Yokoi's conjecture

by András BIRÓ

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

1. Introduction

Let p be an odd positive integer, write $d = p^2 + 4$, and assume that d is squarefree. Let $K = \mathbf{Q}(\sqrt{d})$, where $\mathbf{Q}$ is the rational field. We prove the conjecture of Yokoi (see [Y]) that $h(d)$ (i. e. the class number of K) is greater than 1, if $p > 17$.

This conjecture is one of the real analogues of the famous problem (solved by Heegner, Stark, Baker) of finding all imaginary quadratic fields with class number 1. Since the fundamental unit of K is small, it follows from the ineffective theorem of Siegel (similarly to the imaginary case) that there are only finitely many p for which the special real quadratic field K has class number 1. So the problem is to find an effective upper bound for p assuming $h(d) = 1$. We will prove the following theorem.

THEOREM. *If d is squarefree, $h(d) = 1$ and $d = p^2 + 4$ with some odd 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 the well-known fact that if $h(d) = 1$ then d is a quadratic nonresidue modulo any prime r with $2 < r < p$ (for the sake of completeness, we will prove it, see our Fact B stated in Section 2), we obtain our main result:

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

It is easy to prove on the basis of the above-mentioned Fact B that $h(d) > 1$ if $17 < p \leq 1861$, see the end of Section 2 (this statement follows also from [M]), so we have a full solution of Yokoi's conjecture. Note that there are six exceptional fields where $h(d) = 1$, belonging to $p = 1, 3, 5, 7, 13, 17$.

The same proof with minor modifications works for Chowla's conjecture, which is a similar class number one problem (see [C-F]). We will present that proof in a forthcoming paper. But it seems that the present proof

Research partially supported by the Hungarian National Foundation for Scientific Research (OTKA) Grants No. T 032236, T 029759 and D34576

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

works only for the class number one problem, the class number 2 problem (for example) remains open. The harder problem of giving an effective lower bound tending to infinity for $h(p^2+4)$ (the similar statement in the imaginary case was proved by Goldfeld, Gross, Zagier, see [G] and [G-Z]) is also open. We mentioned above that the fundamental unit is small (hence Siegel's theorem is applicable), however, its logarithm is as large as $\log p$, so it is large enough to cause a problem if one wants to apply the Goldfeld-Gross-Zagier method.

The starting point of our proof is an idea of the paper [B] of J. Beck. In that paper he excluded some residue classes for p, i.e. he gave effective upper bounds for p in the class number 1 case provided p belongs to certain residue classes. He combined elementary number theory with formulas for special values of zetafunctions related to K and certain quadratic Dirichlet characters. In this paper, we use zetafunctions related to nonquadratic Dirichlet characters; this leads us to elementary algebraic number theory. Using also new elementary ingredients, we are able to exclude all residue classes modulo a given concrete modulus, hence to prove the conjecture.

Up until this proof, only quadratic characters have been used in the proof as "parameters". I mean that in the quoted paper of Beck, and also in the classical work of Gelfond-Linnik-Baker in the imaginary case, besides the quadratic Dirichlet character belonging to the given quadratic field K, there are other Dirichlet characters, and one can consider them as parameters, since one tries to choose them in a way which is most useful for the proof. Now, in the present proof these parameter characters are not quadratic. This provides a lot of new possibilities for excluding residue classes for p. The use of such characters was made possible by proving our Lemma 1 (see Section 2 for its statement), which gives a useful expression for the value at 0 of some zetafunctions. The proof of Lemma 1 given here is based on the method of Shintani (see [S1]). Originally I proved this lemma without knowing Shintani's work, by a different (and more complicated) method. I am grateful to S. Egami for drawing the paper [S1] to my attention.

We will give a more detailed sketch of the proof in the next section.

The proof requires also computer work. We emphasize that the results of the computations made by the computer program given in Section 5 are important for the proof of the Theorem (which is a theoretical result). So we think that this computer program belongs to the proof, consequently, for the sake of completeness it is necessary to give its details. However, if one is willing to accept the results of the computer work, one can skip Section 5.

The structure of the paper is the following. In Section 2 we give the plan of the proof, in Section 3 we prove the important Lemma 1 and Fact B mentioned above, in Section 4 we fix the numerical parameters, in Section 5 we give a BASIC program. Finally, in Section 6 we give the results of this computer program and conclude the proof of the Theorem.

I mention here that I am grateful to A. Granville for his many valuable remarks on my original manuscript. These remarks simplified the arguments at some points and made the exposition more clear.

I am also grateful to M. Simonovits, who helped me to simplify the first version of my computer program.

2. Outline of the proof

We introduce some notations. 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 $a \in I(K)$, i.e. its index in R. Let $q > 2$ be an integer with $(q, d) = 1$ (remember that $d = p^2 + 4$), and let χ be an odd (i.e we assume $\chi(-1) = -1$) primitive character with conductor q. (This will be the parameter character.) For $\Re s > 1$ define

$$\zeta_K(s) = \sum_{a \in I(K)} \frac{1}{N(a)^s}, \qquad \zeta_K(s, \chi) = \sum_{a \in I(K)} \frac{\chi(N(a))}{N(a)^s},$$

and

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

It is well-known (see e.g. [W], Theorems 4.3 and 3.11) that

$$\zeta_K(s) = \zeta(s) L(s, \chi_d), \tag{2.1}$$

where

$$\chi_d(n) = \left(\frac{n}{d}\right)$$

is a Jacobi symbol; moreover, if $h(d) = 1$, then d is a prime (see Fact B below), so this is a Legendre symbol. It follows easily that

$$\zeta_K(s, \chi) = L(s, \chi) L(s, \chi\chi_d).$$

It is also well-known (see e.g. [W], Theorem 4.2 and [D], Chapter 9) that for a primitive character ψ with $\psi(-1) = -1$ and with conductor f one has

$$L(0,\psi) = -\frac{1}{f}\sum_{a=1}^{f} a\psi(a) \neq 0.$$

Consequently, since $\chi\chi_d$ is a primitive character with conductor qd by our conditions, and $\chi_d(-1) = 1$ because d is congruent to 1 modulo 4, so

$$\zeta_K(0,\chi) = \frac{1}{q^2 d}\left(\sum_{a=1}^{q} a\chi(a)\right)\left(\sum_{b=1}^{qd} b\chi(b)\chi_d(b)\right). \tag{2.2}$$

