Ann. Sci. Math. Québec **35**, No 2, (2011), 185–195

CONGRUENCES MODULO 4 OF CALIBERS OF REAL QUADRATIC FIELDS

MASANOBU KANEKO AND KEITA MORI

Dedicated to professor Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Nous présentons des conjectures sur les congruences modulo 4 des calibres (au sens restreint) d'ordres quadratiques réels pour certains discriminants, et nous donnons des preuves dans quelques cas.

ABSTRACT. We present conjectures on congruences modulo 4 of the calibers (in the narrow sense) of real quadratic orders of particular discriminants, and prove some partial results on them.

1. Definitions and results

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 $\mathbf{Q}$. It is well known that w is reduced if and only if its usual continued fraction expansion is purely periodic. Consider the set of all reduced quadratic numbers of a given discriminant D:

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

Here, a real quadratic irrationality w is of discriminant D, denoted $\mathrm{disc}(w) = D$, if w satisfies

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

The set $\mathcal{Q}(D)$ is finite and its cardinality is denoted by $\kappa(D)$. When D is a fundamental discriminant, *i.e.*, the discriminant of the real quadratic field $\mathbf{Q}(\sqrt{D})$, the number $\kappa(D)$ is referred to as the *caliber* of $\mathbf{Q}(\sqrt{D})$ (see [1]).

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. It is known that $w_1 \sim w_2$ if and only if their 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:

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

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

Reçu le 22 février 2009 et, sous forme définitive, le 4 avril 2009.

We also consider the corresponding notions for $\mathrm{SL}_2(\mathbf{Z})$-equivalence. We call a real quadratic number w *m-reduced* if $w > 1$ and $0 < w' < 1$. A number is m-reduced if and only if its "minus" continued fraction expansion is purely periodic (see [5, §13]). Let $\mathcal{Q}^+(D)$ be the set of all m-reduced numbers of a given discriminant D:

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

This is also a finite set and its cardinality will be denoted by $\kappa^+(D)$. We refer to this number as the *m-caliber* of (not necessarily fundamental) discriminant D. Consider the equivalence under the action of $\mathrm{SL}_2(\mathbf{Z})$. Two numbers w_1 and w_2 are strictly equivalent, written $w_1 \approx w_2$, if the two are related with each other by a transformation in $\mathrm{SL}_2(\mathbf{Z})$. Any quadratic number of discriminant D is strictly equivalent to an element in $\mathcal{Q}^+(D)$, and two elements in $\mathcal{Q}^+(D)$ are strictly equivalent if and only if the periods of their minus continued fraction expansions are cyclically equivalent. Let $\mathcal{R}^+(D)$ be the set of $\mathrm{SL}_2(\mathbf{Z})$-equivalence classes of $\mathcal{Q}^+(D)$ and $h^+(D)$ be its cardinality (the "narrow" class number):

$$\mathcal{R}^+(D) = \mathcal{Q}^+(D)/\approx, \qquad h^+(D) = \sharp\,\mathcal{R}^+(D).$$

Throughout the paper, we denote by p a prime number congruent to 1 modulo 4, and by q a prime number larger than p which is also congruent to 1 modulo 4. Integers x_p, y_p, x_q, y_q are uniquely defined by the decomposition

$$p = x_p^2 + y_p^2, \quad (0 < x_p < y_p), \qquad q = x_q^2 + y_q^2, \quad (0 < x_q < y_q).$$

We denote by ε_D the fundamental unit of discriminant D and by $N(\varepsilon_D)$ its norm.

We conducted numerical experiments on the 2-orders of the m-calibers $\kappa^+(8p)$ and $\kappa^+(pq)$, which are easily seen to be even integers, and observed the following[1].

Conjectures. (1) *We have*

$$\kappa^+(8p) \equiv 1 - (-1)^{x_p} \pmod 4.$$

(2) *Assume $p < q$ and suppose $x_p \not\equiv x_q \pmod 2$. Then we have*

$$\kappa^+(pq) \equiv 1 - (-1)^{x_p} \left(\frac{q}{p}\right) \pmod 4.$$

For the narrow class numbers $h^+(8p)$ and $h^+(pq)$ (which are always even), the following two properties are known (*cf.* [2]):

(i) $h^+(8p)$ is divisible by 4 if and only if $p \equiv 1 \pmod 8$, and

(ii) $h^+(pq)$ is divisible by 4 if and only if $\left(\frac{q}{p}\right) = 1$.

