On the parity of calibers of real quadratic orders

Masanobu Kaneko, Hideyuki Sakata, and Maiko Takeuchi

1 Definitions and Result

In this paper, we determine the parity of calibers, both in wide and narrow senses, for *all* (not necessarily fundamental) real quadratic discriminants.

In our previous paper [3], we studied congruences modulo 4 of calibers of real quadratic fields whose discriminants are of special type, i.e., contain only two prime factors and are fundamental. For instance, when the discriminant is a product of two odd primes p and q congruent to 1 mod 4, we obtained a (partly conjectural) relationship between the caliber modulo 4 and the quadratic residue symbol (q/p).

For the parity, we can determine it for all discriminants in an elementary way. Although the determination of the parity does not require subtle quantities like the quadratic residue symbol, the complete classification may be of some value.

We use almost the same notation and convention as in [3], which we recall briefly here before stating the main theorem. A real quadratic number w is *reduced* if it satisfies $w > 1$ and $-1 < w' < 0$, where w' is the algebraic conjugate of w over the rationals $\mathbf{Q}$. The usual continued fraction expansion of w is purely periodic if and only if w is reduced. A positive integer D is a discriminant of a real quadratic order if and only if it is not a perfect square and $D \equiv 0$ or $1 \pmod 4$. A real quadratic number w is of discriminant D, denoted $\mathrm{disc}(w) = D$, if w satisfies

$$aw^2 + bw + c = 0,\ a, b, c \in \mathbf{Z}, a > 0,\ GCD(a, b, c) = 1, b^2 - 4ac = D.$$

Let $\mathcal{Q}(D)$ be the set of all reduced quadratic numbers of a given discriminant D:

$$\mathcal{Q}(D) := \{w \mid \mathrm{disc}(w) = D,\ w > 1,\ -1 < w' < 0\}.$$

The set $\mathcal{Q}(D)$ is finite and we call its cardinality $\kappa(D)$ the *caliber* of discriminant D:

$$\kappa(D) := \sharp\mathcal{Q}(D).$$

Any quadratic number of discriminant D is equivalent under the action of $\mathrm{GL}_2(\mathbf{Z})$ (via the linear fractional transformation) to an element in $\mathcal{Q}(D)$. We write $w_1 \sim w_2$ if the two numbers w_1 and w_2 are $\mathrm{GL}_2(\mathbf{Z})$-equivalent under this action. It is well-known that $w_1 \sim w_2$ if and only if their minimal periods of continued fraction expansions are cyclically equivalent. Let $\mathcal{R}(D)$ be the set of $\mathrm{GL}_2(\mathbf{Z})$-equivalence classes of $\mathcal{Q}(D)$ and $h(D)$ be its cardinality:

$$\mathcal{R}(D) := \mathcal{Q}(D)/\sim, \quad h(D) := \sharp\mathcal{R}(D).$$

The number $h(D)$ is nothing but the (wide) class number of discriminant D.

We can also consider the corresponding notions for $\mathrm{SL}_2(\mathbf{Z})$-equivalence, and have the similar sets and quantities $\mathcal{Q}^+(D)$, $\kappa^+(D)$, $\mathcal{R}^+(D)$, $h^+(D)$. For precise definitions and properties, see [3]. The quantity $\kappa^+(D)$ is the "m-caliber" (as we called it in [3]), or the caliber in the narrow sense, of discriminant D.

Our main result is the following.

Theorem 1. *For all positive discriminants D, the parities of $\kappa(D)$ and $\kappa^+(D)$ are completely determined as follows:*

(i) When $D = 8$, or D is of the form p^k or $4p^k$ with a prime $p \equiv 1 \pmod 4$, the caliber $\kappa(D)$ is odd. In all other cases, $\kappa(D)$ is even.

(ii) When D is a power of a single prime and $D \neq 8$, or D is of the form $4q^k$ with a prime $q \equiv 3 \pmod 4$, the m-caliber $\kappa^+(D)$ is odd. In all other cases, $\kappa^+(D)$ is even.

We prove this theorem in §3 after giving some preliminary lemmas and propositions in the next section. The final §4 will be devoted to the proof of lemmas.