Now, if $h(d) = 1$, then

$$\zeta_K(s,\chi) = \zeta_{P(K)}(s,\chi) \tag{2.3}$$

by definition. In the next section we will prove

LEMMA 1. *If $d = p^2+4$ is squarefree, $q > 2$ is an 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*

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

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

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

Note that qd divides the sum

$$\Sigma = \sum_{x=0}^{d-1}(l+xq)\chi_d(l+xq)$$

for any fixed $1 \le l \le q$. Indeed, the numbers $l+xq$ give a complete system of residues modulo d, so

$$\Sigma \equiv l \sum_{\text{y mod } d} \chi_d(y) = 0 \pmod q, \quad \Sigma \equiv \sum_{\text{y mod } d} y\chi_d(y) = 0 \pmod d,$$

since χ_d is an even nonprincipal character modulo d. Now,

$$\sum_{b=1}^{qd} b\chi(b)\chi_d(b) = \sum_{l=1}^{q}\chi(l)\sum_{x=0}^{d-1}(l+xq)\chi_d(l+xq),$$

so using (2.2), (2.3), Lemma 1 and the last remark, we obtain the following **FACT A.** *If $d = p^2 + 4$ is squarefree, $h(d) = 1$, q is an 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 that $m_\chi \neq 0$, and

$$A_\chi(p) m_\chi^{-1}$$

is an algebraic integer.

We will prove that the Theorem follows from Fact A.

First we introduce the following notation. If m is an odd positive integer, we denote by U_m the set of rational integers a satisfying that

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

for every prime divisor r of m. Observe that U_m is a union of certain residue classes modulo m.

We assume that $h(d) = 1$. We will use Fact A in the following way. Denote by $\mathcal{L}_\chi$ the field generated over $\mathbf{Q}$ by the values $\chi(a)$ $(1 \leq a \leq q)$, and take a prime ideal I of $\mathcal{L}_\chi$ such that

$$m_\chi \in I. \tag{2.4}$$

Let

$$p = Pq + p_0 \text{ with } 0 \leq p_0 < q, \tag{2.5}$$

then it is easy to see that

$$A_\chi(p) = PB_\chi(p_0) + A_\chi(p_0), \tag{2.6}$$

where for any integer a we write

$$B_\chi(a) = \sum_{0 \leq C, D \leq q-1} \chi(D^2 - C^2 - aCD) C(C - q). \tag{2.7}$$

We then obtain by (2.4), (2.6) and Fact A that

$$PB_\chi(p_0) + A_\chi(p_0) \equiv 0 \pmod{I}. \tag{2.8}$$

Assume that q is odd, and that $p \in U_q$ (equivalently $p_0 \in U_q$). Observe that this already determines the ideal generated by $B_\chi(p_0)$. Indeed, if $a_1, a_2 \in U_q$, then

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

i.e. $B_\chi(a_1)$ and $B_\chi(a_2)$ generate the same ideal in the ring of integers of $\mathcal{L}_\chi$. We will show this statement at the end of this section. (Note that (2.9) is not important for the proof, but we think it is worth remarking.) Assume also that the positive integers q and r satisfy the following condition:

Condition $(*)$. *The integer q is odd, r is an odd prime, and there is an odd primitive character χ with conductor q and there is 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 $B_\chi(a)$ in the ring of integers of $\mathcal{L}_\chi$, if a is any rational integer with $a \in U_q$.*

Then, since $p_0 \in U_q$, we obtain by (2.8) that

$$P \equiv -\frac{A_\chi(p_0)}{B_\chi(p_0)} \pmod{I},$$

where we divide in the residue field of I (i.e. in R/I). Combining it with (2.5), we see that

$$p \equiv p_0 - q\frac{A_\chi(p_0)}{B_\chi(p_0)} \pmod{I}. \tag{2.10}$$

Let q and p_0 be fixed. Note that in principle it may happen, if the residue field of I is not the prime field (in our concrete applications, the residue field will always be the prime field), that there is no rational integer p satisfying (2.10); but anyway, if there are solutions, then all the solutions belong to a unique residue class modulo r, since I lies above r. This implies that if we know q and p_0, then we can specify a congruence class modulo r such that p must belong to this class.

Summing up: let $h(d) = 1$, and let q and r satisfy Condition $(*)$. Then, if p is in a given congruence class modulo q such that $p \in U_q$, it forces p to be in a certain residue class modulo r; then we can test whether $p \in U_r$ or not. This is our key new elementary tool, and our Theorem follows by several applications of this tool. The technicalities of this are very roughly as follows.

