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 $r|4n$ and $-n < r \leq n$. Then we call $K = \mathbb{Q}(\sqrt{d})$ a real quadratic field of Richaud-Degert type. Specially if $|r| \in \{1, 4\}$, then $K = \mathbb{Q}(\sqrt{d})$ is called a narrow-Richaud-Degert type.*

Chowla and Yokoi conjectures are ones involving 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 complete 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 $h(d) > 1$.*

Basically we follow Biró's idea to prove Theorem 1.2. First we prove the following theorem.

---

*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.

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

Then Theorem 1.2 immediately follows from Theorem 1.3 and 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 $(\frac{d}{q}) = -1$ for all primes $q < n - 2$*

and class number table for real quadratic fields of narrow-Richaud-Degert type. A new ingredient in this paper is developing skill of computation of $\zeta_{P(K)}(0, \chi)$ (See section 2 for definition), where K is a quadratic field whose fundamental unit's norm is positive. We note that norms of fundamental units of real quadratic fields in Chowla or Yokoi conjectures are negative.

Remark. Using the skill 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 in Richaud-Degert type (see [6]), for example, the type of $d = n^2 \pm 2$, are different from those in narrow-Richaud-Degert type. So we can not 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 $\epsilon = \frac{n+\sqrt{n^2-4}}{2}$ the fundamental unit of K. We know that $\{1, \epsilon\}$ 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 $N(\alpha) = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\alpha)$. We note that the norm of ϵ, $N(\epsilon) = 1$. 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 $i : K^* \to I(K)$ by $\alpha(\neq 0) \to (\alpha)$. 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 the pages 242 - 243 in [4]. □

Lemma 2.2 *A given principal ideal (α) in $i(K^+)$ can be written in unique way of the following form;*

$$(\alpha) = (X + Y\epsilon),$$

with some rational numbers $X > 0$, $Y \geq 0$, and if X and Y are a rational number with $X > 0$, $Y \geq 0$, then

$$(X + Y\epsilon) \in i(K^+).$$

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

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

So

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

Thus $X > 0$ and $Y \geq 0$. And if X and Y are a rational number with $X > 0$, $Y \geq 0$, then $X + Y\epsilon > 0$ and $X + Y\bar{\epsilon} > 0$, since ϵ and $\bar{\epsilon}$ are greater than 0. So

$$(X + Y\epsilon) \in i(K^+).$$

□

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

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

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

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

So

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

We shall denote the first part by $\zeta^+(s)$ and the second part by $\zeta^-(s)$.

First we compute $\zeta^+(0)$. By Lemma 2.2, if $a \in (q)i(K^+)$, then $a = q(X+Y\epsilon)$ 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

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

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

Since $C + D\epsilon$ 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 $q(x+y\epsilon) \in C + D\epsilon + qR$. Let $R^1(C,D) = \{(x,y) \in R^1 \,|\, q(x+y\epsilon) \in C + D\epsilon + qR\}$. From the work of Shintani [7] [8],

$$\begin{aligned}
\zeta^+(0) &= \sum_{C,D=0}^{q-1} \chi(N(C+D\epsilon)) \sum_{(x,y)\in R^1(C,D)} \sum_{n_1,n_2=0}^{\infty} \frac{1}{N(q(x+n_1+\epsilon(y+n_2)))^s}\Big|_{s=0} \\
&= \sum_{C,D=0}^{q-1} \chi(C^2+D^2+nCD) \sum_{(x,y)\in R^1(C,D)} \zeta(0, \begin{pmatrix} 1 & \epsilon \\ 1 & \bar{\epsilon} \end{pmatrix}, (x,y)) \\
&= \sum_{C,D=0}^{q-1} \Big[\chi(C^2+D^2+nCD) \\
&\quad \cdot \sum_{(x,y)\in R^1(C,D)} \Big\{(x-\frac{1}{2})(y-\frac{1}{2}) + \frac{n}{4}(x^2+y^2-(x+y)+\frac{1}{3})\Big\}\Big].
\end{aligned}$$

