

Mollin's conjecture

by

DONGHO BYEON, MYOUNGIL KIM and JUNGYUN LEE (Seoul)

1. Introduction and statement of results. Let $K = \mathbb{Q}(\sqrt{d})$, where d is a positive square free integer, and let $h(d)$ be the class number of this field. Chowla [3] conjectured that $h(4n^2 + 1) > 1$ if $n > 13$ and Yokoi [9] conjectured that $h(n^2 + 4) > 1$ if $n > 17$. In the celebrated papers [1], [2], Biró proved these two conjectures.

DEFINITION 1.1. Let $d = n^2 + r$, $d \neq 5$, be a positive square free integer satisfying $r \mid 4n$ and $-n < r \leq n$. Then we call $K = \mathbb{Q}(\sqrt{d})$ a real quadratic field of *Richaud–Degert type*. Specifically if $|r| \in \{1, 4\}$, then $K = \mathbb{Q}(\sqrt{d})$ is of *narrow Richaud–Degert type*.

Chowla and Yokoi conjectures involve narrow Richaud–Degert type. In [5], Mollin also conjectured that $h(n^2 - 4) > 1$ if $n > 21$. In this paper we will prove that Mollin's conjecture is true and thus complete the class number 1 problem for real quadratic fields of narrow Richaud–Degert type.

THEOREM 1.2. *If d is square free and $d = n^2 - 4$ with some positive integer $n > 21$, then $h(d) > 1$.*

To prove Theorem 1.2, we basically follow Biró's idea. First we prove

THEOREM 1.3. *If d is square free, $h(d) = 1$ and $d = n^2 - 4$ with some positive integer n , then $\left(\frac{d}{q}\right) = 0$ or 1 for at least one of $q = 5, 7, 61, 1861$.*

Theorem 1.2 follows immediately from Theorem 1.3, the well known class number 1 criterion [5]:

Let $d = n^2 - 4 > 5$ be a square free. Then $h(d) = 1$ if and only if $\left(\frac{d}{q}\right) = -1$ for all primes $q < n - 2$

and the class number table for real quadratic fields of narrow Richaud–Degert type. A new ingredient in this paper is developing techniques of

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

This work was supported by KRF-R08-2003-000-10243-0 and partially by KRF-2005-070-C00004. The first author holds joint appointment in the Research Institute of Mathematics, Seoul National University.

computing $\zeta_{P(K)}(0, \chi)$ (see Section 2 for definition), where K is a quadratic field whose fundamental unit's norm is positive. We note that the norms of the fundamental units of real quadratic fields in the Chowla or Yokoi conjectures are negative.

REMARK. Using the techniques developed in this paper, we can compute $\zeta_{P(K)}(0, \chi)$ for all real quadratic fields K of Richaud–Degert type. But class number 1 criteria for some real quadratic fields of Richaud–Degert type (see [6]), for example, for $d = n^2 \pm 2$, are different from those for narrow Richaud–Degert type. So we cannot directly apply this method to determine all real quadratic fields of Richaud–Degert type with class number 1.

2. Computation of $\zeta_{P(K)}(0, \chi)$. Let $d = n^2 - 4$ be a positive square free integer with $n \geq 5$. Let $K = \mathbb{Q}(\sqrt{d})$, R the ring of integers of K , and $\varepsilon = (n + \sqrt{n^2 - 4})/2$ the fundamental unit of K . We know that $\{1, \varepsilon\}$ is an integral basis for R . For an integral ideal a , let $N(a)$ be the order of R/a , and for an element α of K , let $N(\alpha) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\alpha)$. We note that $N(\varepsilon) = 1$. Let $I(K)$ be the set of nonzero fractional ideals of K and $P(K)$ the set of nonzero principal ideals of R . Define the map $i : K^* \rightarrow I(K)$ by $\alpha (\neq 0) \mapsto (\alpha)$. Let K^+ be the set of totally positive elements in K . Then we have the following lemmas.

LEMMA 2.1. $[i(K^*) : i(K^+)] = 2$.

Proof. See pages 242–243 in [4]. ■

LEMMA 2.2. *Any principal ideal (α) in $i(K^+)$ can be uniquely written in the form*

$$(\alpha) = (X + Y\varepsilon)$$

with some rational numbers $X > 0, Y \geq 0$; conversely if $X > 0$ and $Y \geq 0$ are rational numbers, then $(X + Y\varepsilon) \in i(K^+)$.

Proof. Let $\alpha \in K^+$ and suppose that $(\alpha) = (\beta)$ for some $\beta \in K$. Then $\beta = \varepsilon^j \alpha$ for some integer j . So there exists a unique $\beta \in K$ such that $(\alpha) = (\beta)$ and $\beta > 0, \bar{\beta} > 0, 1 \leq \beta/\bar{\beta} < \varepsilon^2$. We can write $\beta = X + Y\varepsilon$ for $X, Y \in \mathbb{Q}$. Then

$$X + Y\bar{\varepsilon} \leq X + Y\varepsilon < \varepsilon^2(X + Y\bar{\varepsilon}).$$

So

$$X(\varepsilon^2 - 1) > 0 \quad \text{and} \quad Y(\varepsilon - \bar{\varepsilon}) \geq 0.$$

Thus $X > 0$ and $Y \geq 0$.

