + 1/2)) * (1/2 + INT((d + 1/2 - p(a) * (c + 1/2))/q - 1/2))
56 IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
g = 3: Z = 4 * (c + 1/2 - q) * (c + 1/2)
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
NEXT d: NEXT c
```

Then

```
REM ======= WE PRINT THE RESULTS
```

follows, and everything else is unchanged.

The data files are also changed (except data0.txt); we now give them. We write the contents of data0.txt, data1.txt, data2.txt and data3.txt in consecutive lines:

3, 8, 13, 17, 18, 22, 27, 32, 38, 43, 48, 52, 53, 57, 62, 67, 73, 78, 83, 87;
3, 8, 22, 32, 38, 43, 52, 62, 67, 73, 78, 0, 0, 0, 0, 0, 0, 0, 0, 0;
18, 24, 30, 59, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0;
52, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

5. Concluding the proof. We first prove the analogue of Lemma 3 of [B], which will show that a residue class and its negative behave in the same way also in the present proof. Recall (2.7) and (2.8).

LEMMA 3. *Let q be an odd positive integer, χ a character modulo q and a an integer with $(a,q)=1$. Then*

(i) $D_\chi(q-a) = D_\chi(a)$;
(ii) $E_\chi(q-a) + E_\chi(a) = D_\chi(a)$.

Proof. Write

$$D_\chi(a) = D_\chi^{(i)}(a) + D_\chi^{(h)}(a), \qquad E_\chi(a) = E_\chi^{(i)}(a) + E_\chi^{(h)}(a),$$

where $D_\chi^{(i)}$ and $E_\chi^{(i)}$ are obtained by summing over integer pairs $(C,D) \in H(q)$ on the right-hand side of (2.7) and (2.8), respectively; $D_\chi^{(h)}$ and $E_\chi^{(h)}$ are defined by summing over the half-integral pairs (C,D) there. Observe that

$$D_\chi^{(i)}(a) = B_\chi(a), \qquad E_\chi^{(i)}(a) = A_\chi(a),$$

where $A_\chi(a)$ and $B_\chi(a)$ are defined in Section 2 of [B]. Then, by Lemma 3 of [B], it is enough to prove that

$$D_\chi^{(h)}(q-a) = D_\chi^{(h)}(a), \tag{5.1}$$

$$E_\chi^{(h)}(q-a) + E_\chi^{(h)}(a) = D_\chi^{(h)}(a). \tag{5.2}$$

Now, (5.1) follows at once if we replace D by $q-D$ in the definition of $D_\chi^{(h)}$. The same reasoning gives (5.2) if we remark that by symmetry (using (5.1)) we can assume that a is odd, and that for odd a and for any half-integral pair $(C,D) \in H(q)$ the sum

$$f(a,C,D,q) + f(q-a,C,q-D,q)$$

equals

$$-\frac{1}{2} + \lceil 1/2 + (aC-D)/q \rceil + \lceil ((q-a)C-(q-D))/q \rceil,$$

and this is C, because

$$\left(\frac{1}{2} + \frac{aC-D}{q}\right) + \left(\frac{(q-a)C-(q-D)}{q}\right) = C - \frac{1}{2},$$

which is an integer, but the two terms of this sum are not integers. The lemma is proved.

Proof of the Theorem. We will apply the Statement of Section 2 with the parameters (i.e. q, r, χ and I) of the four examples given in Section 4 of [B]. Once these parameters and our integer p are given, p_0 is defined by (2.1).

Just as in [B], the program applied for the four (q,r) pairs given in the examples of Section 4 of [B] gives 0 for $m_\chi \pmod{I}$, but gives nonzero results for $4D_\chi(p_0) \pmod{I}$ for certain values of $p_0 \in U_q$ (hence for all $p_0 \in U_q$, see (2.9)), so we find that these four (q,r) pairs satisfy Condition $(*)$. Hence we can apply (2.10), and we can follow the steps outlined in Section 2.

By Lemma 3, we have

$$a - q\,\frac{4E_\chi(a)}{4D_\chi(a)} \equiv -\left((q-a) - q\,\frac{4E_\chi(q-a)}{4D_\chi(q-a)}\right) \tag{5.3}$$

modulo I for every $(a,q)=1$, so (see (2.10)) a residue class contained in U_q and its negative determine residue classes modulo r which are again negatives of each other.