We note that

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

Replacing x, y with the above we have

$$\begin{aligned}
& \zeta^{+}(0) \\
= & \sum_{\substack{C=0 \\ 0 \le D \le q-1}} \chi(C^2+D^2+nCD)\Big\{\frac{1}{2}(\frac{D}{q}-\frac{1}{2}) + \frac{n}{4}(1+\frac{D^2}{q^2} - (1+\frac{D}{q}) + \frac{1}{3})\Big\} \\
+ & \sum_{\substack{0 < C \le q-1 \\ 0 \le D \le q-1}} \Big[\chi(C^2+D^2+nCD) \\
\cdot & \Big\{(\frac{C}{q}-\frac{1}{2})(\frac{D}{q}-\frac{1}{2}) + \frac{n}{4}(\frac{C^2}{q^2}+\frac{D^2}{q^2} - (\frac{C+D}{q}) + \frac{1}{3})\Big\}\Big] \\
= & \sum_{C,D=0}^{q-1} \Big[\chi(C^2+D^2+nCD) \\
\cdot & \Big\{(\frac{C}{q}-\frac{1}{2})(\frac{D}{q}-\frac{1}{2}) + \frac{n}{4}(\frac{C^2}{q^2}+\frac{D^2}{q^2} - (\frac{C+D}{q}) + \frac{1}{3})\Big\}\Big] \\
+ & \sum_{D=0}^{q-1} \chi(D^2)(\frac{D}{q}-\frac{1}{2}) \\
= & \frac{1}{12q^2}\sum_{C,D=0}^{q-1} \chi(C^2+D^2+nCD)(6C^2n + 12CD - 6qnC - 12Cq + (n+3)q^2) \\
+ & \frac{1}{12q^2}\sum_{D=0}^{q-1} \chi(D^2)(2D-q)6q.
\end{aligned}$$

Now we compute $\zeta^{-}(0)$. Let $R^2 = \{(x,y) \in \mathbb{Q}^2 \,|\, \omega(qx+qy)\epsilon \in R,\ 0 < x \le 1,\ 0 \le y < 1\}$. Since $C + D\omega$ with integers $0 \le C, D \le q-1$ form a complete system of representatives of R/qR, we can uniquely select an integer pair $0 \le C, D \le q-1$ such that $\omega(qx+qy\epsilon) \in C + D\omega + qR$. Let $R^2(C,D) = \{(x,y) \in R^2 \,|\, \omega(qx+qy\epsilon) \in C + D\omega + qR\}$. Then

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

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

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

We note that

$$
\begin{aligned}
& (x,y) \in R^2(C,D) \\
\Longleftrightarrow\ & q\omega(x+y\epsilon) = C + D\omega + q(i+j\omega) \ \text{ for } i,j \text{ integers and } (x,y)\in R^2 \\
\Longleftrightarrow\ & (n-2)q(x+y\epsilon) = -(n-1)(C+iq) + (n-2)(D+jq) + \epsilon(C+iq) \\
& \text{for } i,j \text{ integers and } (x,y)\in R^2 \\
\Longleftrightarrow\ & 0 < x = \frac{-(n-1)(C+iq)+(n-2)(D+jq)}{(n-2)q} \le 1
\end{aligned}
$$

$$0 \le y = \frac{C+iq}{(n-2)q} < 1 \text{ for } i = 0, 1, \cdots, n-3 \text{ integers and}$$
$$j = \Big[1 + \frac{(C+iq)(n-1)}{q(n-2)} - \frac{D}{q}\Big].$$

Thus

$$\begin{aligned}
x &= \frac{-(C+iq)(n-1)}{(n-2)q} + \frac{D}{q} + \Big[1 + \frac{(C+iq)(n-1)}{q(n-2)} - \frac{D}{q}\Big] \\
&= \Big[i + \frac{C-D}{q} + \frac{C+iq}{q(n-2)}\Big] - (i + \frac{C-D}{q} + \frac{C+iq}{q(n-2)}) + 1 \\
&= \Big[i + [\frac{C-D}{q}] + \frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}\Big] - (i + [\frac{C-D}{q}] + \frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}) + 1 \\
&= \Big[\frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}\Big] - (\frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}) + 1 \text{ for } i = 0, 1, \cdots, n-3 \text{ integers,}
\end{aligned}$$

where $r(C,D) = C - D - q[\frac{C-D}{q}]$. Since

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

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

Let $s(C,D) = [\frac{(n-2)r(C,D)+C}{q}]$. Then $(x,y) \in R^2(C,D)$ if and only if

$$\begin{aligned}
x &= \begin{cases} -(\frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}) + 1 & \text{if } 0 \le i < n-2-s(C,D) \\ -(\frac{r(C,D)}{q} + \frac{C+iq}{q(n-2)}) + 2 & \text{if } n-2-s(C,D) \le i < n-2. \end{cases} \\
y &= \frac{C+iq}{(n-2)q} \quad \text{for } 0 \le i < n-2.
\end{aligned}$$