Denote by $q \to r$ that q and r satisfy Condition $(*)$ above. We could say that we defined a directed graph (with the positive integers as vertices) in this way. We will use a certain triangle in this graph. To be concrete, we

will use the arrows (more precisely, the special cases belonging to these arrows of the above-mentioned tool):

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

There are 40 residue classes modulo $175 = 5^2 \cdot 7$ contained in U_{175}, so we may assume that p belongs to one of these classes. For 20 of these classes, the arrow $175 \to 61$ forces p into a residue class modulo 61 which is not contained in U_{61}. The arrow $175 \to 1861$ similarly eliminates 10 of the remaining residue classes, so 10 possible residue classes remain for p modulo 175.
Next we apply also the arrow $61 \to 1861$, and we find that for eight of the remaining residue classes modulo 175, different residue classes modulo 1861 are prescribed for p by consecutive application of the two arrows

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

and by the arrow $175 \to 1861$. This contradiction eliminates these classes. We are left with

$$p \equiv \pm 13 \pmod{175 \cdot 61 \cdot 1861}.$$

We then use a new arrow

$$61 \to 41,$$

and this finally forces p to residue classes modulo 41 which are not contained in U_{41}. This will prove the Theorem.
We explain briefly how we found the triangle 61,175,1861. It is clear that if q and r satisfy Condition $(*)$, then there is an odd primitive character χ with conductor q such that r divides the norm of m_χ (this is a necessary, but not sufficient condition for $(*)$). Now, such divisibility relations can be found by the table on pp. 353-360. of [W]: this table lists relative class numbers of cyclotomic fields, and in view of Theorem 4.17 of [W], relative class numbers are closely related to the norms of such numbers m_χ.
To deduce the Corollary we use the following

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

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

(Legendre symbol).

We prove it in the next section.

The small values of p, i.e. the cases $1 \leq p \leq 1861$ are easily handled by Fact B. In fact, it can be checked by an easy calculation that if $1 \leq p \leq 1861$ is an odd integer and $p \neq 1, 3, 5, 7, 13, 17$, then there is a prime $3 \leq r \leq 31$ such that $r < p$ and

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

Hence Yokoi's conjecture is proved.

Examining the proof, we see that Yokoi's conjecture follows from Facts A and B by elementary algebraic number theory and a finite amount of computation. I think that the present way is not the only one to prove the conjecture on the basis of these two facts.

We also see that in order to get the linear congruence (2.8), it was very important that once χ, its conductor q and the residue of p modulo q are fixed, then $\zeta_{P(K)}(0, \chi)$ depends linearly on p (see Lemma 1, (2.5) and (2.6)). In the case of quadratic characters χ, this linear dependence was proved by Beck in [B].

Finally, we prove formula (2.9). By (2.7), we have

$$\frac{\chi(4)}{\chi(a_1^2+4)} B_\chi(a_1) = \sum_{0 \leq C, D \leq q-1} \chi\left(\frac{(2D - a_1 C)^2}{a_1^2+4} - C^2\right) C(C-q), \quad (2.11)$$

where dividing by a_1^2+4 means multiplying by its inverse modulo q (which exists by the assumption that $a_1 \in U_q$). Now, if C is fixed, then $(2D - a_1 C)$ runs over a complete residue system modulo q. A similar formula is valid for a_2 in place of a_1. Since

$$(a_2^2+4)(a_1^2+4)^{-1}$$

is the square of a reduced residue class modulo q, if $a_1, a_2 \in U_q$, so the right-hand side of (2.11) remains unchanged if we replace a_1 by a_2, hence (2.9) is proved. In fact one can say more about the numbers $B_\chi(a)$, especially if q is a prime, but we do not need it, so we do not analyze it any further.

3. Proof of Lemma 1 and Fact B

Before proving these two important results stated in Section 2, we introduce some further notations.

Let α be the positive root of the equation $x^2 + px = 1$. It is easily seen that $1, \alpha^{-1}$ is an integral basis of R, and $1, \alpha$ is also an integral basis. On the other hand, α^{-1} is the fundamental unit of K, this is true because

the fundamental solution of $X^2 - (p^2+4)Y^2 = -4$ is $(X,Y) = (p,1)$. Hence the units of R are $\pm\alpha^j$ with integer j. For $\beta \in R$, denote by $\overline{\beta}$ the algebraic conjugate of β, and let

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

It is easy to verify that for

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

with integers C,D one has

$$\beta\overline{\beta} = -Q(C,D). \tag{3.1}$$

Proof of Lemma 1. Suppose that (γ) is a principal ideal of R. If $\gamma < 0$, then replace γ by $-\gamma$. If, then, $\overline{\gamma} < 0$, replace γ by $\gamma\alpha^{-1}$, which is positive, and its conjugate, $\overline{\gamma}(\overline{\alpha})^{-1}$, is also positive. Therefore, without loss of generality, we may assume that $\gamma > 0$ and $\overline{\gamma} > 0$. The units of R which are positive and whose conjugate are also positive are $(\alpha^2)^j$ with integer j. So there is a unique $\beta \in R$ such that $(\gamma) = (\beta)$ and

$$\beta > 0,\ \overline{\beta} > 0,\ 1 \le \frac{\beta}{\overline{\beta}} < \alpha^{-4}.$$

Since α^{-2} is irrational, we can write any element of K as a $\mathbf{Q}$-linear combination of 1 and α^{-2}. Say

$$\beta = X + Y\alpha^{-2}.$$

Now

$$1 \le \frac{\beta}{\overline{\beta}} \Leftrightarrow \overline{\beta} \le \beta \Leftrightarrow Y(\alpha^{-2} - \alpha^2) \ge 0 \Leftrightarrow Y \ge 0.$$

Similarly

$$\frac{\beta}{\overline{\beta}} < \alpha^{-4} \Leftrightarrow \beta < \overline{\beta}\alpha^{-4} \Leftrightarrow X(\alpha^{-4} - 1) > 0 \Leftrightarrow X > 0.$$

We deduce that every principal ideal of R can be written in a unique way in the form (β), where

$$\beta \in R,\ \beta = X + Y\alpha^{-2} \text{ with some rationals } X > 0,\ Y \ge 0.$$