The above conjectures say that the divisibility by 4 of $\kappa^+(8p)$ and $\kappa^+(pq)$ depends on the *parity* of x_p or x_q, not only on $\left(\frac{q}{p}\right)$ in the case (2), which may be of considerable interest.

[1] Special case of the conjecture and Theorem 1.1 were discussed in Umeno [4].

In this paper, we prove (1) in the case where $N(\varepsilon_{8p}) = -1$, and some partial result for (2) also in the case where $N(\varepsilon_{pq}) = -1$.

Theorem 1.1. *Let p be a prime number such that $p \equiv 1 \pmod 4$, and suppose $N(\varepsilon_{8p}) = -1$. Then the class modulo 4 of the m-caliber $\kappa^+(8p)$ is given by*

$$\kappa^+(8p) \equiv 1 - (-1)^{x_p} \pmod 4.$$

As far as Conjecture (2) is concerned, we are not able to prove it even under the condition $N(\varepsilon_{pq}) = -1$, but we obtain the following partial result. Notice that, corresponding to the two decompositions of pq into sums of two squares

$$pq = (x_p x_q + y_p y_q)^2 + (x_p y_q - y_p x_q)^2 = (x_p y_q + y_p x_q)^2 + (x_p x_q - y_p y_q)^2,$$

there exist exactly two quadratic numbers $\alpha, \beta \in \mathcal{Q}(pq)$ whose periods of usual continued fraction expansions are palindromic. We denote by $l(\alpha)$ and $l(\beta)$ their period lengths.

Theorem 1.2. *Besides the assumptions $p < q$ and $x_p \not\equiv x_q \pmod 2$, we further suppose $N(\varepsilon_{pq}) = -1$. Then we have*

$$\kappa^+(pq) \equiv 1 + \operatorname{sgn}(x_p y_q - y_p x_q)(-1)^{x_p + \frac{l(\alpha)-l(\beta)}{2}} \left(\frac{q}{p}\right) \pmod 4.$$

Thus our conjecture in the case $N(\varepsilon_{pq}) = -1$ is that

$$x_p y_q - y_p x_q < 0 \text{ if and only if } l(\alpha) \equiv l(\beta) \pmod 4.$$

2. Preliminaries

As it is recalled in the previous section, the elements $\alpha \in \mathcal{Q}(D)$ and $\beta \in \mathcal{Q}^+(D)$ have purely periodic usual and minus continued fraction expansions

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

and

$$\beta = [[\overline{b_0, \ldots, b_{m-1}}]] = b_0 - \cfrac{1}{b_1 - \cfrac{1}{\ddots - \cfrac{1}{b_{m-1} - \cfrac{1}{b_0 - \cfrac{1}{b_1 - \cfrac{1}{\ddots}}}}}}$$

respectively. We define $l(\alpha) := n$ and $l^+(\beta) := m$ to be their minimum period lengths; moreover,

$$S(\alpha) := \sum_{i=0}^{n-1} a_i \quad \text{and} \quad S^+(\beta) := \sharp\left\{ j \mid 0 \le j \le m-1,\ b_j \ge 3 \right\}$$

are respectively called the sum of partial quotients and the number of partial quotients greater than or equal to 3 in the period.

In order to establish our results, we use the following result which may be standard, but for which, for the sake of convenience, we reproduce the proof given in Suzuki [3].

Proposition 2.1. *We have*

$$\kappa^+(D) = \sum_{[\alpha]\in\mathcal{R}(D)} S(\alpha) \quad \textit{and} \quad \kappa(D) = \sum_{[\beta]\in\mathcal{R}^+(D)} S^+(\beta).$$

Proof. We prove the first assertion, the second being similarly proved (we shall not use the second formula). By definition, we have

$$\kappa^+(D) = \sum_{[\beta]\in\mathcal{R}^+(D)} l^+(\beta).$$

We may assume that all representatives β are bigger than 2, because at least one of the partial quotients b_j in the expansion $\beta = [[\,\overline{b_0, \dots, b_{m-1}}\,]]$ is bigger than 2 and hence by a cyclic permutation we obtain a number greater than 2, equivalent to β. As is easily seen, the map

$$T :\ \mathcal{Q}(D) \ni \alpha \mapsto \alpha + 1 \in \mathcal{Q}^+(D) \tag{2.1}$$

