On a certain invariant for real quadratic fields

By Seok-Min Lee and Takashi Ono

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland, 21218-2689, U. S. A.

(Communicated by Shokichi Iyanaga, M. J. A., Oct. 14, 2003)

Abstract: Let $K = \mathbf{Q}(\sqrt{m})$ be a real quadratic field, $\mathcal{O}_K$ its ring of integers and $G = \mathrm{Gal}(K/\mathbf{Q})$. For $\gamma \in H^1(G, \mathcal{O}_K^\times)$, we associate a module M_c/P_c for $\gamma = [c]$. It is known that $M_c/P_c \approx \mathbf{Z}/\Delta_m\mathbf{Z}$ where $\Delta_m = 1$ or 2 and we will determine Δ_m.

Key words: Real quadratic field; fundamental unit; parity; continued fractions.

1. Introduction. This is a continuation and completion of [1]. Let m be a square free positive integer, $K = \mathbf{Q}(\sqrt{m})$ the corresponding real quadratic field, $\mathcal{O}_K$ the ring of integers of K, $\mathcal{O}_K^\times$ the group of units of K and $G = \mathrm{Gal}(K/\mathbf{Q}) = \langle s \rangle$. To each $\gamma = [c] \in H^1(G, \mathcal{O}_K^\times)$, T. Ono [1] associated a module M_c/P_c where

$$M_c = \{\alpha \in \mathcal{O}_K; c^{\,s}\alpha = \alpha\},$$

$$P_c = \{p_c(z) = z + c^{\,s}z,\ z \in \mathcal{O}_K\}.$$

The module M_c/P_c is of order 1 or 2 and depends only on the cohomology class $\gamma = [c]$. Actually the case $c = \varepsilon$, the fundamental unit of K, with $N\varepsilon = 1$, is essential and he put

$$\Delta_m = [M_\varepsilon : P_\varepsilon].$$

So the problem is to determine $\Delta_m = 1$ or 2 in terms of m. On the basis of Lee's computation for $m < 1000$, Ono conjectured that

(I) $m \equiv 1 \pmod 4 \Rightarrow \Delta_m = 1$,
(II) $m \equiv 2 \pmod 4 \Rightarrow \Delta_m = 2$,
(III) $m \equiv 3 \pmod 4$;

$$a_s \equiv 1 \pmod 2 \Rightarrow \Delta_m = 1$$
$$a_s \equiv 0 \pmod 2 \Rightarrow \Delta_m = 2$$

where $\sqrt{m} = [a_0; \overline{a_1, \dots, a_{s-1}, a_s, a_{s-1}, \dots, a_1, 2a_0}]$, the standard continued fraction expansion.

In this paper, we shall prove that (I), (II), (III) are all true (Theorem 9, Theorem 10, Theorem 13).

2. Notation. Let $K = \mathbf{Q}(\sqrt{m})$, $m > 0$, square free. Let $\{1, \omega\}$ be the standard basis of $\mathcal{O}_K$;

$$\omega = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod 4, \\ \dfrac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4. \end{cases}$$

We write the fundamental unit ε as $\varepsilon = u + v\omega$, $u, v \in \mathbf{Z}$. Note that $(u, v) = 1$. Following [1], we put

$$d = (v, u-1), \quad e = (v, u+1),$$
$$D = v/e.$$

In [1], we find $[M_\varepsilon : P_\varepsilon] =$

$$\Delta_m = \frac{d}{(D, d)}. \tag{1}$$

Proposition 1. $\Delta_m = 1 \Leftrightarrow de \mid v$.

Proof. $d/(D, d) = 1 \Leftrightarrow d = (D, d) \Leftrightarrow d \mid D \Leftrightarrow d \mid (v/e) \Leftrightarrow de \mid v$. □

3. Proof of (I), (II).

Proposition 2. *If v is odd, then $\Delta_m = 1$.*

Proof. Note that $(v, u-1)$ and $(v, u+1)$ are odd divisors of v but $(u+1, u-1) \mid 2$. Then $(v, u-1)$ and $(v, u+1)$ are mutually prime divisors of v. Hence we get $(v, u-1)(v, u+1) \mid v$. □

When v is even (then u is odd), let $v' = v/2$ and $u' = (u-1)/2$. Then

$$d = (v, u-1) = (2v', 2u') = 2(v', u') = 2d'$$

with $d' = (u', v')$ and

$$e = (v, u+1) = (2v', 2u'+2) = 2(v', u'+1) = 2e'$$

with $e' = (v', u'+1)$. Note that d' and e' are mutually prime divisors of v'. Hence we have

$$d'e' = (v', u')(v', u'+1) \mid v', \tag{2}$$

that is,

$$d' \,\Big|\, \frac{v'}{e'} = \frac{2v'}{2e'} = \frac{v}{e} = D. \tag{3}$$

2000 Mathematics Subject Classification. Primary 11R11, 11A55; Secondary 11A07.

We have two cases;

(i) $2d'e' \mid v'$: we have $de = 4d'e' \mid 2v' = v$ so $\Delta_m = 1$ by Proposition 1.