Conversely, if $X > 0$ and $Y \geq 0$ are rational numbers, then $X + Y\varepsilon > 0$ and $X + Y\bar{\varepsilon} > 0$, since ε and $\bar{\varepsilon}$ are greater than 0. So $(X + Y\varepsilon) \in i(K^+)$. ■

Let $q > 2$ be an integer with $(q, d) = 1$ and let χ be an odd primitive character with conductor q . For $s \in \mathbb{C}$ with $\text{Re } s > 1$ define

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

We note that $\zeta_{P(K)}(s, \chi)$ extends meromorphically in s to the whole complex plane. From Lemma 2.1,

$$i(K^*) = (q)i(K^+) \cup (q)bi(K^+),$$

where

$$b = (\omega) \in i(K^*) - i(K^+) \quad \text{and} \quad \omega = \frac{n - 2 + \sqrt{n^2 - 4}}{2}.$$

So

$$\zeta_{P(K)}(s, \chi) = \sum_{\substack{a \in (q)i(K^+) \\ \text{integral}}} \frac{\chi(N(a))}{N(a)^s} + \sum_{\substack{a \in (q)bi(K^+) \\ \text{integral}}} \frac{\chi(N(a))}{N(a)^s} =: \zeta^+(s) + \zeta^-(s).$$

First we compute $\zeta^+(0)$. By Lemma 2.2, if $a \in (q)i(K^+)$, then $a = q(X + Y\varepsilon)$ for $X, Y \in \mathbb{Q}$ such that $X > 0$ and $Y \geq 0$. We can write $X = x + n_1$ and $Y = y + n_2$, where $0 < x \leq 1$, $0 \leq y < 1$ and n_1, n_2 are nonnegative integers. So

$$\begin{aligned} \zeta^+(s) &= \sum_{\substack{a \in (q)i(K^+) \\ \text{integral}}} \frac{\chi(N(a))}{N(a)^s} = \sum_{(x,y) \in R^1} \sum_{n_1, n_2=0}^{\infty} \frac{\chi(N(q(x + n_1 + \varepsilon(y + n_2))))}{N(q(x + n_1 + \varepsilon(y + n_2)))^s} \\ &= \sum_{(x,y) \in R^1} \sum_{n_1, n_2=0}^{\infty} \frac{\chi(N(q(x + y\varepsilon)))}{N(q(x + n_1 + \varepsilon(y + n_2)))^s}, \end{aligned}$$

where

$$R^1 = \{(x, y) \in \mathbb{Q}^2 \mid qx + qy\varepsilon \in R, 0 < x \leq 1, 0 \leq y < 1\}.$$

Since $C + D\varepsilon$ 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 $q(x + y\varepsilon) \in C + D\varepsilon + qR$. Let

$$R^1(C, D) = \{(x, y) \in R^1 \mid q(x + y\varepsilon) \in C + D\varepsilon + qR\}.$$

From the work of Shintani [7], [8],

$$\begin{aligned} \zeta^+(0) &= \sum_{C, D=0}^{q-1} \chi(N(C + D\varepsilon)) \\ &\quad \times \sum_{(x,y) \in R^1(C,D)} \sum_{n_1, n_2=0}^{\infty} \frac{1}{N(q(x + n_1 + \varepsilon(y + n_2)))^s} \Big|_{s=0} \end{aligned}$$

$$\begin{aligned}
&= \sum_{C,D=0}^{q-1} \chi(C^2 + D^2 + nCD) \sum_{(x,y) \in R^1(C,D)} \zeta\left(0, \begin{pmatrix} 1 & \varepsilon \\ 1 & \bar{\varepsilon} \end{pmatrix}, (x, y)\right) \\
&= \sum_{C,D=0}^{q-1} \left[\chi(C^2 + D^2 + nCD) \right. \\
&\quad \times \left. \sum_{(x,y) \in R^1(C,D)} \left\{ \left(x - \frac{1}{2}\right) \left(y - \frac{1}{2}\right) + \frac{n}{4} \left(x^2 + y^2 - (x+y) + \frac{1}{3}\right) \right\} \right].
\end{aligned}$$

We note that

$$\begin{aligned}
(x, y) \in R^1(C, D) &\Leftrightarrow q(x + y\varepsilon) = C + D\varepsilon + q(i + j\varepsilon) \text{ for } i, j \text{ integers and } (x, y) \in R^1 \\
&\Leftrightarrow 0 < x = \frac{C + qi}{q} \leq 1, \quad 0 \leq y = \frac{D + qj}{q} < 1 \text{ for } i, j \text{ integers} \\
&\Leftrightarrow x = \begin{cases} 1 & \text{if } C = 0, \\ C/q & \text{if } C \neq 0, \end{cases} \quad y = \frac{D}{q}.
\end{aligned}$$