We first consider Example 1 from Section 4 of [B]. We have 20 possible values of p_0 (i.e. for the residue of $4p$ modulo 175) such that $p_0 \in U_{175}$ and $0 < p_0 < 175/2$; we write these values in the first column of Table 1. This table is completely similar to the corresponding table of [B] (but $4E_\chi(p_0)$ plays the role of $A_\chi(p_0)$, and $4D_\chi(p_0)$ plays the role of $B_\chi(p_0)$): the second and third columns are computed by the program, the fourth column gives $4p$ modulo 61, it is computed from the first three columns, using (2.10); the fifth column gives a square root of $(4p)^2+4 \bmod 61$, if it exists.

Table 1

p_0	$4E_\chi(p_0)$	$4D_\chi(p_0)$	$4p$ mod r	$\sqrt{(4p)^2+4}$ mod r
3	29	15	51	
8	0	42	8	
13	32	25	33	19
17	34	22	46	30
18	37	56	32	28
22	55	12	18	
27	27	47	29	28
32	6	56	59	
38	36	16	56	
43	1	57	41	
48	23	47	0	2
52	0	13	52	
53	43	15	19	11
57	37	57	44	7
62	45	25	52	
67	19	22	24	
73	14	13	30	
78	25	12	54	
83	25	42	50	8
87	18	16	35	3

We use the parameters of Example 1 of [B], in particular $q=175$, $r=61$. The second and third columns are meant modulo I.

Here we have 11 values of p_0 where the fifth column of Table 1 is empty (which means that the square root does not exist, hence $4p \in U_{61}$). We apply the program for these 11 values with the parameters of Example 2 (of Section 4 of [B], as usual), in particular, $q = 175$ and $r = 1861$. The results are in Table 2, which is again similar to Table 2 of [B]; the fourth column is computed on the basis of (2.10). Here we have five values where the fifth column is empty (which means that $4p \in U_{1861}$).

Table 2

p_0	$4E_\chi(p_0)$	$4D_\chi(p_0)$	$4p$ mod r	$\sqrt{(4p)^2+4}$ mod r
3	667	1518	913	867
8	0	582	8	505
22	973	602	1189	
32	459	1480	1166	
38	769	546	388	914
43	1733	99	852	751
52	0	726	52	
62	1798	371	1110	62
67	1743	1313	1313	
73	343	726	1454	
78	748	602	1635	837

We use the parameters of Example 2 of [B], in particular $q=175$, $r = 1861$. The second and third columns are meant modulo I.

The remaining possibilities (i.e. when $4p$ modulo 175 is such that $4p \in U_{175}, U_{61}, U_{1861}$) are in Table 3, where we mean that either the plus or the minus sign is valid within a row, and one of the rows must be valid for $4p$ (we are taking into account also (5.3)).

Table 3

$4p$ mod 175	$4p$ mod 61	$4p$ mod 1861
±22	±18	±1189
±32	±59	±1166
±52	±52	±52
±67	±24	±1313
±73	±30	±1454

For four remaining values modulo 61 we apply the program with the parameters of Example 3. The result is Table 4. The fourth column is computed by (2.10). We see (using again also (5.3)) that in these cases the two ways of the determination of $4p$ modulo 1861 give in fact different values, hence a contradiction.

Table 4

p_0	$4E_\chi(p_0)$	$4D_\chi(p_0)$	$4p$ mod r
18	327	1722	282
24	728	823	515
30	1850	1232	1742
59	1146	1146	1859

We use the parameters of Example 3 of [B], in particular $q = 61$, $r = 1861$. The second and third columns are meant modulo I.

So the only possible values for $4p$ modulo 61 are ±52. Hence, if we consider Example 4 ($q = 61$, $r = 41$), the only possibilities for p_0 are 52 and $61 - 52 = 9$. For $p_0 = 52$ we apply the program to obtain

$$4E_\chi(p_0) \equiv 0 \pmod{I} \quad \text{and} \quad 4D_\chi(p_0) \equiv 22 \pmod{I}.$$

Hence (2.10) gives

$$4p \equiv 52 \equiv 11 \pmod{41}.$$

By (5.3) we know that then $p_0 = 9$ gives

$$4p \equiv -11 \pmod{41}.$$

In both cases, we have

$$(4p)^2 + 4 \equiv 125 \equiv 17^2 \pmod{41}.$$

Hence $(4p)^2 + 4 = 4(4p^2 + 1)$ is a quadratic residue modulo 41, so the Theorem is proved.

References

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

[C-F] S. Chowla and J. Friedlander, *Class numbers and quadratic residues*, Glasgow Math. J. 17 (1976), 47–52.

[S1] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo 23 (1976), 393–417.

[S2] —, *On special values of zeta functions of totally real algebraic number fields*, in: Proc. Internat. Congress of Math., Helsinki, 1978, 591–597.

A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
Reáltanoda u. 13-15
1053 Budapest, Hungary
E-mail: biroand@renyi.hu

Received on 9.11.2001 (4141)