gives a bijection between the sets $\mathcal{Q}(D)$ and $\{\beta \in \mathcal{Q}^+(D) \mid \beta > 2\}$. If the usual continued fraction expansion of $\alpha \in \mathcal{Q}(D)$ is $\alpha = [\,\overline{a_0, \dots, a_{n-1}}\,]$, then the minus continued fraction expansion of $T(\alpha) = \alpha + 1$ is given by (see *e.g.* [5])

$$\begin{cases} [[\,\overline{a_0+2, \underbrace{2, \dots, 2}_{a_1-1}, a_2+2, \underbrace{2, \dots, 2}_{a_3-1}, \dots, a_{n-2}+2, \underbrace{2, \dots, 2}_{a_{n-1}-1}}\,]] & \text{if } n \text{ is even,} \\ [[\,\overline{a_0+2, \underbrace{2, \dots, 2}_{a_1-1}, \dots, a_{n-1}+2, \underbrace{2, \dots, 2}_{a_0-1}, \dots, a_{n-2}+2, \underbrace{2, \dots, 2}_{a_{n-1}-1}}\,]] & \text{if } n \text{ is odd.} \end{cases}$$

If n is even, then the images under T of $[\,\overline{a_i, \dots, a_{n-1}, a_0, \dots, a_{i-1}}\,]$ which are equivalent to α split into two classes (under the equivalence $\approx$) according to the parity of i. By the formula above we have

$$l^+\big(T([\,\overline{a_0, \dots, a_{n-1}}\,])\big) = a_1 + a_3 + \cdots + a_{n-1},$$

$$l^+\big(T([\,\overline{a_1, \dots, a_{n-1}, a_0}\,])\big) = a_2 + a_4 + \cdots + a_{n-2} + a_0,$$

and hence

$$l^+\big(T([\,\overline{a_0, \dots, a_{n-1}}\,])\big) + l^+\big(T([\,\overline{a_1, \dots, a_{n-1}, a_0}\,])\big) = S(\alpha).$$

If n is odd, then all $T([\,\overline{a_i, \dots, a_{n-1}, a_0, \dots, a_{i-1}}\,])$ are equivalent and

$$l^+(T(\alpha)) = S(\alpha).$$

It is clear that the equivalence $T(\alpha_1) \approx T(\alpha_2)$ implies $\alpha_1 \sim \alpha_2$. From this and the surjectivity of (2.1), we conclude the assertion $\kappa^+(D) = \sum_{[\alpha]\in\mathcal{R}(D)} S(\alpha)$. □

The following lemma is repeatedly used in our proof.

Lemma 2.2. *Let*

$$E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \textit{and} \quad O = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

be elements in $\mathrm{GL}_2(\mathbf{F}_2)$ *of order 2 and 3 respectively. Consider the product*

$$M = M_1 \cdots M_n$$

of length n *of* k O*'s and* $(n-k)$ E*'s (i.e.,* $M_i = E$ *or* O *and the number of* O*'s is* k*). Then we have the equivalence*

$$n \equiv k \pmod 2 \Longleftrightarrow M \in \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, O = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, O^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Proof. Using relations $E^2 = I$, $O^3 = I$, $OEO = E$ $(OE = EO^2)$, any product of E's and O's reduces to one of the six elements

$$I,\ O,\ O^2,\ E,\ EO = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ OE = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

In this reduction process, the parity of

$$\text{(total length of product)} - \text{(number of } O\text{'s)}$$

does not change, and out of the above six elements this parity is even exactly when it is $I,\ O,\ O^2$. □

Lemma 2.3. *Let* $\alpha \in \mathcal{Q}(D)$.

(i) *If* D *is odd, then we have* $l(\alpha) \equiv S(\alpha) \pmod 2$.

(ii) *If* D *is even and* $N(\varepsilon_D) = -1$*, then* $S(\alpha)$ *is even.*

Proof. Let the quadratic equation satisfied by α be

$$a\alpha^2 + b\alpha + c = 0 \quad \text{with} \quad \mathrm{GCD}(a,b,c) = 1 \quad \text{and} \quad b^2 - 4ac = D.$$

For the continued fraction expansion $\alpha = [\overline{a_0, a_1, \ldots, a_{n-1}}]$, we 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 we have $\alpha = \dfrac{p\alpha + q}{r\alpha + s}$ and thus

$$r\alpha^2 + (s-p)\alpha - q = 0.$$

Put $d := \mathrm{GCD}(r, s-p, q)$ (> 0). Then we have $r = da$, $s - p = db$, and $q = -dc$.