(ii) $2d'e' \nmid v'$: we have $de \nmid v$ and $d \nmid (v/e) = D$. Since $d' \mid D$, $(D,d) = (D, 2d') = d'$ and hence $\Delta_m = d/(D,d) = (d/d') = 2$.

Therefore we have proved $\Delta_m = 1$ or 2 for any m and;

Proposition 3. *If v is even, using the notations above,*

$$2d'e' \mid v' \Leftrightarrow \Delta_m = 1,$$

or equivalently,

$$2d'e' \nmid v' \Leftrightarrow \Delta_m = 2.$$

Proposition 4. *If v is even (and u is odd), let $\nu \geq 1$ be such that*

$$2^\nu \| v$$

i.e. the largest positive integer such that $2^\nu \mid v$. Then

$$u \equiv \pm 1 \pmod{2^\nu} \Leftrightarrow \Delta_m = 2.$$

Proof.

(Case 1) $\nu = 1$: $v \equiv 2 \pmod 4$ so v' is odd, and $2d'e' \nmid v'$. Hence $\Delta_m = 2$ by Proposition 2. On the other hand, u is odd so $u \equiv \pm 1 \pmod 2$.

(Case 2) $\nu \geq 2$: $2^\nu \| v$ then $2^{\nu-1} \| v' = (v/2)$. Since $u' = (u-1)/2$, note that $u \equiv \pm 1 \pmod{2}^\nu \Leftrightarrow$ one of $u+1$, $u-1 \equiv 0 \pmod{2}^\nu \Leftrightarrow$ one of u', $u'+1 \equiv 0 \pmod{2}^{\nu-1}$.

($\Leftarrow$) If $u \not\equiv \pm 1 \pmod{2^\nu}$, neither u' nor $u'+1$ is congruent to $0 \pmod{2}^{\nu-1}$.
Since (v', u') and $(v', u'+1)$ are mutually prime, we have $2^{\nu-1} \nmid (v', u')(v', u'+1)$. But since $(v', u')(v', u'+1) \mid v'$ and $2^{\nu-1} \mid v'$, we have $2(v', u')(v', u'+1) \mid v'$ and thus $\Delta_m = 1$.

($\Rightarrow$) If $u \equiv \pm 1 \pmod{2^\nu}$, one of u', $u'+1 \equiv 0 \pmod{2}^{\nu-1}$. So $2^{\nu-1} \mid (v', u')(v', u'+1)$ and $2^\nu \mid 2(v', u')(v', u'+1)$. But $2^\nu \nmid v'$ so $2(v', u')(v', u'+1) \nmid v'$ and hence $\Delta_m = 2$. □

Proposition 5. *If v is even but $8 \nmid v$ then $\Delta_m = 2$.*

Proof. For $\nu = 2$ or 4 (resp.), odd u should be congruent to $\pm 1 \pmod 2$ or $\pmod 4$ (resp.). □

Lemma 6. *For $\nu \geq 3$,*

$$a^2 \equiv 1 \pmod{2}^\nu \Leftrightarrow a \equiv \pm 1 \pmod{2^\nu}$$
$$\text{or} \quad a \equiv \pm(2^{\nu-1} - 1) \pmod{2^\nu}.$$

Proof. First, $(\pm 1)^2 = 1$ and $(\pm(2^{\nu-1}-1))^2 = 2^{2\nu-2} - 2^\nu + 1 \equiv 1 \pmod{2}^\nu$ since $2\nu - 2 \geq \nu$ for $\nu \geq 3$. It is known that the unit group mod 2^ν is isomorphic to the direct product of two cyclic groups of order 2 and $2^{\nu-2}$

$$(\mathbf{Z}/2^\nu\mathbf{Z})^\times \simeq \langle -1 \rangle \times \langle 5 \rangle$$

where $(-1)^2 \equiv 1$ and $5^{2^{\nu-2}} \equiv 1 \pmod{2^\nu}$. Let $a \in (\mathbf{Z}/2^\nu\mathbf{Z})^\times$ such that $a^2 \equiv 1 \pmod{2^\nu}$ other than ± 1. We can write $a = (-1)^i 5^j$ with $i = 0$ or 1 and $1 \leq j < 2^{\nu-2}$.