2 Preliminaries

An element $w \in \mathcal{Q}(D)$ has a purely periodic continued fraction expansion

$$w = [\overline{a_0, \ldots, a_{n-1}}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}}}}}.$$

We define the quantities $l(w)$ and $s(w)$ by

$$l(w) := n \quad \text{and} \quad s(w) := \sum_{i=0}^{n-1} a_i,$$

the minimum period length and the sum of partial quotients in the period, respectively. Note that, for $w \in \mathcal{Q}(D)$, the period length $l(w)$ is even or odd according to $N(\varepsilon_D) = 1$ or -1, where ε_D is the fundamental unit of the quadratic order $\mathbf{Z}[(D+\sqrt{D})/2]$ of discriminant D, i.e., $\varepsilon_D > 1$ and the set $\{\pm\varepsilon_D^n\}_{n\in\mathbf{Z}}$ forms the group of units in the ring $\mathbf{Z}[(D+\sqrt{D})/2]$. In particular, the parity of $l(w)$ depends only on the discriminant. We use the following lemmas to establish the theorem. The proof of the lemmas will be postponed to the end of the paper.

Lemma 1. *We have*

$$\kappa(D) = \sum_{[w]\in\mathcal{R}(D)} l(w) \tag{1}$$

and

$$\kappa^+(D) = \sum_{[w]\in\mathcal{R}(D)} s(w), \tag{2}$$

where the sums run over a set of representatives of $\mathcal{R}(D)$ in $\mathcal{Q}(D)$.

Lemma 2. *Let $w \in \mathcal{Q}(D)$.*

(i) If D is odd, then we have $l(w) \equiv s(w) \pmod 2$.

(ii) If D is even and $N(\varepsilon_D) = -1$, then $s(w)$ is even.

(iii) Suppose D is even and $N(\varepsilon_D)=1$. If $w \in \mathcal{Q}(D)$ satisfies $w \sim -1/w'$, then we have

$$s(w) \equiv u_D \pmod 2, \tag{3}$$

where u_D is the coefficient u of $\sqrt{D}$ in the expression of the fundamental unit $\varepsilon_D = (t + u\sqrt{D})/2$. If furthermore $D \not\equiv 0 \pmod{32}$ and $D \not\equiv 12 \pmod{16}$, then $s(w)$ is even.

As a corollary, we have

Corollary 1. *When D is even and $N(\varepsilon_D)=1$, the congruence*

$$\kappa^+(D) \equiv h(D)u_D \pmod 2$$

holds.

We also need the following propositions, the first of which is a consequence of the theory of genera for general discriminants (see e.g., [1, §14.3, 14.5][1]), and the second is the classical class number formula (see e.g., [2, Ch. XIII]).

Proposition 1. *Let ν be the number of distinct odd primes dividing D and put*

$$\lambda = \begin{cases} \nu - 1 & \text{if} \quad D \text{ is odd}, \quad \text{or} \quad D \equiv 4 \pmod{16}, \\ \nu + 1 & \text{if} \quad D \equiv 0 \pmod{32}, \\ \nu & \text{otherwise}. \end{cases}$$

Then the narrow class number $h^+(D)$ is divisible by 2^λ.

Proposition 2. *Let $D = f^2 D_0$ be a discriminant, D_0 being the fundamental discriminant of $\mathbf{Q}(\sqrt{D})$ and f the conductor. Let μ be the unit index, i.e., the integer satisfying $\varepsilon_D = \varepsilon_{D_0}^{\mu}$. Then the class number $h(D)$ is given by*

$$h(D) = \frac{h(D_0) f}{\mu} \prod_{\ell | f} \left(1 - \frac{\chi_{D_0}(\ell)}{\ell}\right),$$

where ℓ runs over prime factors of f and χ_{D_0} is the Kronecker character associated to $\mathbf{Q}(\sqrt{D_0})$.

3 Proof of Theorem

In this section, we prove Theorem by using the lemmas and propositions in §2.

3.1 Parity of $\kappa(D)$

If $N(\varepsilon_D) = 1$, then $l(w)$ is even for any $w \in \mathcal{Q}(D)$, and so is $\kappa(D)$ by (1) of Lemma 1. In particular, we see that $\kappa(D)$ is even for a discriminant D divisible by 16 or a prime $q \equiv 3 \pmod 4$, as the congruence $x^2 - Dy^2 \equiv -4$ has no solutions modulo 16 or q respectively.