Replacing x, y with the above we have

$$\begin{aligned}
\zeta^+(0) &= \sum_{\substack{C=0 \\ 0 \leq D \leq q-1}} \chi(C^2 + D^2 + nCD) \\
&\quad \times \left\{ \frac{1}{2} \left(\frac{D}{q} - \frac{1}{2}\right) + \frac{n}{4} \left(1 + \frac{D^2}{q^2} - \left(1 + \frac{D}{q}\right) + \frac{1}{3}\right) \right\} \\
&\quad + \sum_{\substack{0 < C \leq q-1 \\ 0 \leq D \leq q-1}} \left[\chi(C^2 + D^2 + nCD) \right. \\
&\quad \times \left. \left\{ \left(\frac{C}{q} - \frac{1}{2}\right) \left(\frac{D}{q} - \frac{1}{2}\right) + \frac{n}{4} \left(\frac{C^2}{q^2} + \frac{D^2}{q^2} - \left(\frac{C+D}{q}\right) + \frac{1}{3}\right) \right\} \right] \\
&= \sum_{C,D=0}^{q-1} \left[\chi(C^2 + D^2 + nCD) \right. \\
&\quad \times \left. \left\{ \left(\frac{C}{q} - \frac{1}{2}\right) \left(\frac{D}{q} - \frac{1}{2}\right) + \frac{n}{4} \left(\frac{C^2}{q^2} + \frac{D^2}{q^2} - \left(\frac{C+D}{q}\right) + \frac{1}{3}\right) \right\} \right] \\
&\quad + \sum_{D=0}^{q-1} \chi(D^2) \left(\frac{D}{q} - \frac{1}{2}\right)
\end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{12q^2} \sum_{C,D=0}^{q-1} \chi(C^2 + D^2 + nCD) \\
 &\quad \times (6C^2n + 12CD - 6qnC - 12Cq + (n + 3)q^2) \\
 &\quad + \frac{1}{12q^2} \sum_{D=0}^{q-1} \chi(D^2)(2D - q)6q.
 \end{aligned}$$

Now we compute $\zeta^-(0)$. Let

$$R^2 = \{(x, y) \in \mathbb{Q}^2 \mid \omega(qx + qy)\varepsilon \in R, 0 < x \leq 1, 0 \leq y < 1\}.$$

Since $C + D\omega$ 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 $\omega(qx + qy\varepsilon) \in C + D\omega + qR$. Let

$$R^2(C, D) = \{(x, y) \in R^2 \mid \omega(qx + qy\varepsilon) \in C + D\omega + qR\}.$$

Then

$$\begin{aligned}
 \zeta^-(s) &= \sum_{\substack{a \in (q)bi(K^+) \\ \text{integral}}} \frac{\chi(N(a))}{N(a)^s} \\
 &= \sum_{(x,y) \in R^2} \sum_{n_1, n_2=0}^{\infty} \frac{\chi(-N(q\omega(x + n_1 + \varepsilon(y + n_2))))}{(-N(q\omega(x + n_1 + \varepsilon(y + n_2))))^s} \\
 &= \sum_{(x,y) \in R^2} \sum_{n_1, n_2=0}^{\infty} \frac{\chi(-N(q\omega(x + y\varepsilon)))}{(-N(q\omega(x + n_1 + \varepsilon(y + n_2))))^s} \\
 &= \sum_{C,D=0}^{q-1} -\chi(N(C + D\omega)) \\
 &\quad \times \sum_{(x,y) \in R^2(C,D)} \sum_{n_1, n_2=0}^{\infty} \frac{1}{(-N(q\omega(x + n_1 + \varepsilon(y + n_2))))^s} \\
 &= \sum_{C,D=0}^{q-1} \left[-\chi(N(C + D\omega)) \sum_{(x,y) \in R^2(C,D)} \sum_{n_1, n_2=0}^{\infty} \frac{1}{(n - 2)^s q^{2s} ((x + n_1 + (y + n_2)\varepsilon)(x + n_1 + (y + n_2)\bar{\varepsilon}))^s} \right].
 \end{aligned}$$

From the work of Shintani [7], [8],

$$\begin{aligned}
\zeta^-(0) &= \sum_{C,D=0}^{q-1} -\chi(C^2 - (n-2)D^2 + (n-2)CD) \\
&\quad \times \sum_{(x,y) \in R^2(C,D)} \zeta\left(0, \begin{pmatrix} 1 & \varepsilon \\ 1 & \bar{\varepsilon} \end{pmatrix}, (x, y)\right) \\
&= \sum_{C,D=0}^{q-1} \left[-\chi(C^2 - (n-2)D^2 + (n-2)CD) \right. \\
&\quad \left. \times \sum_{(x,y) \in R^2(C,D)} \left\{ \left(x - \frac{1}{2}\right) \left(y - \frac{1}{2}\right) + \frac{n}{4} \left(x^2 + y^2 - (x+y) + \frac{1}{3}\right) \right\} \right].
\end{aligned}$$