(i) Assume D is odd. Then b is odd. If d is odd, then $s - p$ is odd and so ps is even, hence qr is odd because $ps - qr = (-1)^n$. Thus

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

If d is even, then $r \equiv q \equiv 0,\ p \equiv s \pmod 2$, whereupon

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

By Lemma 2.2, we conclude $n \equiv S(\alpha) \pmod 2$, because the parities of $S(\alpha)$ and of the number of odd a_i are the same.

(ii) Assume D is even. Then b should be even and so $p \equiv s \pmod 2$. If $p \equiv s \equiv 1 \pmod 2$ and $q \equiv r \equiv 0 \pmod 2$, then d is even (otherwise a, b, c are all even) and $s - p = db \equiv 0 \pmod 4$. In this case we have $ps - qr \equiv 1 - 0 \equiv 1 \pmod 4$. This contradicts $ps - qr = -1$ which is equivalent to the condition $N(\varepsilon_D) = -1$. Therefore, we have the possibilities

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

By Lemma 2.2, we see $S(\alpha) \not\equiv n \pmod 2$ and thus $S(\alpha)$ is even because n is odd. □

3. Proofs of Theorems

Proof of Theorem 1.1. Corresponding to the decomposition

$$8p = \big(2(x_p + y_p)\big)^2 + \big(2(y_p - x_p)\big)^2,$$

there exist exactly two elements $\alpha, \beta \in \mathcal{Q}(8p)$ which satisfy $\alpha = -1/\alpha'$, $\beta = -1/\beta'$. These are the largest roots of the equations

$$(3.1)\quad (x_p + y_p)\alpha^2 + 2(x_p - y_p)\alpha - (x_p + y_p) = 0$$
$$\text{and} \quad (y_p - x_p)\beta^2 - 2(x_p + y_p)\beta + x_p - y_p = 0$$

respectively. By our assumption on the norm of the fundamental unit ($N(\varepsilon_{8p}) = -1$), we may take α and β as part of the representatives of $\mathcal{R}(8p)$, the other representatives being in the form $\gamma_1, -1/\gamma_1', \ldots, \gamma_t, -1/\gamma_t'$. From Lemma 2.3 (ii) we have

$$S(\gamma_i) + S(-1/\gamma_i) = 2S(\gamma_i) \equiv 0 \pmod 4.$$

Hence, by Proposition 2.1, it suffices to prove that

$$S(\alpha) + S(\beta) \equiv \begin{cases} 0 \pmod 4 & \text{if} \quad x_p \text{ is even,} \\ 2 \pmod 4 & \text{if} \quad x_p \text{ is odd.} \end{cases}$$

Let

$$\alpha = [\,\overline{a_0, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_0}\,] \quad \text{and} \quad \beta = [\,\overline{b_0, \ldots, b_{m-1}, b_m, b_{m-1}, \ldots, b_0}\,]$$

be their (palindromic) continued fraction expansions (by our assumption $N(\varepsilon_{8p}) = -1$, their period lengths are odd) and set

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} := \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix} := \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix},$$

$$\begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} := \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_{m-1} & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} P' & Q' \\ R' & S' \end{pmatrix} := \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix} \begin{pmatrix} b_m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p' & r' \\ q' & s' \end{pmatrix}.$$

Then we have

$$R\alpha^2 + (S-P)\alpha - Q = 0, \quad R'\beta^2 + (S'-P')\beta - Q' = 0. \tag{3.2}$$

Set $d := \mathrm{GCD}(R, S-P, Q)$ and $d' = \mathrm{GCD}(R', S'-P', Q')$.

Lemma 3.1.

(i) $P + S = P' + S'$.

(ii) $d = d'$.