If $N(\varepsilon_D) = -1$, then $h(D) = h^+(D)$ holds. If D is divisible by at least two distinct odd primes, then we conclude by Proposition 1 that $h(D)\,(= h^+(D))$ is even, and hence $\kappa(D)$ is

[1] We thank Tomoyoshi Ibukiyama for informing us of the proposition and drawing attention to this reference.

even by equation (1). Note that all $l(w)$ have the same parity. For the case $D = 8$, it can be computed directly.

The remaining cases are $D = p^k, 4p^k, 8p^k$ with a prime $p \equiv 1 \pmod 4$. If $D = 8p^k$ and $N(\varepsilon_D) = -1$, then $h^+(D) = h(D)$ is even by Proposition 1 and hence $\kappa(D)$ is even by (1).

Now we show that if $D = p^k$ or $4p^k$, then $N(\varepsilon_D) = -1$ and $h(D)$ is odd. This implies that $\kappa(D)$ is odd by (1), and the proof of (i) is done. To show that $N(\varepsilon_D) = -1$ and $h(D)$ is odd in these cases, we use Proposition 2. Recall the classical facts that $N(\varepsilon_p) = -1$ and $h(p)$ is odd for a prime $p \equiv 1 \pmod 4$. Suppose $D = p^k$. Since D is not a perfect square, we see that k is odd, and also $D_0 = p$, $f = p^{(k-1)/2}$ and $\ell = p$ with the notation in Proposition 2. Hence the unit index μ should be odd. Thus, $N(\varepsilon_D) = N(\varepsilon_p)^\mu = -1$, and $h(D)$ is odd. If $D = 4p^k$, then $f = 2p^{(k-1)/2}$ and $D_0 = p$. In this case, the factor $1 - \chi_{D_0}(\ell)/\ell$ in the formula of Proposition 2 for $\ell = 2$ is $1/2$ or $3/2$ and hence the denominator 2 cancels out the factor 2 in f. This shows again that the unit index μ is odd, and the same conclusion as in the case $D = p^k$ holds. This establishes (i) of Theorem 1.

3.2 Parity of $\kappa^+(D)$

We proceed to determine the parity of $\kappa^+(D)$.

When D is odd, we know by (i) of Lemma 2 and Lemma 1 that $\kappa^+(D) \equiv \kappa(D) \pmod 2$. Hence the theorem is already proved in the previous subsection. We note that when D is a power of an odd prime p, it is necessary that $p \equiv 1 \pmod 4$ because $D \equiv 1 \pmod 4$ and D cannot be a perfect square.

From now on, we assume that D is even. Let us first look at the case when D is a power of 2. For $D = 8$, we can directly compute as $\kappa^+(8) = 2$. When $D = 2^{2k+3}$ with $k \geq 1$, the corresponding fundamental discriminant is 8 and the conductor is 2^k. The fundamental unit of the ring $\mathbf{Z}[\sqrt{2}]$ of discriminant 8 is $1+\sqrt{2}$. It is then easy to see that $\varepsilon_D = (1+\sqrt{2})^{2^k}$ whose norm is 1, and thus that $h(D)$ is odd by Proposition 2. Furthermore, we see inductively that $(1+\sqrt{2})^{2^k} = (t_D + u_D\sqrt{D})/2$ with u_D odd. Hence by Corollary 1, we conclude that $\kappa^+(D)$ is odd.

Suppose D is divisible by an odd prime. When $N(\varepsilon_D) = -1$, every $s(w)$ is even by (ii) of Lemma 2 and thus $\kappa^+(D)$ is even.

Assume $N(\varepsilon_D) = 1$. If $D \equiv 0 \pmod{32}$, then $h(D)$ is even by Proposition 1, and hence $\kappa^+(D)$ is even by Corollary 1. If $D \not\equiv 0 \pmod{32}$ and $D \not\equiv 12 \pmod{16}$, then $\kappa^+(D)$ is even by (iii) of Lemma 2 and (2) of Lemma 1.