We note that

$$(x, y) \in R^2(C, D)$$

$$\Leftrightarrow q\omega(x + y\varepsilon) = C + D\omega + q(i + j\omega) \text{ for } i, j \text{ integers and } (x, y) \in R^2$$

$$\Leftrightarrow (n-2)q(x + y\varepsilon) = -(n-1)(C + iq) + (n-2)(D + jq) + \varepsilon(C + iq)$$

$$\text{for } i, j \text{ integers and } (x, y) \in R^2$$

$$\Leftrightarrow 0 < x = \frac{-(n-1)(C + iq) + (n-2)(D + jq)}{(n-2)q} \leq 1,$$

$$0 \leq y = \frac{C + iq}{(n-2)q} < 1 \text{ for } i = 0, 1, \dots, n-3 \text{ integers and}$$

$$j = \left[1 + \frac{(C + iq)(n-1)}{q(n-2)} - \frac{D}{q} \right].$$

Thus

$$\begin{aligned}
x &= \frac{-(C + iq)(n-1)}{(n-2)q} + \frac{D}{q} + \left[1 + \frac{(C + iq)(n-1)}{q(n-2)} - \frac{D}{q} \right] \\
&= \left[i + \frac{C-D}{q} + \frac{C+iq}{q(n-2)} \right] - \left(i + \frac{C-D}{q} + \frac{C+iq}{q(n-2)} \right) + 1 \\
&= \left[i + \left[\frac{C-D}{q} \right] + \frac{r(C, D)}{q} + \frac{C+iq}{q(n-2)} \right] \\
&\quad - \left(i + \left[\frac{C-D}{q} \right] + \frac{r(C, D)}{q} + \frac{C+iq}{q(n-2)} \right) + 1 \\
&= \left[\frac{r(C, D)}{q} + \frac{C+iq}{q(n-2)} \right] - \left(\frac{r(C, D)}{q} + \frac{C+iq}{q(n-2)} \right) + 1
\end{aligned}$$

for $i = 0, 1, \dots, n-3$ integers, where $r(C, D) = C - D - q\left[\frac{C-D}{q}\right]$. Since

$$0 \leq \frac{r(C, D)}{q} + \frac{C+iq}{q(n-2)} < 2,$$

it follows that

$$x = \begin{cases} -\left(\frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)}\right) + 1 & \text{if } \frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)} < 1, \\ -\left(\frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)}\right) + 2 & \text{if } \frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)} \geq 1. \end{cases}$$

Let

$$s(C, D) = \left\lceil \frac{(n-2)r(C, D) + C}{q} \right\rceil.$$

Then $(x, y) \in R^2(C, D)$ if and only if

$$x = \begin{cases} -\left(\frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)}\right) + 1 & \text{if } 0 \leq i < n - 2 - s(C, D), \\ -\left(\frac{r(C, D)}{q} + \frac{C + iq}{q(n-2)}\right) + 2 & \text{if } n - 2 - s(C, D) \leq i < n - 2, \end{cases}$$

$$y = \frac{C + iq}{(n-2)q} \quad \text{for } 0 \leq i < n - 2.$$

Replacing x, y with the above we have

$$\zeta^-(0) = \sum_{C, D=0}^{q-1} -\chi(C^2 - (n-2)D^2 + (n-2)CD)S(C, D),$$

where

$$\begin{aligned} S(C, D) = & \sum_{i=0}^{n-3-s(C, D)} \left\{ -\frac{C + iq}{2q} \left(-\frac{r(C, D)}{q} - \frac{C + iq}{(n-2)q} + 1 \right) \right. \\ & \left. - \frac{n+2}{4} \left(1 - \frac{r(C, D)}{q} \right) + \frac{n}{4} \left(1 - \frac{r(C, D)}{q} \right)^2 + \frac{n+3}{12} \right\} \\ & + \sum_{i=n-2-s(C, D)}^{n-3} \left\{ -\frac{C + iq}{2q} \left(-\frac{r(C, D)}{q} - \frac{C + iq}{(n-2)q} + 2 \right) \right. \\ & \left. - \frac{n+2}{4} \left(2 - \frac{r(C, D)}{q} \right) + \frac{n}{4} \left(2 - \frac{r(C, D)}{q} \right)^2 + \frac{n+3}{12} \right\} \end{aligned}$$

(by using MATHEMATICA)

$$\begin{aligned} = & \frac{1}{12q^2} (-6Cq - 6Cqs(C, D) + 6C^2 - q^2n - 12Cr(C, D) + 3q^2 \\ & + 6Cr(C, D)n + 6r(C, D)q - 3r(C, D)qn + 9q^2s(C, D) + 3q^2s(C, D)^2 \\ & - 6r(C, D)qs(C, D)n - 6nr(C, D)^2 + 3n^2r(C, D)^2) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{12q^2} \{3((n-2)r(C, D) + C - s(C, D)q)^2 + 3C^2 \\
&\quad + (3-n)q^2 - 6Cq + 9q^2s(C, D) - 12r(C, D)qs(C, D) \\
&\quad + 6nr(C, D)^2 - 12r(C, D)^2 + 6r(C, D)q - 3r(C, D)qn\}.
\end{aligned}$$