Proof. Let ε_D be the fundamental unit of discriminant D. The classical construction of ε_D from the continued fraction expansions shows that the equalities

$$\varepsilon_D = R\alpha + S = R'\beta + S'$$

holds. Computing $\varepsilon_D + \varepsilon'_D$ in two ways and using it as

$$\varepsilon_D + \varepsilon'_D = R(\alpha + \alpha') + 2S = R \cdot \frac{P-S}{R} + 2S = P + S$$

$$= R'(\beta + \beta') + 2S' = R' \cdot \frac{P'-S'}{R'} + 2S' = P' + S',$$

we obtain equality (i). The second equality (ii) follows similarly from the computation of $(\varepsilon_D - \varepsilon'_D)/\sqrt{D}$. □

From (3.1) and (3.2), we have

$$R = Q = d(x_p + y_p), \tag{3.3}$$

$$R' = Q' = d(y_p - x_p), \tag{3.4}$$

$$P - S = 2d(y_p - x_p), \tag{3.5}$$

$$P' - S' = 2d(x_p + y_p). \tag{3.6}$$

By (3.3) and (3.4), we obtain

$$R - R' = Q - Q' = 2dx_p, \tag{3.7}$$

and by (3.5), (3.6) and Lemma 3.1 (i), we have

$$P - P' = S' - S = -2dx_p.$$

By Lemma 2.3 (ii) and its proof, we have $a_n \equiv b_m \equiv 0 \pmod 2$ and

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} P' & Q' \\ R' & S' \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2.$$

Then from (3.3), we have that d is odd and from (3.5), we deduce that

$$P - S \equiv 2 \pmod 4.$$

Assume $P \equiv 0,\ S \equiv 2 \pmod 4$. By $S = r^2 a_n + 2rs \equiv 2 \pmod 4$, r must be odd and we have $a_n + 2s \equiv 2 \pmod 4$. If $a_n \equiv 2 \pmod 4$, then s is even and q is odd. In this case, we have

$$Q = pra_n + qr + ps = pra_n + 2qr + (-1)^n \equiv 2p + 2 + (-1)^n \pmod 4.$$

When $Q \equiv 1 \pmod 4$, p is odd or even according as n is even or odd, and we have respectively

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

In either case, we conclude by Lemma 2.2 that $S(\alpha) \equiv 2 \pmod 4$. Similarly we have $S(\alpha) \equiv 0 \pmod 4$ when $Q \equiv -1 \pmod 4$. Also by the same argument we see that when $a_n \equiv 0 \pmod 4$ we have $S(\alpha) \equiv 0 \pmod 4$ or $S(\alpha) \equiv 2 \pmod 4$ according as $Q \equiv -1 \pmod 4$ or $Q \equiv 1 \pmod 4$.

In summary, we have

$$S(\alpha) \equiv \begin{cases} 0 \pmod 4 & \text{if} \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 0 & -1 \\ -1 & 2 \end{pmatrix} \pmod 4, \\ \\ 2 \pmod 4 & \text{if} \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \pmod 4. \end{cases}$$

Likewise, we obtain by considering the different cases and using Lemma 2.2 that

$$S(\alpha) \equiv \begin{cases} 0 \pmod 4 & \text{if} \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 2 & -1 \\ -1 & 0 \end{pmatrix} \pmod 4, \\ \\ 2 \pmod 4 & \text{if} \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \pmod 4. \end{cases}$$

All these show that we have

$$S(\alpha) \equiv \begin{cases} 0 \pmod 4 & \text{if } Q \equiv -1 \pmod 4, \\ 2 \pmod 4 & \text{if } Q \equiv 1 \pmod 4. \end{cases}$$

Exactly the same holds for $S(\beta)$, that is to say,

$$S(\beta) \equiv \begin{cases} 0 \pmod 4 & \text{if } Q' \equiv -1 \pmod 4, \\ 2 \pmod 4 & \text{if } Q' \equiv 1 \pmod 4. \end{cases}$$

Now, by (3.7), $Q \equiv Q' \pmod 4$ if and only if x_p is even. Hence we have

$$S(\alpha) + S(\beta) \equiv \begin{cases} 0 \pmod 4 & \text{if} \quad x_p \text{ is even}, \\ 2 \pmod 4 & \text{if} \quad x_p \text{ is odd}, \end{cases}$$

which is what we need to establish Theorem 1.1. □

Proof of Theorem 1.2. We proceed similarly, and keep the same notation. Let α and β be the largest roots of the equations

$$\frac{x_p x_q + y_p y_q}{2}\alpha^2 - |x_p y_q - y_p x_q|\alpha - \frac{x_p x_q + y_p y_q}{2} = 0$$

and

$$\frac{y_p y_q - x_p x_q}{2}\beta^2 - (x_p y_q + y_p x_q)\beta + \frac{x_p x_q - y_p y_q}{2} = 0$$

respectively. These are the only elements in $\mathcal{Q}(pq)$ satisfying $\alpha = -1/\alpha'$, $\beta = -1/\beta'$, corresponding to the decompositions

$$\begin{aligned} pq &= (x_p x_q + y_p y_q)^2 + (x_p y_q - y_p x_q)^2 \\ &= (x_p y_q + y_p x_q)^2 + (x_p x_q - y_p y_q)^2. \end{aligned}$$