Next write $X = qx + qn_1$ and $Y = qy + qn_2$ for some nonnegative integers n_1 and n_2 and real numbers $0 < x \leq 1$, $0 \leq y < 1$ which can be done in a unique way. Then $\beta \in R$ if and only if

$$q(x + y\alpha^{-2}) \in R,$$

since, evidently, $q(n_1 + n_2\alpha^{-2}) \in qR$.
Now, since $C + D\alpha^{-1}$ with integers $0 \leq C, D \leq q-1$ form a complete system of representatives of R/qR, we can uniquely select an integer pair $0 \leq C, D \leq q-1$ such that

$$q(x + y\alpha^{-2}) \in C + D\alpha^{-1} + qR.$$

Therefore

$$x + y\alpha^{-2} - \frac{C + D\alpha^{-1}}{q} \in R. \tag{3.2}$$

Tracing this back gives

$$X + Y\alpha^{-2} \equiv C + D\alpha^{-1} \pmod{qR},$$

and since for the principal ideal a generated by $(X + Y\alpha^{-2})$ we have

$$N(a) = (X + Y\alpha^{-2})\overline{(X + Y\alpha^{-2})}$$

because $X > 0,\ Y \geq 0$, so

$$N(a) \equiv (C + D\alpha^{-1})\overline{(C + D\alpha^{-1})} = -Q(C, D) \pmod{q},$$

where we used (3.1). Therefore, using also (3.2), if we partition the $\beta \in R$ according to the associated values for C and D we obtain the following formula of Shintani (p. 595. of [S2]):

$$\zeta_{P(K)}(s, \chi) = \frac{-1}{q^{2s}} \sum_{C,D=0}^{q-1} \chi(Q(C, D)) \sum_{(x,y)\in R(C,D)} \zeta\left(s, \begin{pmatrix} 1 & \alpha^{-2} \\ 1 & \alpha^2 \end{pmatrix}, (x, y)\right) \tag{3.3}$$

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

$$\left\{(x, y) \in \mathbf{Q}^2 :\ 0 < x \leq 1,\ 0 \leq y < 1,\ x + y\alpha^{-2} - \frac{C + D\alpha^{-1}}{q} \in R\right\},$$

and for a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 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

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

The key result we need to quote is easily deduced from the Corollary to Proposition 1 of [S1]:

Proposition (Shintani). *For any $a,b,c,d,x>0$ and $y\geq 0$ the function*

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

which is absolutely convergent for $\Re s>1$, extends meromorphically in s to the whole complex plane and the special value

$$\zeta\left(0,\begin{pmatrix} a & b \\ c & d\end{pmatrix},(x,y)\right)$$

equals to

$$B_1(x)B_1(y)+\frac{1}{4}\left(B_2(x)\left(\frac{c}{d}+\frac{a}{b}\right)+B_2(y)\left(\frac{d}{c}+\frac{b}{a}\right)\right),$$

where B_1 and B_2 are the Bernoulli polynomials

$$B_1(z)=z-\frac{1}{2},\ B_2(z)=z^2-z+\frac{1}{6}.$$

We thus can substitute the result of this proposition into (3.3) to evaluate $\zeta_{P(K)}(0,\chi)$. Using that

$$\alpha^{-2}+\alpha^2=p^2+2,$$

we obtain

$$\zeta_{P(K)}(0,\chi)=-\sum_{0\leq C,D\leq q-1}\chi(Q(C,D))\Sigma_{C,D}, \tag{3.4}$$

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

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

To investigate $\Sigma_{C,D}$ for a fixed pair $0\leq C,D\leq q-1$, we observe that for any m,n we have

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

and so it is easy to see that the possibilities for (m,n) having $(x,y) \in R(C,D)$ with

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

are

$$m_j = D + jq, \;\; n_j = C + q\left[1 + \frac{j}{p} - \frac{(pC-D)/q}{p}\right]$$

with any integer $0 \le j \le p-1$. This is so because the possible values of m are obviously these p values, and once m is fixed, n is unique.
One has

$$0 < 1 + \frac{j}{p} - \frac{(pC-D)/q}{p} < 2,$$

so

$$n_j = C \text{ for } 0 \le j < A$$

and

$$n_j = C + q \text{ for } A \le j < p,$$

where we put

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

and clearly $0 \le A \le p$.
So we have

$$\Sigma_{C,D} = \sum_{j=0}^{p-1}\left(-\frac{p^2}{2q^2}(n_j - \frac{m_j}{p})\frac{m_j}{p} - \frac{p^2+4}{4q}n_j + \frac{p^2+2}{4q^2}n_j^2 + \frac{p^2+5}{12}\right).$$

By the description of n_j and m_j above, considering separately the cases $0 \le j < A$ and $A \le j < p$, using the summation formulas for $\sum_{j=0}^{N} j$ and $\sum_{j=0}^{N} j^2$ (for any integer $N \ge 0$), straightforward (but tedious) calculations give

$$\Sigma_{C,D} = A(1 - \frac{C}{q}) + \frac{p}{4q^2}\Sigma_{C,D}^{(1)} - \frac{1}{4q}\Sigma_{C,D}^{(2)}, \tag{3.5}$$

where

$$\Sigma_{C,D}^{(1)} = 2C^2 + D^2 + (D - pC + qA)^2,$$

and

$$\Sigma_{C,D}^{(2)} = 2pC + (p-2)D + (p+2)(D - pC + qA).$$

Remember that A depends on C and D, but for brevity we do not denote it.
We show that

$$\sum_{0 \le C,D \le q-1} \chi(Q(C,D))\Sigma_{C,D}^{(j)} = 0$$

for $j = 1, 2$. To this end we introduce the transformation

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

with

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

(here we used lower integer part). We will also use the notation

$$T^2\left((C, D)\right) = (\hat{\hat{C}}, \hat{\hat{D}}).$$

Note that $\hat{C}$ (similarly to $\hat{\hat{C}}$, $\hat{D}$ and $\hat{\hat{D}}$) depends on the pair (C, D). The transformation T is a permutation of the set of the pairs (C, D) with $0 \leq C, D \leq q - 1$.
Now, observe that

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

Using this relation, and

$$C = \hat{D}, \;\; \hat{C} = \hat{\hat{D}},$$

we obtain the identities

$$\Sigma^{(1)}_{C,D} = \left(D^2 + \left(\hat{D}\right)^2\right) + \left(\left(\hat{D}\right)^2 + \left(\hat{\hat{D}}\right)^2\right)$$

and

$$\Sigma^{(2)}_{C,D} = (p - 2)\left(D + \hat{D}\right) + (p + 2)\left(\hat{D} + \hat{\hat{D}}\right).$$