Replacing x, y with 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

$$
\begin{aligned}
& S(C,D) \\
= & \sum_{i=0}^{n-3-s(C,D)} \Big\{ -\frac{C+iq}{2q}(-\frac{r(C,D)}{q} - \frac{C+iq}{(n-2)q} + 1) \\
& -\frac{n+2}{4}(1-\frac{r(C,D)}{q}) + \frac{n}{4}(1-\frac{r(C,D)}{q})^2 + \frac{n+3}{12}\Big\} \\
& + \sum_{i=n-2-s(C,D)}^{n-3} \Big\{ -\frac{C+iq}{2q}(-\frac{r(C,D)}{q} - \frac{C+iq}{(n-2)q} + 2) \\
& -\frac{n+2}{4}(2-\frac{r(C,D)}{q}) + \frac{n}{4}(2-\frac{r(C,D)}{q})^2 + \frac{n+3}{12}\Big\} \\
& \text{(by using MATHEMATICA)} \\
= & \frac{1}{12q^2}(-6Cq - 6Cqs(C,D) + 6C^2 - q^2n - 12Cr(C,D) + 3q^2 + 6Cr(C,D)n \\
& +6r(C,D)q - 3r(C,D)qn + 9q^2s(C,D) + 3q^2s(C,D)^2 - 6r(C,D)qs(C,D)n \\
& -6nr(C,D)^2 + 3n^2r(C,D)^2) \\
= & \frac{1}{12q^2}\Big\{3\Big((n-2)r(C,D) + C - s(C,D)q\Big)^2 + 3C^2 \\
& +(3-n)q^2 - 6Cq + 9q^2s(C,D) - 12r(C,D)qs(C,D) \\
& +6nr(C,D)^2 - 12r(C,D)^2 + 6r(C,D)q - 3r(C,D)qn\Big\}.
\end{aligned}
$$

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;

$$
\begin{aligned}
(1) \qquad & \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n))r(C,D) \\
= & \sum_{\substack{C,D=0 \\ C<D}}^{q-1} \chi(Q_{C,D}(n))q + \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n))(C-D),
\end{aligned}
$$

$$(2)\quad \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n)) r(C,D)^2$$

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

$$(3)\quad \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n)) s(C,D) r(C,D)$$

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

$$+ \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n))(C-D) v_{C,D}(n),$$

$$(4)\quad \sum_{C,D=0}^{q-1} \chi(Q_{C,D}(n)) s(C,D)$$

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

where

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

And

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

$$\begin{aligned} &= (n-2)(C-D) + C - q(n-2)\Big[\frac{C-D}{q}\Big] - q\Big[\frac{(n-2)(C-D) + C - q(n-2)\big[\frac{C-D}{q}\big]}{q}\Big] \\ &= (n-2)(C-D) + C - q\Big[\frac{(n-2)(C-D)+C}{q}\Big] \\ &= u_{C.D}(n) \end{aligned}$$

By the equations (1) - (5), we have the following value of $\zeta^-(0)$.