By the assumption $x_p \not\equiv x_q \pmod 2$, $x_p y_q - y_p x_q$ and $x_p y_q + y_p x_q$ are odd. As in the proof of Theorem 1.1, we may take as representatives of $\mathcal{R}(pq)$ α, β, and the other in the form $\gamma_1, -1/\gamma_1', \ldots, \gamma_t, -1/\gamma_t'$. By Lemma 2.3 (i) and the assumption $N(\varepsilon_{pq}) = -1$, we have

$$S(\gamma_i) + S(-1/\gamma_i) = 2S(\gamma_i) \equiv 2 \pmod 4.$$

By the theorem of Rédei-Reichardt [2],

$$\sharp\mathcal{R}(pq) \equiv 0 \pmod 4 (\Leftrightarrow t \text{ is odd}) \Longleftrightarrow \left(\frac{q}{p}\right) = 1.$$

Thus,

$$\sum_{i=1}^{t} \big(S(\gamma_i) + S(-1/\gamma_i')\big) \equiv 2 \pmod 4 \Longleftrightarrow \left(\frac{q}{p}\right) = 1,$$

that is,

$$\sum_{i=1}^{t} \big(S(\gamma_i) + S(-1/\gamma_i')\big) \equiv 1 + \left(\frac{q}{p}\right) \pmod 4.$$

Since

$$\kappa^+(pq) = S(\alpha) + S(\beta) + \sum_{i=1}^{t} \big(S(\gamma_i) + S(-1/\gamma_i')\big)$$

by Proposition 2.1, to prove the theorem we need to show

$$\begin{aligned} S(\alpha) + S(\beta) &\equiv \left(\frac{q}{p}\right)\left(-1 + \operatorname{sgn}(x_p y_q - y_p x_q)(-1)^{x_p + \frac{l(\alpha)-l(\beta)}{2}}\right) \\ &\equiv 1 - \operatorname{sgn}(x_p y_q - y_p x_q)(-1)^{x_p + \frac{l(\alpha)-l(\beta)}{2}} \pmod 4. \end{aligned} \tag{3.8}$$

(We have used the simple fact that $k \equiv \pm k \pmod 4$ when k is even.)

Let the continued fraction expansions of α and β be the same as in the proof of Theorem 1.1, and similarly construct the matrices

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}, \quad \begin{pmatrix} P & Q \\ R & S \end{pmatrix}, \quad \textit{etc.}$$

Then we have

$$R = Q = d\,\frac{x_p x_q + y_p y_q}{2}, \tag{3.9}$$

$$R' = Q' = d\,\frac{y_p y_q - x_p x_q}{2}, \tag{3.10}$$

$$P - S = d|x_p y_q - y_p x_q|, \tag{3.11}$$

$$P' - S' = d(x_p y_q + y_p x_q), \tag{3.12}$$

and (because Lemma 3.1 also holds in this case)

$$R - R' = Q - Q' = dx_p x_q, \tag{3.13}$$

$$P - P' = S' - S = -d\min(x_p y_q, y_p x_q). \tag{3.14}$$

Since $D = pq$ is odd, by Lemma 2.3 (i) and Lemma 2.2 we have

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2$$

and $a_n \equiv b_m \equiv 1 \pmod 2$.

We need to carry out rather tedious case distinctions, but here we describe how to deduce the conclusion only in the case when