It is easy to verify that

$$Q(\hat{C}, \hat{D}) \equiv -Q(C, D) \pmod{q},$$

hence

$$\chi\left(Q(\hat{C}, \hat{D})\right) = -\chi\left(Q(C, D)\right),$$

since χ is odd. Consequently, any orbit of T (where χ is not 0) has an even number of elements, and the value of $\chi\left(Q(C, D)\right)$ changes to its negative at each step by T. Our last identities then show that in fact, when we substitute (3.5) into (3.4), the terms

$$\Sigma^{(1)}_{C,D}, \; \Sigma^{(2)}_{C,D}$$

give 0 after the summation over C, D (since they give 0 on each orbit). Lemma 1 is proved.

For the proof of Fact B, we need the following lemma.

LEMMA 2. *If $0 \neq \beta \in R$, and $|\beta\overline{\beta}| < p$, then β is associated in R to a rational integer.*

Proof. Let $\beta = c\alpha - d$ with integers c and d. We may assume that $\alpha \leq |\beta| \leq 1$ and $c > 0$ (since for $c = 0$ we are done). Then

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

hence

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

The right-hand side is greater than $p - 1$ for $c \geq p$, so we have $1 \leq c < p$. Then $0 < c\alpha < 1$, and by $|\beta| \leq 1$ we can assume $d = 1$, because in the case $d = 0$ the proof is complete. Then

$$p > |\beta\overline{\beta}| = 1 - c^2 + pc,$$

which is impossible for c in the given range, and the lemma is proved.

Proof of Fact B. Assume that d is not a prime (but, by our assumptions, it is odd and squarefree). Let t be the least prime divisor of d. Since $(p, d) = 1$, and $(p + 1)^2$ is greater than d, we have $2 < t < p$. The discriminant of K is d, hence the prime t is ramified in K, so the ideal generated by t in R is a square of an ideal, say $(t) = a^2$. The class number is 1, so $a = (\beta)$ with some $0 \neq \beta \in R$, and this implies that

$$|\beta\overline{\beta}| = N(a) = t,$$

hence $|\beta\overline{\beta}| < p$ and $|\beta\overline{\beta}|$ is not a square, which is a contradiction by Lemma 2.

So we know that d is a prime, it is obviously congruent to 1 modulo 4, and by quadratic reciprocity it is enough to prove that $\left(\frac{r}{d}\right) = -1$. Assume that $\left(\frac{r}{d}\right) = 1$. It is well-known (and we can see from (2.1)) that the ideal (r) is then a product of two prime ideals in R; both prime ideals must have norm r. Since the class number is 1, it follows that there is a $0 \neq \beta \in R$ such that $|\beta\overline{\beta}| = r$, and since $r < p$ and r is not a square, this contradicts to Lemma 2, just as above. Fact B is proved.

4. Fixing the parameters

We will use the notations introduced in Section 2.

We will use Fact A for three concrete characters χ, denote them by χ_1, χ_2 and χ_3. The character χ_1 has conductor $175 = 5^2 \cdot 7$, while χ_2 and χ_3 have conductor 61.
Since 2 is a primitive root modulo 25, and 3 is a primitive root modulo 7, the character χ_1 is well defined by

$$\chi_1 = \chi_1^{(25)} \chi_1^{(7)},$$

where $\chi_1^{(25)}$ is a character modulo 25, $\chi_1^{(7)}$ is a character modulo 7, and

$$\chi_1^{(25)}(2) = i\xi,\ \chi_1^{(7)}(3) = \omega,$$

where ξ is a primitive fifth root of unity, i is the usual primitive fourth root of unity, and ω is a primitive third root of unity. It is easily seen that χ_1 is a primitive character modulo 175 and $\chi_1(-1) = -1$.
Since 2 is a primitive root modulo 61, the characters χ_2 and χ_3 are well defined by

$$\chi_2(2) = i\omega\xi,\ \chi_3(2) = i\xi.$$

These are obviously primitive characters modulo 61, and

$$\chi_2(-1) = \chi_3(-1) = -1.$$

Clearly

$$\mathcal{L}_\chi = \mathbf{Q}(\xi_{60}) \text{ for } \chi = \chi_1 \text{ and } \chi = \chi_2,$$

and

$$\mathcal{L}_\chi = \mathbf{Q}(\xi_{20}) \text{ for } \chi = \chi_3,$$

where ξ_n denotes a primitive nth root of unity.
Before giving the concrete examples we will work with, we quote a well-known general fact on the factorization of rational primes in cyclotomic fields. Let r be a rational prime and assume that

$$r \equiv 1 \pmod{n}. \tag{4.1}$$

Then, in the ring of algebraic integers of $\mathbf{Q}(\xi_n)$ the ideal (r) is a product of $\phi(n)$ distinct prime ideals, and these prime ideals have the form

$$(r, \xi_n - a), \tag{4.2}$$

where a runs over the rational integers $1 \leq a \leq r$ with

$$o_r(a) = n, \tag{4.3}$$

and $o_r(a)$ denotes the order of a modulo r. (See [W], pp. 14-15.) What we actually need is the fact that in the case of (4.1), the ideal (4.2) is a prime ideal for every rational integer a satisfying (4.3).
We now give our four examples. These examples correspond to the four arrows