Finally, suppose $D \equiv 12 \pmod{16}$. If D is divisible by at least two distinct odd primes, then $h^+(D)$ is divisible by 4 and hence $h(D)$ is even, by Proposition 1. We then see that $\kappa^+(D)$ is even by Corollary 1. When D is divisible by a single odd prime q, we necessarily have $D = 4q^k$ with $q \equiv 3 \pmod 4$ because of the congruence $D \equiv 12 \pmod{16}$. The corresponding fundamental discriminant D_0 is $4q$ and we know by [4] that $h(4q)$ is odd. From this we see by Proposition 2 that $h(D)$ is odd. Therefore, by Corollary 1, the m-caliber $\kappa^+(D)$ is odd if and only if u_D is odd. But when $D = 4q^k$ with a prime $q \equiv 3 \pmod 4$, the number u_D is always odd. To see this, we only need to see that u_{4q} is odd because the unit index μ in $\varepsilon_D = \varepsilon_{4q}^\mu$ is odd (by Proposition 2 and that $h(4q)$ is odd). The fact that u_{4q} is odd is proved in [6] (see also [5] for a simpler proof and a historical remark).[2] This completes the proof of Theorem. □

[2]We thank Kenneth S. Williams for informing us of these references as well as showing us the simple proof of this fact using the method of Dirichlet.

4 Proof of Lemmas

Equation (1) of Lemma 1 is immediate from the definition, and (2) has appeared in [3, Proposition 2.1]. For the assertions (i) and (ii) of Lemma 2, see also [3, Lemma 2.3]. In the following, we shall prove (iii) of Lemma 2 and Corollary 1.

Suppose D is even and $N(\varepsilon_D) = 1$. Let $w = [\overline{a_0, \dots, a_{n-1}}] \in \mathcal{Q}(D)$ satisfies $w \sim -1/w'$. Set

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} := \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}.$$

Then from the standard theory we have

$$w = \frac{pw + q}{rw + s}$$

which is equivalent to $rw^2 + (s-p)w - q = 0$, and the fundamental discriminant is given by

$$\varepsilon_D = \frac{t_D + u_D\sqrt{D}}{2} = rw + s. \tag{4}$$

Let $g := GCD(r, s-p, q)$. The minimal equation of w is then

$$\frac{r}{g}w^2 + \frac{s-p}{g}w - \frac{q}{g} = 0,$$

and hence

$$w = \frac{-s + p + g\sqrt{D}}{2r} \tag{5}$$

and

$$g^2 D = (s-p)^2 + 4rq. \tag{6}$$

We thus obtain

$$g = u_D \tag{7}$$

by (4) and (5).

Now we look at $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ mod 2. First note that $l(w)$ is even because $N(\varepsilon_D) = 1$. Assume $s(w)$ is even. Then, among the partial quotients a_i of $w = [\overline{a_0, \dots, a_{n-1}}]$, the numbers of odd a_i's and even a_i's are both even. Then by [3, Lemma 2.2], we have

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2.$$

But since D is even, the number $s - p$ is even by (6) and thus the only possibility is

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2.$$

From this we see that r and q are also even and hence $g = GCD(r, s-p, q)$ is even. By (7), we conclude that u_D is even and so $s(w) \equiv u_D \pmod 2$.

Next assume $s(w)$ is odd. Because $w \in \mathcal{Q}(D)$ satisfies $w \sim -1/w'$, the periods $[a_0, \dots, a_{n-1}]$ and $[a_{n-1}, \dots, a_0]$ of w and $-1/w'$ are cyclically equivalent, i.e., there is an index i such that

$$[a_0, \dots, a_{i-1}, a_i, \dots, a_{n-1}] = [a_{i-1}, \dots, a_0, a_{n-1}, \dots, a_i]. \tag{8}$$

This means that the two subsequences $[a_0, \dots, a_{i-1}]$ and $[a_i, \dots, a_{n-1}]$ are both palindromic. Recall that the length n is even. Thus, in order to have $s(w)$ odd, the only possibility is that both i and $n-i$ are odd, and one and the only one of the "centers" of $[a_0, \dots, a_{i-1}]$ and $[a_i, \dots, a_{n-1}]$ is odd. Set $E := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $O := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then, by the congruences

$$E^2 \equiv O^3 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad OEO \equiv E, \quad EOE \equiv O^2 \pmod 2,$$

we conclude that the possibility is

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv E, \quad OE, \quad O^2E, \quad EO, \quad \text{or} \quad EO^2 \pmod 2.$$

Therefore, we have

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ or } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod 2.$$

In any cases, at least one of r, q is odd and hence $u_D(=g)$ is odd. This establishes (3).