$$\begin{aligned} a^2 \equiv 1 \pmod{2^\nu} &\Leftrightarrow 5^{2j} \equiv 1 \pmod{2^\nu} \\ &\Leftrightarrow 2^{\nu-2} \mid 2j \\ &\Leftrightarrow 2^{\nu-3} \mid j. \end{aligned}$$

Since $1 \leq j < 2^{\nu-2}$, $j = 2^{\nu-3}$. So we have only four elements ± 1, $\pm 5^{2^{\nu-3}}$, with square $\equiv 1 \pmod{2^\nu}$. □

Lemma 7. *If a, b are integers and b is even such that $a^2 - mb^2 = 1$ and $2^\nu || b$ where $\nu \geq 2$ then $a \equiv \pm 1 \pmod{2^{\nu+1}}$.*

Proof. First note that

$$2^\nu || b \Rightarrow a^2 \equiv 1 \pmod{2^{2\nu}}. \tag{4}$$

Then by the previous lemma, $a \equiv \pm 1$ or $\pm 2^{2\nu-1} - 1)$ $\pmod{2^{2\nu}}$. Since $\nu \geq 2$, $2\nu - 1 \geq \nu + 1$ so $\pm(2^{2\nu-1} - 1) \equiv \mp 1 \pmod{2^{\nu+1}}$. □

Proposition 8. *If $\varepsilon = u + v\sqrt{m}$ with v even, then $\Delta_m = 2$.*

Proof. If $8 \nmid v$ then $\Delta_m = 2$ by Proposition 5. If $2^\nu \| v$ with $\nu \geq 3$ then $u \equiv \pm 1 \pmod{2^\nu}$ by Lemma 7, hence $\Delta_m = 2$ by Proposition 4. □

Theorem 9. *If $m \equiv 2 \pmod 4$ then $\Delta_m = 2$. For $m \equiv 3 \pmod 4$, $\Delta_m = 1 \Leftrightarrow v$ is odd.*

Proof. If $m \equiv 2 \pmod 4$ then $1 = u^2 - mv^2 \equiv u^2 - 2v^2 \pmod 4$. Since all squares mod 4 are 0 and 1, only possibility is $v^2 \equiv 0$ and $u^2 \equiv 1$. So v is even. The rest follows from Proposition 2 and Propositon 8. □

Theorem 10. *If $m \equiv 1 \pmod 4$ then $\Delta_m = 1$.*

Proof. By Proposition 2, we may assume that v is even. Denote $\varepsilon = u + v\omega = a + b\sqrt{m}$ where $a = u + (v/2)$ and $b = v/2$. Then $1 = a^2 - mb^2 \equiv a^2 - b^2 \pmod 4$. Since $0, 1$ are all squares mod 4, only possible case is for $b^2 \equiv 0$ and $a^2 \equiv 1 \pmod 4$ and so a is odd and b is even. Now, consider the equation $a^2 - mb^2 \equiv 1 \pmod 8$. The only square mod 8 are 0, 1, and 4. Since a is odd, $a^2 \equiv 1 \pmod 8$. We have $b^2 \equiv 0$ or $4 \pmod 8$, and $m \equiv 1$ or $m \equiv 5 \pmod 8$. Only possible case is $b^2 \equiv 0 \pmod 8$. We get $b \equiv 0$

(mod 4) and so $8 \mid v$. Let $\nu \geq 3$ be the integer such that $2^\nu \| v$. Then $2^{\nu-1} \| b$, and we get $a \equiv \pm 1 \pmod{2^\nu}$ by Lemma 7. Since $2^\nu \nmid b$, $u = a - b \equiv \pm 1 - 2^{\nu-1} \not\equiv \pm 1 \pmod{2^\nu}$. Then by Proposition 4, we get $\Delta_m = 1$. □

4. Proof of (III). Now it remains to determine Δ_m for $m \equiv 3 \pmod 4$. In this section, we consider the continued fraction of $\sqrt{m} = [a_0; \overline{a_1, a_2, \ldots, a_r}]$. As for basic properties of continued fractions, see [2];