Since

$$r(C, D) = \begin{cases} C - D & \text{if } C - D \geq 0, \\ q + C - D & \text{if } C - D < 0, \end{cases}$$

we obtain the following equations:

$$\begin{aligned}
(1) \quad &\sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))r(C, D) \\
&= \sum_{\substack{C, D=0 \\ C < D}}^{q-1} \chi(Q_{C, D}(n))q + \sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))(C - D), \\
(2) \quad &\sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))r(C, D)^2 \\
&= \sum_{\substack{C, D=0 \\ C < D}}^{q-1} \chi(Q_{C, D}(n))(q^2 + 2q(C - D)) + \sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))(C - D)^2, \\
(3) \quad &\sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))s(C, D)r(C, D) \\
&= \sum_{\substack{C, D=0 \\ C < D}}^{q-1} \chi(Q_{C, D}(n))((q + C - D)(n - 2) + qv_{C, D}(n)) \\
&\quad + \sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))(C - D)v_{C, D}(n), \\
(4) \quad &\sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))s(C, D) \\
&= \sum_{\substack{C, D=0 \\ C < D}}^{q-1} \chi(Q_{C, D}(n))(n - 2) + \sum_{C, D=0}^{q-1} \chi(Q_{C, D}(n))v_{C, D}(n),
\end{aligned}$$

where

$$v_{C,D}(n) = \left\lfloor \frac{n(C-D) + 2D - C}{q} \right\rfloor,$$

$$Q_{C,D}(n) = C^2 - (n-2)D^2 + (n-2)CD.$$

Moreover,

$$(5) \quad (n-2)r(C, D) + C - qs(C, D)$$

$$= (n-2)(C-D) + C - q(n-2) \left\lfloor \frac{C-D}{q} \right\rfloor$$

$$- q \left\lfloor \frac{(n-2)(C-D) + C - q(n-2) \left\lfloor \frac{C-D}{q} \right\rfloor}{q} \right\rfloor$$

$$= (n-2)(C-D) + C - q \left\lfloor \frac{(n-2)(C-D) + C}{q} \right\rfloor =: u_{C,D}(n).$$

From equations (1)–(5), we have the following value of $\zeta^-(0)$:

$$\zeta^-(0) = -\frac{1}{12q^2} \sum_{C,D=0}^{q-1} [\chi(C^2 - (n-2)D^2 + (n-2)CD)$$

$$\times \{3u_{C,D}(n)^2 + 3C^2 + 6n(C-D)^2 - 12(C-D)^2 - 6Cq$$

$$- 12qv_{C,D}(n)(C-D)$$

$$- 3nq(C-D) + 6q(C-D) + q^2(3 + 9v_{C,D}(n) - n)\}]$$

$$- \frac{1}{12q^2} \sum_{\substack{C,D=0 \\ C < D}}^{q-1} [\chi(C^2 - (n-2)D^2 + (n-2)CD)$$

$$\times \{(6n-12)(q^2 + 2q(C-D)) - 12q((q+C-D)(n-2)$$

$$+ qv_{C,D}(n)) + (6q-3qn)q + 9q^2(n-2)\}]$$

$$= -\frac{1}{12q^2} \sum_{C,D=0}^{q-1} [\chi(C^2 - (n-2)D^2 + (n-2)CD)$$

$$\times \{3u_{C,D}(n)^2 + 3C^2 + 6n(C-D)^2 - 12(C-D)^2 - 6Cq$$

$$- 12qv_{C,D}(n)(C-D)$$

$$- 3nq(C-D) + 6q(C-D) + q^2(3 + 9v_{C,D}(n) - n)\}]$$

$$- \frac{1}{12q^2} \sum_{\substack{C,D=0 \\ C < D}}^{q-1} \chi(C^2 - (n-2)D^2 + (n-2)CD)(-v_{C,D}(n)12q^2).$$

Combining the values of $\zeta^+(0)$ and $\zeta^-(0)$, we have

$$\begin{aligned}
(6) \quad \zeta_{P(K)}(0, \chi) &= \frac{1}{12q^2} \sum_{C,D=0}^{q-1} \chi(C^2 + D^2 + nCD) \\
&\quad \times \{6C^2n + 12CD - 6qnC - 12Cq + (n+3)q^2\} \\
&\quad + \frac{1}{12q^2} \sum_{D=0}^{q-1} \chi(D^2)(2D - q)6q \\
&\quad - \frac{1}{12q^2} \sum_{C,D=0}^{q-1} [\chi(C^2 - (n-2)D^2 + (n-2)CD) \\
&\quad \times \{3u_{C,D}(n)^2 + 3C^2 + 6n(C-D)^2 - 12(C-D)^2 - 6Cq \\
&\quad - 12qv_{C,D}(n)(C-D) - 3nq(C-D) \\
&\quad + 6q(C-D) + q^2(3 + 9v_{C,D}(n) - n)\}] \\
&\quad + \frac{1}{12q^2} \sum_{\substack{C,D=0 \\ C < D}}^{q-1} \chi(C^2 - (n-2)D^2 + (n-2)CD)v_{C,D}(n)12q^2.
\end{aligned}$$

Finally, we obtain the following lemma.