Assume furthermore $D \not\equiv 0 \pmod{32}$ and $D \not\equiv 12 \pmod{16}$. If $s(w)$ is odd, by rotating cyclically (8) to place the odd center of either $[a_0, \dots, a_{i-1}]$ or $[a_i, \dots, a_{n-1}]$ at the top, we see that there exists an element w_1 equivalent to w such that its continued fraction expansion is of the form

$$[\overline{b_0, b_1, \dots, b_s, b_{s+1}, b_s, \dots, b_1}]$$

with b_0 odd. Then we have

$$w_1 = b_0 + \frac{1}{-\frac{1}{w_1'}} = b_0 - w_1'.$$

Let

$$aw_1^2 + bw_1 + c = 0, \ GCD(a, b, c) = 1, \ a > 0$$

be the minimal equation of w_1. Then we have $b_0 = w_1 + w_1' = -b/a$. Because b_0 is odd, we may write $a = 2^k a'$ and $b = 2^k b'$ with a', b' both odd. Since the discriminant D of w_1 is even, we conclude from $D = b^2 - 4ac$ that b is even, i.e., $k \geq 1$ and a is also even. Since $GCD(a, b, c) = 1$, the integer c must be odd. Now look at

$$D = b^2 - 4ac = 2^{2k}b'^2 - 2^{k+2}a'c.$$

If $k = 1$, then $D = 4(b'^2 - 2a'c) \equiv 12 \pmod{16}$, and if $k \geq 2$, then $D = 2^{k+2}(2^{k-2}b'^2 - a'c)$ is divisible by 32. This contradicts to $D \not\equiv 0 \pmod{32}$ and $D \not\equiv 12 \pmod{16}$. Thus $s(w)$ cannot be odd. This completes the proof of Lemma 2. □

Finally, we prove Corollary 1. Recall that, for any $w = [\overline{a_0, \dots, a_{n-1}}] \in \mathcal{Q}(D)$, we see that $-1/w' = [\overline{a_{n-1}, \dots, a_0}]$ and hence $s(w) = s(-1/w')$. From this we have

$$\kappa^+(D) = \sum_{[w] \in \mathcal{R}(D)} s(w) \equiv \sum_{[w] \in \mathcal{R}(D), w \sim -1/w'} s(w) \pmod 2.$$

By (iii) of Lemma 2, we then have

$$\kappa^+(D) \equiv \sum_{[w] \in \mathcal{R}(D), w \sim -1/w'} u_D \equiv \sum_{[w] \in \mathcal{R}(D)} u_D = h(D)u_D \pmod 2$$

as desired. □

Acknowledgments. This work was partially supported by JSPS Grant-in-Aid for Scientific Research (S) 24224001 and (B) 23340010.

References

[1] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press (1978), xiv+318 pp.

[2] H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, INC., (1962), xiii+276 pp.

[3] M. Kaneko and K. Mori, Congruenced modulo 4 of calibers of real quadratic fields, *Ann. Sci. Math. Québec*, **35-2** (2011), 185–195.

[4] L. Rédei and H. Reichardt, Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.*, **170** (1934), 69–74.

[5] K. S. Williams, Historical remark on a theorem of Zhang and Yue, *J. Number Theory*, **147** (2015), 691–693.

[6] Z. Zhang and Q. Yue, Fundamental units of real quadratic fields of odd class number, *J. Number Theory*, **137** (2014), 122–129.

Masanobu Kaneko
Faculty of Mathematics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka 819-0395, Japan
mkaneko@math.kyushu-u.ac.jp

Hideyuki Sakata
CLIS Co., Ltd.
CR EAST Building,1-15-1, Kotobashi, Sumida-ku, Tokyo 130-0022, Japan
da.san@hotmail.co.jp

Maiko Takeuchi
Graduate School of Mathematics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka 819-0395, Japan
m.takeuchi.math@gmail.com