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

respectively, mentioned in Section 2.
Example 1. Here

$$q = 175,\ r = 61,\ \chi = \chi_1,\ \mathcal{L}_\chi = \mathbf{Q}(\xi_{60}),$$

and we choose

$$I = (61, i\omega\xi - 10).$$

Since $o_{61}(10) = 60$, this is a prime ideal. We then have

$$\chi_1^{(25)}(2) = (i\omega\xi)^{21} \equiv 10^{21} \equiv 8 \pmod{I},$$

and

$$\chi_1^{(7)}(3) = (i\omega\xi)^{40} \equiv 10^{40} \equiv 47 \pmod{I}.$$

Consequently, for rational integers a,

$$\text{if } a \equiv 2^s \pmod{25}, \text{ then } \chi_1^{(25)}(a) \equiv 8^s \pmod{I}, \tag{4.4}$$

$$\text{if } a \equiv 3^t \pmod{7}, \text{ then } \chi_1^{(7)}(a) \equiv 47^t \pmod{I}. \tag{4.5}$$

Example 2. Here

$$q = 175,\ r = 1861,\ \chi = \chi_1,\ \mathcal{L}_\chi = \mathbf{Q}(\xi_{60}),$$

and we choose

$$I = (1861, i\omega\xi - 173).$$

Since $o_{1861}(173) = 60$, this is a prime ideal. We then have, just as above,

$$\chi_1^{(25)}(2) \equiv 173^{21} \equiv 380 \pmod{I},\ \text{and } \chi_1^{(7)}(3) \equiv 173^{40} \equiv 1406 \pmod{I}.$$

Consequently, for rational integers a,

$$\text{if } a \equiv 2^s \pmod{25}, \text{ then } \chi_1^{(25)}(a) \equiv 380^s \pmod{I}, \tag{4.6}$$

$$\text{if } a \equiv 3^t \pmod{7}, \text{ then } \chi_1^{(7)}(a) \equiv 1406^t \pmod{I}. \tag{4.7}$$

Example 3. Here

$$q = 61,\ r = 1861,\ \chi = \chi_2,\ \mathcal{L}_\chi = \mathbf{Q}(\xi_{60}),$$

and we choose

$$I = (1861, i\omega\xi - 1833).$$

Since $o_{1861}(1833) = 60$, this is a prime ideal. We then have, for rational integers a:

$$\text{if } a \equiv 2^s \pmod{61}, \text{ then } \chi(a) \equiv 1833^s \pmod{I}. \tag{4.8}$$

Example 4. Here

$$q = 61,\ r = 41,\ \chi = \chi_3,\ \mathcal{L}_\chi = \mathbf{Q}(\xi_{20}),$$

and we choose

$$I = (41, i\xi - 33).$$

Since $o_{41}(33) = 20$, this is a prime ideal. We then have, for rational integers a:

$$\text{if } a \equiv 2^s \pmod{61}, \text{ then } \chi(a) \equiv 33^s \pmod{I}. \tag{4.9}$$

It is clear that using formulas (4.4)−(4.9), we can verify whether Condition $(*)$ (see Section 2) is valid for these four (q, r) pairs or not (with the given χ and I). We will use for this the computer program of the next section, and we will find that it is satisfied in each case. Then we will have a possibility to apply the arguments of Section 2, in particular, formula (2.10).

5. The computer program

The aim of the computer program of this section is to compute m_χ modulo I, and also $A_\chi(p_0)$, $B_\chi(p_0)$ modulo I for every relevant residue class p_0 modulo q (see Section 2 for these notations). We will compute these quantities with the concrete parameters of the examples of Section 4, i.e. we compute them in four separate cases. Since I lies above r, and $|R/I| = r$, the computation modulo I is in practice a computation with rational integers modulo r.

Before giving the BASIC program itself, we say a few words about it.

We will apply the program for the four examples given in the previous section. We have to give the value of q, and then the value of r. These two

values already identify the example, and the program then works with the other data (i.e. χ and I) of that example.
The program uses data from a file depending on (q, r). Each data file contains 20 numbers, we write the interesting values of p_0 followed by zeros, if there are less than 20 interesting values. See the contents of the data files below. It will turn out in Section 6 that indeed these are the interesting values of p_0. Firstly, the program computes the values of our characters modulo the ideal I, based on equations (4.4)-(4.9). If $q = 175$, we have

$$d(n, 0) \equiv \chi_1^{(25)}(n) \pmod{I},\ d(n, 1) \equiv \chi_1^{(7)}(n) \pmod{I}.$$

If $q = 61$, we have

$$d(n, 2) \equiv \chi(n) \pmod{I}.$$

We use two subroutines. The first one (at line 20) is used only if $q = 175$. If $1 \leq g \leq 3$ is fixed, and the integers J, Z and $s(g)$ are given, this subroutine adds $\chi(J)Z$ to $s(g)$ (modulo the ideal I, of course). The second subroutine (at line 30) is the same as the previous one, but it is used when $q = 61$.
After computing the values of the characters, the program computes m_χ (we get it in result1.txt), then $A_\chi(p_0)$ (we get in result2.txt) and $B_\chi(p_0)$ (result3.txt) modulo I for every interesting value of p_0.
We now give the data files. In the first line we write the contents of data0.txt, the second line is data1.txt, the third line is data2.txt, while the fourth one is data3.txt:

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

8, 13, 18, 22, 32, 38, 43, 53, 67, 78, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0;

6, 10, 24, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0;