LEMMA 2.3. *Let $d = n^2 - 4$, $n > 5$, be a positive square free integer, $q > 2$ an integer with $(q, d) = 1$, and χ an odd character with conductor q . Let*

$$\begin{aligned}
u_{C,D}(n) &= n(C - D) + 2D - C - q \left[\frac{n(C - D) + 2D - C}{q} \right], \\
v_{C,D}(n) &= \left[\frac{n(C - D) + 2D - C}{q} \right].
\end{aligned}$$

If $n = qk + r$ where $0 \leq r < q$, then

$$\zeta_{P(K)}(0, \chi) = \frac{1}{12q^2} (B_\chi(r)k + A_\chi(r)),$$

where

$$\begin{aligned}
&A_\chi(r) \\
&= \sum_{C,D=0}^{q-1} [\chi(C^2 + D^2 + rCD)\{6C^2r + 12CD - 6qrC + (r+3)q^2 - 12Cq\} \\
&\quad - \chi(C^2 - (r-2)D^2 + (r-2)CD)\{3u_{C,D}(r)^2 + 3C^2 + (6r-12)(C-D)^2 \\
&\quad - 6qC + (-3qr + 6q - 12qv_{C,D}(r))(C-D) + q^2(3 + 9v_{C,D}(r) - r)\}]
\end{aligned}$$

$$\begin{aligned}
 &+ \sum_{\substack{C,D=0 \\ C < D}}^{q-1} \chi(C^2 - (r-2)D^2 + (r-2)CD)v_{C,D}(r)12q^2 \\
 &+ \sum_{D=0}^{q-1} \chi(D^2)(2D - q)6q,
 \end{aligned}$$

and

$$\begin{aligned}
 &B_\chi(r) \\
 &= \sum_{C,D=0}^{q-1} [\chi(C^2 + D^2 + rCD)(6C^2q - 6Cq^2 + q^3) \\
 &\quad - \chi(C^2 - (r-2)D^2 + (r-2)CD)\{-6q(C-D)^2 + 6q^2(C-D) - q^3\}] \\
 &\quad + \sum_{\substack{C,D=0 \\ C < D}}^{q-1} \chi(C^2 - (r-2)D^2 + (r-2)CD)(C-D)12q^2.
 \end{aligned}$$

Proof. We know that if $n = qk + r$ where $0 \leq r < q$, then

$$\begin{aligned}
 &u_{C,D}(qk + r) = u_{C,D}(r), \quad v_{C,D}(qk + r) = (C - D)k + v_{C,D}(r), \\
 &\chi(C^2 - (n-2)D^2 + (n-2)CD) = \chi(C^2 - (r-2)D^2 + (r-2)CD), \\
 &\chi(C^2 + D^2 + nCD) = \chi(C^2 + D^2 + rCD).
 \end{aligned}$$

Thus the lemma follows immediately from the computation of $\zeta_{P(K)}(0, \chi)$ in (6). ■

3. Proof of Theorem 1.3. Let $d = n^2 - 4$ be a positive square free integer with $n \geq 5$ and $K = \mathbb{Q}(\sqrt{d})$. Let $q > 2$ be an integer with $(q, d) = 1$, χ an odd primitive character with conductor q , $\chi_d(\cdot) = \left(\frac{d}{\cdot}\right)$ the usual Kronecker character and L_χ the field generated over \mathbb{Q} by the values $\chi(a)$ ($1 \leq a \leq q$). We assume that $h(d) = 1$. Then

$$\zeta_K(0, \chi) = \zeta_{P(K)}(0, \chi)$$

where

$$\zeta_K(s, \chi) = \sum_{\substack{a \in I(K) \\ \text{integral}}} \frac{\chi(N(a))}{N(a)^s}.$$

We note the formula (2.2) in [1]:

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

Thus from Lemma 2.3, we have

$$\frac{1}{12q^2} (B_\chi(r)k + A_\chi(r)) = \frac{1}{q^2d} \sum_{a=1}^q a\chi(a) \sum_{b=1}^{qd} b\chi(b)\chi_d(b),$$

where $n = qk + r$, $0 \leq r < q$. Let

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

Since we know from Fact A in [1] that $\frac{1}{qd} \sum_{b=1}^{qd} b\chi(b)\chi_d(b)$ is an algebraic integer,

$$B_\chi(r)k + A_\chi(r) \equiv 0 \pmod{I},$$

where I is a prime ideal of L_χ for which $m_\chi \in I$. Let

$$U_m = \left\{ a \in \mathbb{Z} \mid \left(\frac{a^2 - 4}{t} \right) = -1 \text{ for every prime divisor } t \text{ of } m \right\},$$

and assume that the positive integers q and p satisfy the following condition:

- (*) The integer q is odd, p is an odd prime, and there is an odd primitive character χ with conductor q and a prime ideal I of L_χ lying over p such that $m_\chi \in I$, but I does not divide the ideal generated by $B_\chi(a)$ in the ring of integers of L_χ , if a is any rational integer with $a \in U_q$.

If the integers q and p satisfy condition (*), then for $r \in U_q$ we have

$$n \equiv -q \frac{A_\chi(r)}{B_\chi(r)} + r \pmod{I}.$$

And if the residue field of I is the prime field, then

$$R/I = \mathbb{Z}/p\mathbb{Z}.$$

So there is a unique $T(r) \in \{0, 1, \dots, p - 1\}$ such that

$$-q \frac{A_\chi(r)}{B_\chi(r)} + r + I = T(r) + I,$$

and

$$-q \frac{A_\chi(r)}{B_\chi(r)} + r \equiv T(r) \pmod{p}.$$

3.1. The computer program. In this section, we provide the computer program to compute $T(r)$ for each $r \in U_q$. Firstly we compute $\chi(r)$ modulo I . In the program, `chi[a_]` ($i = 1, 2, 3$) is the function computing $\chi_i(a)$ modulo I_i , where the character χ_i and the ideal I_i are defined in Example 1, Example 3 and Example 2 of Section 4 in [1] respectively for $i = 1, 2, 3$.