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2,$$

the other cases being similarly treated. In this case, because

$$Q = pra_n + 2qr + (-1)^n \equiv 0 \pmod 2,$$

p and r are both odd, and thus

$$P = p^2 a_n + 2pq \equiv a_n + 2q \pmod 4.$$

Suppose $P \equiv 1 \pmod 4$. If $a_n \equiv 1 \pmod 4$, then q is even and by Lemma 2.2 we conclude $S(\alpha) \equiv 1 \pmod 4$ (resp. $\equiv 3 \pmod 4$) when n is odd (resp. even). If $a_n \equiv 3 \pmod 4$, then q is odd and we similarly have $S(\alpha) \equiv 1 \pmod 4$ (resp. $\equiv 3 \pmod 4$) when n is odd (resp. even). Likewise, when $P \equiv -1 \pmod 4$, we have $S(\alpha) \equiv 1 \pmod 4$ (resp. $\equiv 3 \pmod 4$) when n is even (resp. odd). Summing up, we conclude

$$S(\alpha) \equiv \begin{cases} (-1)^{n-1} \pmod 4 & \text{if} \quad P \equiv 1 \pmod 4, \\ (-1)^n \pmod 4 & \text{if} \quad P \equiv -1 \pmod 4. \end{cases}$$

Because $QR \equiv 0 \pmod 4$ and $PS - QR = -1$, we have $P \not\equiv S \pmod 4$, whereupon d necessarily satisfies $d \equiv 2 \pmod 4$ (note $x_p y_q - y_p x_q$ is odd). By (3.13) and the assumption $x_p \not\equiv x_q \pmod 2$, we have $R \equiv R', Q \equiv Q' \pmod 4$. Hence we have

$$\begin{pmatrix} P' & Q' \\ R' & S' \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

and

$$S(\beta) \equiv \begin{cases} (-1)^{m-1} \pmod 4 & \text{if} \quad P' \equiv 1 \pmod 4, \\ (-1)^m \pmod 4 & \text{if} \quad P' \equiv -1 \pmod 4. \end{cases}$$

Suppose $x_p y_q > y_p x_q$, *i.e.*, $\operatorname{sgn}(x_p y_q - y_p x_q) = 1$. Then by (3.14)

$$P - P' = -dy_p x_q \equiv 2y_p x_q \equiv 1 + (-1)^{x_p} \pmod 4$$

(recall the assumption $x_p \not\equiv x_q \pmod 2$). From the above, we have,

$$S(\alpha) + S(\beta) \equiv \begin{cases} (-1)^n + (-1)^m \equiv 1 + (-1)^{n-m} \pmod 4 & \text{if } x_p \text{ is odd}, \\ (-1)^n - (-1)^m \equiv 1 - (-1)^{n-m} \pmod 4 & \text{if } x_p \text{ is even}. \end{cases}$$

We can combine these into the congruence

$$S(\alpha) + S(\beta) \equiv 1 - (-1)^{x_p+n-m} \pmod 4.$$

When $x_p y_q < y_p x_q$, we have

$$P - P' = -dx_p y_q \equiv 2x_p y_q \equiv 1 - (-1)^{x_p} \pmod 4$$

and in the same way we obtain

$$S(\alpha) + S(\beta) \equiv 1 + (-1)^{x_p+n-m} \pmod 4.$$

We therefore have

$$S(\alpha) + S(\beta) \equiv 1 - \operatorname{sgn}(x_p y_q - y_p x_q)(-1)^{x_p+n-m} \pmod 4.$$

Since $n - m = (l(\alpha) - l(\beta))/2$, we have (3.8) and Theorem 1.2 is proved. □

Acknowledgement. The present work was partially supported by Grant-in-Aid for Scientific Research (B) No. 19340009.

REFERENCES

[1] G. Lachaud, *On real quadratic fields*, Bull. Amer. Math. Soc. (N.S.), **17** (1987), no. 2, 307–311.

[2] L. Rédei and H. Reichardt, *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math., **170** (1934), no. 1, 69–74.

[3] K. Suzuki, *Reduced quadratic forms and continued fraction expansions* (in Japanese), Master's thesis, Kyushu University, March 2008.

[4] T. Umeno, *On the 2-divisibility of calibers of real quadratic fields* (in Japanese), Master's thesis, Kyushu University, March 2006.

[5] D. B. Zagier, *Zetafunktionen und quadratische Körper*, University Text, Springer-Verlag, Berlin-New York, 1981. viii+144 pp.

M. KANEKO, FACULTY OF MATH., KYUSHU U., 744 MOTOOKA, NISHI-KU, FUKUOKA 819-0395, JAPAN
mkaneko@math.kyushu-u.ac.jp

K. MORI, URESHINO SPECIAL NEEDS EDUCATION SCHOOL, GOCHOUDAKOU 2877-1, SHIOTA, URESHINO, SAGA 849-1425, JAPAN
mori-keita@st.saga-ed.jp