$$\begin{aligned}
& \zeta^-(0) \\
= & -\frac{1}{12q^2}\sum_{C,D=0}^{q-1}\Big[\chi(C^2-(n-2)D^2+(n-2)CD) \\
\cdot & \Big\{3u_{C.D}(n)^2+3C^2+6n(C-D)^2-12(C-D)^2-6Cq-12qv_{C,D}(n)(C-D) \\
- & 3nq(C-D)+6q(C-D)+q^2(3+9v_{C,D}(n)-n)\Big\}\Big] \\
- & \frac{1}{12q^2}\sum_{\substack{C,\,D\,=\,0\\ C\,<\,D}}^{q-1}\Big[\chi(C^2-(n-2)D^2+(n-2)CD) \\
\cdot & \Big\{(6n-12)(q^2+2q(C-D))-12q((q+C-D)(n-2)+qv_{C,D}(n)) \\
+ & (6q-3qn)q+9q^2(n-2)\Big\}\Big] \\
= & -\frac{1}{12q^2}\sum_{C,D=0}^{q-1}\Big[\chi(C^2-(n-2)D^2+(n-2)CD) \\
\cdot & \Big\{3u_{C.D}(n)^2+3C^2+6n(C-D)^2-12(C-D)^2-6Cq-12qv_{C,D}(n)(C-D) \\
- & 3nq(C-D)+6q(C-D)+q^2(3+9v_{C,D}(n)-n)\Big\}\Big] \\
- & \frac{1}{12q^2}\sum_{\substack{C,\,D\,=\,0\\ C\,<\,D}}^{q-1}\chi(C^2-(n-2)D^2+(n-2)CD)(-v_{C,D}(n)12q^2).
\end{aligned}$$

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

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

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

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

Finally we can have 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 is an odd character with conductor q. Let*

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

Then if $n = qk+r$ where $0 \le r < q$,

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

where

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

and

$$\begin{aligned} & B_\chi(r) \\ = & \sum_{C,D=0}^{q-1} \Big[\chi(C^2+D^2+rCD)(6C^2q-6Cq^2+q^3) \end{aligned}$$

$$- \quad \chi(C^2-(r-2)D^2+(r-2)CD)\Big\{-6q(C-D)^2+6q^2(C-D)-q^3\Big\}\Big]$$
$$- \quad \sum_{\substack{C,\,D\,=\,0\\ C\,<\,D}}^{q-1} \chi(C^2-(r-2)D^2+(r-2)CD)(C-D)12q^2.$$

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

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

Thus the lemma immediately follows from the above 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 $n \ge 5$ and $K = \mathbb{Q}(\sqrt{d})$. Let $q > 2$ be an integer with $(q,d) = 1$, χ an odd primitive character with conductor q, $\chi_d(\cdot) = (\frac{d}{\cdot})$ the usual Kronecker character and L_χ the field generated over $\mathbb{Q}$ by the values $\chi(a)$ $(1 \le a \le q)$. We assume that $h(d) = 1$. Then

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

where

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

We note the formula (2.2) in [1]

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

Thus from Lemma 2.3, we have

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

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

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

Since we know form the 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

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

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

Condition(*). *The integer q is odd, p is an odd prime, and there is an odd prime 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 the 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 $T(r) \in \{0, 1, \cdots, p-1\}$ 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 4 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 with 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 with 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 followings are needed to compute $A_{\chi_i}(r)$ and $B_{\chi_i}(r)$ modulo I_i.)

```
u[x_, y_, a_,q_] := a (x - y) + 2 y - x - q  Floor[(a (x - y) +
2y-x)/q];

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

ax11[x_, y_, a_, q_] :=
    Mod[-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)
  + 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];

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

ax13[x_, y_, a_, q_] := Mod[ch1[x^2 - (a - 2)y^2 + (a - 2) x y]*
                    12*q^2*v[x, y, a, q], 61];
```

```
bx11[x_, y_,  a_, q_] :=
       Mod[ch1[x^2 + y^2 + a x y] *
         (6 x^2 q - 6 q^2 x + q^3)
       - ch1[x^2 - (a - 2)y^2 + (a - 2)x y]*
         (-6 q (x - y)^2 + 6 q^2 *( x - y) - q^3), 61];

bx12[x_, y_, a_, q_] :=
       Mod[ch1[x^2 - (a - 2)y^2 + (a - 2)x y]*
                 12*q^2*(x - y), 61];

ax21[x_, y_, a_, q_] :=
    Mod[-ch2[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)
  + ch2[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 ), 1861];

ax22[x_, q_] := Mod[ch2[x^2]*(2 x - q)*6*q, 1861];

ax23[x_, y_, a_, q_] :=
        Mod[ch2[x^2 - (a - 2)y^2 + (a - 2) x y]*
                    12*q^2*v[x, y, a, q],1861];

bx21[x_, y_,  a_, q_] :=
       Mod[ch2[x^2 + y^2 + a x y] *
         (6 x^2 q - 6 q^2 x + q^3)
       - ch2[x^2 - (a - 2)y^2 + (a - 2)x y]*
         (-6 q (x - y)^2 + 6 q^2 *( x - y) - q^3),1861];

bx22[x_, y_, a_, q_] :=
       Mod[ch2[x^2 - (a - 2)y^2 + (a - 2)x y]*
                 12*q^2*(x - y), 1861];

ax31[x_, y_, a_, q_] :=
    Mod[-ch3[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)
```

```
  + ch3[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 ), 1861];

ax32[x_, q_] := Mod[ch3[x^2]*(2 x - q)*6*q, 1861];

ax33[x_, y_, a_, q_] :=
        Mod[ch3[x^2 - (a - 2)y^2 + (a - 2) x y]*
                    12*q^2*v[x, y, a, q],1861];

bx31[x_, y_,  a_, q_] :=
       Mod[ch3[x^2 + y^2 + a x y] *
         (6 x^2 q - 6 q^2 x + q^3)
       - ch3[x^2 - (a - 2)y^2 + (a - 2)x y]*
         (-6 q (x - y)^2 + 6 q^2 *( x - y) - q^3),1861];

bx32[x_, y_, a_, q_] :=
       Mod[ch3[x^2 - (a - 2)y^2 + (a - 2)x y]*
                 12*q^2*(x - y), 1861];
```