Next we compute $A_\chi(r)$ and $B_\chi(r)$ modulo I . Finally, we compute $T(r)$. In the program, $T1[r_]$ is the function computing $T_1(r)$ for which

$$-175 \frac{A_{\chi_1}(r)}{B_{\chi_1}(r)} + r + I_1 = T_1(r) + I_1,$$

$T2[r_]$ is the function computing $T_2(r)$ for which

$$-61 \frac{A_{\chi_2}(r)}{B_{\chi_2}(r)} + r + I_2 = T_2(r) + I_2,$$

$T3[r_]$ is the function computing $T_3(r)$ for which

$$-175 \frac{A_{\chi_3}(r)}{B_{\chi_3}(r)} + r + I_3 = T_3(r) + I_3.$$

The following is the MATHEMATICA program to compute $T(r)$ for each $r \in U_q$.

($f[x_ , y_]$ computes the logarithm of x to base 2 modulo y .)

```
f[x_, y_] := ( j = 0; m = Mod[x, y];
  If [Mod[x, y] == 0, Return[0]];
  While[ Mod[m, y] >1, m = Mod[m*2, y] ; j = j + 1];
  Return[y - 1 - j]);
```

($g[x_ , y_]$ computes the logarithm of x to base 3 modulo y .)

```
g[x_, y_] := ( j = 0; m = Mod[x, y];
  If[Mod[x, y] == 0, Return[0]];
  While[ Mod[m, y] >1, m = Mod[m*3, y]; j = j + 1];
  Return[y - 1 - j]);
```

```
g7[x_] := g[x, 7]; f25[x_] := ( j = 0; m = Mod[x, 25];
  If [ Mod[m, 5] == 0, Return[0]];
  While[Mod[m, 25] >1, m = Mod[m*2, 25]; j = j + 1];
  Return[20 - j]);
```

```
f61[x_] := f[x, 61];
```

($iv[x_ , y]$ computes the multiplicative inverse of x modulo y .)

```
iv[x_, y_] := (
  i = 1;
  While[Mod[ i*x, y] >1, i++];
  Return[i] );
```

($chi[a_]$ computes $\chi_i(a)$ modulo I_i .)

```
ch1[a_] := (If [Mod[a, 5] == 0 || Mod[a, 7] == 0, Return[0]];
  Return[Mod[PowerMod[8, f25[Mod[a, 25]], 61]*
  PowerMod[47, g7[Mod[a, 7] ], 61], 61]]);
ch2[a_] := (If[Mod[a, 61] == 0, Return[0]];
  Return[PowerMod[1833, f61[Mod[a, 61]], 1861]]);
ch3[a_] := (If [Mod[a, 5] == 0 || Mod[a, 7] == 0, Return[0]];
  Return[Mod[PowerMod[380, f25[Mod[a, 25]], 1861]*
  PowerMod[1406, g7[Mod[a, 7] ], 1861], 1861]]);
```

(The following is needed to compute $A_{\chi_i}(r)$ and $B_{\chi_i}(r)$ modulo I_i . We write down in detail only the case $i = 1$. The other two cases are computed similarly.)

$$u[x_, y_, a_, q_] := a (x - y) + 2 y - x - q \text{ Floor}[(a (x - y) + 2y-x)/q];$$

$$v[x_, y_, a_, q_] := \text{Floor}[(a (x - y) + 2 y - x)/q];$$

$$\begin{aligned} \text{ax11}[x_, y_, a_, q_] := & \\ & \text{Mod}[-\text{ch1}[x^2 - (a - 2)y^2 + (a - 2)x y] * \\ & (3 u[x, y, a, q]^2 + 3 x^2 + 6 a (x - y)^2 - 12 (x - y)^2 \\ & - 6 q x - 3 q a (x - y) + 6 q(x - y) - 12 q v[x, y, a, q] (x - y) \\ & + 3 q^2 + 9 v[x, y, a, q] q^2 - a q^2) \\ & + \text{ch1}[x^2 + y^2 + a x y] * \\ & (6 x^2 a - 6 x q a + q^2 *(a + 3) + 12 x y - 12 x q), 61]; \end{aligned}$$

$$\text{ax12}[x_, q_] := \text{Mod}[\text{ch1}[x^2]*(2 x - q)*6*q, 61];$$

$$\begin{aligned} \text{ax13}[x_, y_, a_, q_] := & \text{Mod}[\text{ch1}[x^2 - (a - 2)y^2 + (a - 2) x y] * \\ & 12*q^2*v[x, y, a, q], 61]; \end{aligned}$$

$$\begin{aligned} \text{bx11}[x_, y_, a_, q_] := & \\ & \text{Mod}[\text{ch1}[x^2 + y^2 + a x y] * \\ & (6 x^2 q - 6 q^2 x + q^3) \\ & - \text{ch1}[x^2 - (a - 2)y^2 + (a - 2)x y] * \\ & (-6 q (x - y)^2 + 6 q^2 *(x - y) - q^3), 61]; \end{aligned}$$

$$\begin{aligned} \text{bx12}[x_, y_, a_, q_] := & \\ & \text{Mod}[\text{ch1}[x^2 - (a - 2)y^2 + (a - 2)x y]*12*q^2*(x - y), 61]; \end{aligned}$$