1. the period r is odd $\Leftrightarrow$ the equation $x^2 - my^2 = -1$ has an integer solution. Since $N(\varepsilon) = +1$ if $m \equiv 3 \pmod 4$, r is even.
2. $a_0 = [\sqrt{m}]$ (the integer part), $a_r = 2a_0$, and $a_i = a_{r-i}$ for $i = 1, \ldots, r-1$, so $\sqrt{m} = [a_0; \overline{a_1, \ldots, a_{s-1}, a_s, a_{s-1}, \ldots, a_1, 2a_0}]$ where $s = r/2$.
3. We can associate a finite continued fraction with a matrix product,
$$[a_0, a_1, \ldots, a_n] \leftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix},$$
or inductively,
$$p_{-1} = 1, \quad p_0 = a_0, \quad p_i = a_i p_{i-1} + p_{i-2},$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_i = a_i q_{i-1} + q_{i-2}.$$
Then
$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$
We set $P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$. Then we have
$$(5) \qquad \det P_n = p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}.$$
If we write
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma = \frac{a\gamma + b}{c\gamma + d}$$
where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z})$ and $\gamma \in \mathbf{R} - \mathbf{Q}$, then we have $[a_0, \ldots, a_{n-1}, \gamma] = P_{n-1}\gamma$.
4. The fundamental unit $\varepsilon = u + v\sqrt{m}$ is given by $u = p_{r-1}$, $v = q_{r-1}$ if $m \equiv 2, 3 \pmod 4$.

Lemma 11.
$$\begin{pmatrix} mq_{r-1} & p_{r-1} \\ p_{r-1} & q_{r-1} \end{pmatrix} = \begin{pmatrix} p_{r-1} & p_{r-2} \\ q_{r-1} & q_{r-2} \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. We have
$$\begin{aligned} \sqrt{m} &= [a_0, a_1, \ldots, a_{r-1}, a_0 + \sqrt{m}] \\ &= P_{r-1}(a_0 + \sqrt{m}) \\ &= \frac{p_{r-1}(a_0 + \sqrt{m}) + p_{r-2}}{q_{r-1}(a_0 + \sqrt{m}) + q_{r-2}}. \end{aligned}$$
So $\sqrt{m}(a_0 q_{r-1} + q_{r-2} - p_{r-1}) = a_0 p_{r-1} + p_{r-2} - mq_{r-1}$, i.e.
$$mq_{r-1} = a_0 p_{r-1} + p_{r-2},$$
$$p_{r-1} = a_0 q_{r-1} + q_{r-2}.$$
□

Lemma 12.
$$v = q_{s-1}(q_s + q_{s-2}) = q_{s-1}(a_s q_{s-1} + 2q_{s-2}),$$
$$mv = p_{s-1}(p_s + p_{s-2}) = p_{s-1}(a_s p_{s-1} + 2p_{s-2})$$
where $s = r/2$.

Proof.
$$\begin{aligned} P_{r-1} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_s & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{s-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s \left(\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} P_{s-1} \right)^T \\ &= P_s P_{s-1}^T \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}. \end{aligned}$$
Then by Lemma 11,
$$\begin{aligned} \begin{pmatrix} mq_{r-1} & p_{r-1} \\ p_{r-1} & q_{r-1} \end{pmatrix} &= P_{r-1} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s P_{s-1}^T \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= P_s P_{s-1}^T \\ &= \begin{pmatrix} p_s & p_{s-1} \\ q_s & q_{s-1} \end{pmatrix} \begin{pmatrix} p_{s-1} & q_{s-1} \\ p_{s-2} & q_{s-2} \end{pmatrix} \\ &= \begin{pmatrix} p_{s-1}(p_s + p_{s-2}) & p_s q_{s-1} + p_{s-1} q_{s-2} \\ p_{s-1} q_s + p_{s-2} q_{s-1} & q_{s-1}(q_s + q_{s-2}) \end{pmatrix}. \end{aligned}$$
Now remember that $v = q_{r-1}$. □

Theorem 13. *For $m \equiv 3 \pmod 4$ and $\sqrt{m} = [a_0; \overline{a_1, a_2, \ldots, a_r}]$, then $v \equiv a_s \pmod 2$ where $s = r/2$. So $\Delta_m = 1 \Leftrightarrow a_s$ is odd.*

Proof. By Lemma 12, $v \equiv a_s p_{s-1} \pmod 2$ and $v \equiv a_s q_{s-1} \pmod 2$. Since p_{s-1} and q_{s-1} are mutually prime by (5), they cannot be both even. One of the congruences says $v \equiv a_s \pmod 2$. □

References

[1] Ono, T.: A Note on Poincaré sums for finite groups. Proc. Japan Acad., **79A**, 95–97 (2003).

[2] Stark, H. M.: An Introduction to Number Theory. The MIT Press, Cambridge, Massachusetts-London, England (1978).