13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

Here is the QBasic program:

```
DEFDBL A−Z
IF q = 175 AND r = 61 THEN OPEN "data0.txt" FOR INPUT AS #1
IF q = 175 AND r = 1861 THEN OPEN "data1.txt" FOR INPUT AS #1
IF q = 61 AND r = 1861 THEN OPEN "data2.txt" FOR INPUT AS #1
IF q = 61 AND r = 41 THEN OPEN "data3.txt" FOR INPUT AS #1
OPEN "result1.txt" FOR OUTPUT AS #2
OPEN "result2.txt" FOR OUTPUT AS #3
OPEN "result3.txt" FOR OUTPUT AS #4
```

```
DIM d(60, 2): DIM s(3)
REM ======= WE COMPUTE THE VALUES OF THE CHARAC-
TERS
p = 1: d(1, 0) = 1: FOR J = 1 TO 19
v = p: p = (2 * p) MOD 25
IF r = 61 THEN d(p, 0) = (8 * d(v, 0)) MOD r
IF r = 1861 THEN d(p, 0) = (380 * d(v, 0)) MOD r
NEXT J
p = 1: d(1, 1) = 1: FOR J = 1 TO 5
v = p: p = (3 * p) MOD 7
IF r = 61 THEN d(p, 1) = (47 * d(v, 1)) MOD r
IF r = 1861 THEN d(p, 1) = (1406 * d(v, 1)) MOD r
NEXT J
p = 1: d(1, 2) = 1: FOR J = 1 TO 59
v = p: p = (2 * p) MOD 61
IF r = 1861 THEN d(p, 2) = (1833 * d(v, 2)) MOD r
IF r = 41 THEN d(p, 2) = (33 * d(v, 2)) MOD r
NEXT J
GOTO 40
REM ======= IF q = 175, THIS SUBROUTINE ADDS χ(J)Z 20 IF
J
MOD 5 = 0 OR J MOD 7 = 0 THEN GOTO 25
s = d(((J MOD 25) + 25) MOD 25, 0): L = d(((J MOD 7) + 7) MOD 7,
1)
w = (s * L) MOD r
s(g) = (((s(g) + w * Z) MOD r) + r) MOD r
25 RETURN
REM ======= IF q = 61, THIS SUBROUTINE ADDS χ(J)Z
30 IF J MOD 61 = 0 THEN GOTO 35
s = d(((J MOD 61) + 61) MOD 61, 2)
s(g) = (((s(g) + s * Z) MOD r) + r) MOD r
35 RETURN
REM ======= WE COMPUTE m_χ (AS s(1))
40 g = 1: FOR J = 1 TO q − 1
Z = J: IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
NEXT J
REM ======= p(a) ARE THE POSSIBLE VALUES OF p_0
DIM p(20): FOR a = 1 TO 20: INPUT #1, p(a)
IF p(a) = 0 THEN GOTO 70
REM ======= WE COMPUTE A_χ(p_0) (AS s(2)) AND
REM ======= B_χ(p_0) (AS s(3))
FOR c = 0 TO q − 1: FOR d = 0 TO q − 1
J = d * d − c * c − p(a) * c * d
```

```
g = 2: Z = (q − c) ∗ INT((d − p(a) ∗ c) / q)
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
g = 3: Z = (c − q) ∗ c
IF q = 175 THEN GOSUB 20
IF q = 61 THEN GOSUB 30
NEXT d: NEXT c
REM ======= WE PRINT THE RESULTS
FOR g = 1 TO 3: IF a > 1 AND g = 1 THEN GOTO 60
IF g > 1 THEN PRINT #(g + 1), "for "; p(a); " we get "; s(g)
IF g = 1 THEN PRINT #(g + 1), " we get "; s(g)
s(g) = 0
60 NEXT g
70 NEXT a
CLOSE #1: CLOSE #2: CLOSE #3: CLOSE #4
```

6. Concluding the proof

Firstly, we show that a residue class and its negative always behave in the same way during our proof. We can spare half of the computations by this observation.

Recall the definitions of $A_\chi(j)$ and $B_\chi(j)$ from Section 2.

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

(i) $B_\chi(q-j)=B_\chi(j)$;

(ii) $A_\chi(q-j)+A_\chi(j)=B_\chi(j)$.

Proof. Let $(t)_q$ denote the least nonnegative residue of t modulo q. Then, replacing D by $(q-D)_q$ in the definition of $B_\chi(q-j)$, we get (i). The same reasoning gives that the left-hand side of (ii) equals to

$$\sum_{C,D=0}^{q-1}\chi(D^2-C^2-jCD)\left(\left\lceil\frac{(q-j)C-(q-D)_q}{q}\right\rceil+\left\lceil\frac{jC-D}{q}\right\rceil\right)(C-q).$$

If $D\neq 0$, then

$$\left\lceil\frac{(q-j)C-(q-D)_q}{q}\right\rceil+\left\lceil\frac{jC-D}{q}\right\rceil=\begin{cases}C-1, \text{ if } D\equiv jC \pmod q\\ \\ C \text{ otherwise}\end{cases},$$

since the sum of the arguments of the upper integer parts is $C-1$. If $D=0$, then the sum is 1 larger. Thus, using $(j,q)=1$, the left-hand side of (ii) equals to

$$B_\chi(j) - \sum_{1\le C,D\le q-1,\ D\equiv jC} \chi(-C^2)(C-q) + \sum_{1\le C\le q-1,\ D=0} \chi(-C^2)(C-q)$$

(the congruence in the first sum is meant modulo q), which proves (ii).

Proof of the Theorem. Since our program in Section 5 applied for the four (q,r) pairs given in the examples of Section 4 gives 0 for $m_\chi \pmod I$, but gives nonzero results for $B_\chi(p_0) \pmod I$ (i.e. the results are rational integers not divisible by r) for certain values of $p_0 \in U_q$ (hence for all $p_0 \in U_q$, see (2.9)), we get that these four (q,r) pairs satisfy Condition $(*)$. Hence we can apply (2.10), and we can follow the steps outlined in Section 2. Note that if two rational integers are congruent modulo I, then they are congruent modulo r, so (2.10) gives us the value of p modulo r.
By Lemma 3, we have

$$j - q\frac{A_\chi(j)}{B_\chi(j)} \equiv -\left((q-j) - q\frac{A_\chi(q-j)}{B_\chi(q-j)}\right) \tag{6.1}$$

modulo I for every $(j,q)=1$, 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. In the first column of Table 1 we list the 20 values of p_0 (see (2.5) for its meaning) for which

$$0 < p_0 < \frac{175}{2},\ p_0 \equiv \pm 2 \pmod 5 \text{ and } \ p_0 \equiv \pm 1, \pm 3 \pmod 7.$$

These are the elements of U_{175} in the given range (for $p_0 \notin U_{175}$ we are done, p^2+4 is a square modulo 5 or 7). In the second and third columns we give $A_\chi(p_0)$ and $B_\chi(p_0)$ modulo I, respectively (obtained by the program); the fourth column gives p modulo 61, and it is computed from the first three columns, using (2.10). The fifth column is determined by the fourth

column: if p^2+4 is a square modulo 61, then we write a number n into the fifth column such that

$$n^2 \equiv p^2 + 4 \pmod{61};$$

otherwise we leave the fifth column empty.