($\text{Ax1}[a_, q_]$ and $\text{Bx1}[a_, q_]$) compute $A_{\chi_i}(r)$ and $B_{\chi_i}(r)$ modulo I_i respectively, where q is the conductor for the character χ_i for $i = 1, 2, 3$. We write down only the case $i = 1$.)

$$\begin{aligned} \text{Ax1}[a_, q_] := & \\ & \text{Sum}[\text{Sum}[\text{ax11}[x, y, a, q], \{x, 0, q - 1\}], \{y, 0, q - 1\}] \\ & + \text{Sum}[\text{Sum}[\text{ax13}[x, y, a, q], \{y, x + 1, q - 1\}], \{x, 0, q - 2\}] \\ & + \text{Sum}[\text{ax12}[x, q], \{x, 0, q - 1\}]; \\ \text{Bx1}[a_, q_] := & \\ & \text{Sum}[\text{Sum}[\text{bx11}[x, y, a, q], \{x, 0, q - 1\}], \{y, 0, q - 1\}] \\ & + \text{Sum}[\text{Sum}[\text{bx12}[x, y, a, q], \{y, x + 1, q - 1\}], \{x, 0, q - 2\}]; \end{aligned}$$

($\text{Ti}[a_]$ ($i = 1, 2, 3$) are the functions defined at the beginning of this section.)

$$\begin{aligned} \text{T1}[a_] := & \text{Mod}[-\text{Ax1}[a, 175]*175*iv[\text{Bx1}[a, 175], 61] + a, 61]; \\ \text{T2}[a_] := & \text{Mod}[-\text{Ax2}[a, 61]*61*iv[\text{Bx2}[a, 61], 1861] + a, 1861]; \\ \text{T3}[a_] := & \text{Mod}[-\text{Ax3}[a, 175]*175*iv[\text{Bx3}[a, 175], 1861] + a, 1861]; \end{aligned}$$

3.2. The result of computation. We denote by $q \rightarrow p$ that q, p satisfy condition (*). From Section 4 in [1], since our computation shows that I does not divide $(B_{\chi}(a))$ in each case for every $a \in U(q)$, we can find that

$$175 \rightarrow 61, \quad 61 \rightarrow 1861, \quad 175 \rightarrow 1861.$$

Let a_{175} be a residue modulo 175 for which $a_{175} \in U_{175}$, and b_{61} the residue modulo 61 for which

$$b_{61} = T_1(a_{175})$$

and $b_{61} \in U_{61}$. By the computation in Section 3.1, we obtain

$$\{(a_{175}, b_{61})\} = \{(14, 48), (21, 21), (39, 45), (46, 15), (56, 36), (81, 55), \\ (84, 38), (91, 23), (94, 6), (119, 25), (129, 46), (136, 16), (154, 40), (161, 13)\}.$$

For a b_{61} , let c_{1861} be the residue modulo 1861 for which

$$c_{1861} = T_2(b_{61})$$

and $c_{1861} \in U_{1861}$. Then we obtain

$$\{(b_{61}, c_{1861})\} = \{(48, 163), (45, 1176), (36, 1164), (55, 1855), (38, 1726), \\ (23, 135), (6, 6), (25, 697), (16, 685), (13, 1698)\}.$$

For an a_{175} such that the corresponding b_{61} appears in the above $\{(b_{61}, c_{1861})\}$, let d_{1861} be the residue modulo 1861 for which

$$d_{1861} = T_3(a_{175})$$

and $d_{1861} \in U_{1861}$. Then we obtain

$$\{(a_{175}, d_{1861})\} = \{(14, 1702), (39, 874), (56, 894), (81, 176), (84, 309), \\ (91, 1552), (94, 1685), (119, 967), (136, 987), (161, 159)\}.$$

But $c_{1861} \neq d_{1861}$ for all c_{1861}, d_{1861} . Thus if $h(d) = 1$, then $(\frac{d}{q}) = 0$ or 1 for at least one of $q = 5, 7, 61, 1861$. This completes the proof of Theorem 1.3.

Acknowledgements. The authors thank the referee for many valuable suggestions.

References

- [1] A. Biró, *Yokoi's conjecture*, Acta Arith. 106 (2003), 85–104.
- [2] —, *Chowla's conjecture*, ibid. 107 (2003), 179–194.
- [3] S. Chowla and J. Friedlander, *Class numbers and quadratic residues*, Glasgow Math. J. 17 (1976), 47–52.
- [4] G. Janusz, *Algebraic Number Fields*, Grad. Stud. Math. 7, Amer. Math. Soc., 1996.
- [5] R. A. Mollin, *Class number one criteria for real quadratic fields. I*, Proc. Japan Acad. 63 (1987), 121–125.
- [6] —, *Class number one criteria for real quadratic fields. II*, ibid. 63 (1987), 162–164.
- [7] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo 63 (1976), 393–417.
- [8] —, *On special values of zeta functions of totally real algebraic number fields*, in: Proc. Internat. Congress of Math., Helsinki, 1978, 591–597.

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

Department of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail: dhbyeon@math.snu.ac.kr

*Received on 30.5.2005
and in revised form on 3.10.2006*

(4994)