(`Axi[a_,q_]` and `Bxi[a_,q_]`) computes $A_{\chi_i}(r)$ and $B_{\chi_i}(r)$ modulo I_i respectively, where `q` is the conductor for the character χ_i for $i = 1, 2, 3$.)

```
Ax1[a_, q_] :=
    Sum[Sum[ax11[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
  + Sum[Sum[ax13[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}]
  + Sum[ax12[x, q], {x, 0, q - 1}];
Bx1[a_, q_] :=
    Sum[Sum[bx11[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
  + Sum[ Sum[bx12[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}];
Ax2[a_, q_] :=
    Sum[Sum[ax21[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
  + Sum[Sum[ax23[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}]
  + Sum[ax22[x,q], {x, 0, q - 1}];
Bx2[a_, q_] :=
    Sum[Sum[bx21[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
 + Sum[Sum[bx22[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}];
Ax3[a_, q_] :=
   Sum[Sum[ax31[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
+ Sum[Sum[ax33[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}] +
Sum[ax32[x, q], {x, 0, q - 1}];
```

```
 Bx3[a_, q_] :=
  Sum[Sum[bx31[x, y, a, q], {x, 0, q - 1}], {y, 0, q - 1}]
+ Sum[Sum[bx32[x, y, a, q], {y, x + 1, q - 1}], {x, 0, q - 2}];
```

(`Ti[a_]`($i = 1, 2, 3$) are previously defined functions at the beginning of this section.)

```
T1[a_] :=
  Mod[-Ax1[a, 175]*175*iv[Bx1[a, 175], 61] + a, 61];
T2[a_] :=
  Mod[-Ax2[a, 61]*61*iv[Bx2[a, 61], 1861] + a, 1861];
T3[a_] :=
  Mod[-Ax3[a, 175]*175*iv[Bx3[a, 175], 1861] + a, 1861];
```

3.2 The result of the computer work

We denote by $q \to p$ that q, p satisfy Condition(*). From the Section 4 in [1], we can find that

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

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

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

and $b_{61} \in U_{61}$. By the computer work in section 3.1, we can 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 can 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 can 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] A. Biró, *Chowla's conjecture,* Acta Arith. **107** (2003), 179–194.

[3] S. Chowla and J. Friedlandler, *Class numbers and quadratic residues,* Glasgow Math. J. **17** (1976), 47–52.

[4] G. Janusz, *Algebraic number fields,* Amer. Math. Soc., Graduate Studies in Math. **7** (1996).

[5] R. A. Mollin, *Class number one criteria for real quadratic fields. I,* Proc. Japan Acad. **63** (1987), 121–125.

[6] R. A. Mollin, *Class number one criteria for real quadratic fields. II,* Proc. Japan Acad. **63** (1987), 162–164.

[7] T. Shintani, *On evaualation of zeta funtions of totally real algebraic number fields at non-positive integers,* J. Fac. Sci. Univ. Tokyo. **63** (1976), 393–417.

[8] T. Shintani, *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