For the 10 values of p_0 where the fifth column of Table 1 is empty, we apply the program with the parameters of Example 2 (in particular, $q = 175$ and $r = 1861$). The results are summarized in Table 2, which is completely analogous to Table 1.

We know from (6.1) that if we replace a particular p_0 by $175 - p_0$ in the first column of Table 1 or Table 2, then in the fourth column we obtain the negative of the residue class belonging to p_0 in the fourth column. Consequently, p^2+4 modulo 61 (or modulo 1861 in the case of Table 2) is unchanged. Hence, if the fifth column is nonempty at the row of a p_0 in Table 1 or in Table 2, then p_0 and $175 - p_0$ are excluded in the sense that for

$$p \equiv \pm p_0 \pmod{175}$$

p^2+4 is a square modulo 61 or modulo 1861. The remaining possibilities are summarized in Table 3, where we mean that either the plus or the minus sign is valid inside a row, and one of the rows must be valid for our p.

For $p \equiv 6$, 10 or 24 modulo 61 we apply the program with the parameters of Example 3. The result is Table 4, which is completely analogous to Tables 1 and 2, but we do not need the fifth column, so we omit it. Since

$$612 \not\equiv \pm 1058,\ 881 \not\equiv \pm 1107,\ 881 \not\equiv \pm 1062 \text{ and } 460 \not\equiv \pm 1634$$

modulo 1861, so, using (6.1), we see by Tables 3 and 4 that the only possible values for p modulo 61 are ± 13 (since otherwise p would belong to two different residue classes modulo 1861, which is a contradiction).

Hence, if we consider Example 4 ($q = 61$, $r = 41$), the only possibilities for p_0 are 13 and $61 - 13 = 48$. For p_0= 13 we apply the program and we obtain

$$A_\chi(p_0) \equiv 0 \,(\mathrm{mod}\ I) \text{ and } B_\chi(p_0) \equiv 13 \,(\mathrm{mod}\ I).$$

Hence (2.10) gives

$$p \equiv 13 \,(\mathrm{mod}\ 41).$$

By (6.1), we know that then $p_0 = 48$ gives

$$p \equiv -13 \,(\mathrm{mod}\ 41).$$

In both cases, we have

$$p^2 + 4 \equiv 173 \equiv 3^2 \,(\mathrm{mod}\ 41),$$

so the Theorem is proved.

TABLE 1.

We use the parameters of Example 1, in particular q=175, $r = 61$.

The second and third columns are meant modulo I.

p_0	$A_\chi(p_0)$	$B_\chi(p_0)$	$p \bmod r$	$\sqrt{p^2+4} \bmod r$
3	0	51	3	14
8	0	33	8	
13	0	24	13	
17	0	26	17	7
18	34	44	2	
22	34	53	49	
27	24	50	4	9
32	1	44	10	
38	40	30	8	
43	46	23	59	
48	20	50	39	0
52	14	32	25	18
53	13	51	6	
57	54	23	36	18
62	42	24	15	30
67	28	26	24	
73	6	32	44	7
78	27	53	51	
83	32	33	39	0
87	19	30	27	1

TABLE 2.

We use the parameters of Example 2, in particular q=175, $r = 1861$.

The second and third columns are meant modulo I.

p_0	$A_\chi(p_0)$	$B_\chi(p_0)$	$p \bmod r$	$\sqrt{p^2+4} \bmod r$
8	0	1121	8	505
13	0	1498	13	
18	1254	1060	285	385
22	60	1588	1492	263
32	135	1060	1107	
38	1633	1397	321	760
43	1294	1102	1685	748
53	1275	1389	1058	
67	1773	1720	1634	
78	344	1588	1062	

TABLE 3.

$p \bmod 175$	$p \bmod 61$	$p \bmod 1861$
± 13	± 13	± 13
± 32	± 10	± 1107
± 53	± 6	± 1058
± 67	± 24	± 1634
± 78	± 51	± 1062

TABLE 4.

We use the parameters of Example 3, in particular q=61, $r = 1861$.

The second and third columns are meant modulo I.

p_0	$A_\chi(p_0)$	$B_\chi(p_0)$	$p \bmod r$
6	957	1000	612
10	1150	616	881
24	173	663	460

References

[B] J. Beck, *Diophantine approximation and quadratic fields,* 55-93., in: Number Theory, eds. Győry, Pethő, Sós; Walter de Gruyter, 1998

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

[D] H. Davenport, *Multiplicative Number Theory*, 2nd edition, Springer, 1980

[G] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer,* Ann. Scuola Norm. Sup. Pisa (4) 3 (1976), 623-663.

[G-Z] B. Gross and J. Zagier, *Points de Heegner et derivees de fonctions L,* C.R. Acad. Sci. Paris, 297 (1983), 85-87.

[M] Ming-yao Zhang, *On Yokoi's conjecture*, Math. Comp. 64 (212) (1995), 1675-85.

[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] T. Shintani, *On special values of zeta functions of totally real algebraic number fields*, in: Proc. Internat. Cong. of Math., Helsinki, 1978, 591-597.

[Y] H.Yokoi, *Class number one problem for certain kind of real quadratic fields*, in: Proc. Internat. Conference, Katata, Japan (1986), 125-137., Nagoya Univ., Nagoya, 1986

[W] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1982