BEHAVIOR OF THE RING CLASS NUMBERS OF A REAL QUADRATIC FIELD

RABIA QURESHI and TORU NAKAHARA

National University of Computer & Emerging Sciences[NUCES], Peshawar Campus,
160-Industrial Estate, Hayatabad, Khyber Pakhtunkhwa [K.P.K.],
The Islamic Republic of Pakistan.

E-mail: *rabiaqureshi1981@yahoo.com, toru.nakahara@nu.edu.pk,*

nakahara@ms.saga-u.ac.jp

ABSTRACT. Let K be a real quadratic field $Q(\sqrt{n})$ with an integer $n = df^2$ with the field discriminant d of K and $f \geqq 1$. Q. Mushtaq found an interesting phenomena that any totally negative number κ_0 with $\kappa_0 < 0$ and ${\kappa_0}^{\sigma} < 0$ belonging to the discriminant n, attains an ambiguous number κ_m with $\kappa_m \kappa_m^{\sigma} < 0$ after a finitely many actions ${\kappa_0}^{A_j}$ with $0 \leqq j \leqq m$ by modular transformations $A_j \in \mathrm{SL}_2^+(\boldsymbol{Z})$. Here σ denotes the embedding of K distinct from the identity. In this paper we give a new aspect for the process to reach an ambiguous number from a totally negative or totally positive number, by which the gap of the proof of Q. Mushtaq's Theorem is complemented. Next as an analogue of Gauß′ Genus Theory, we prove that the ring class number $h_+(df^2)$, coincides with the ambiguous class number belonging to the discriminant $n = df^2$ and it's behavior is unbounded, when f with suitable prime factors goes to infinity using the ring class number formula.

Mathematics Subject Classification(2010) 11R04, 11R11, 11R29

Keywords real quadratic field, continued fraction expansion, ring class number.

1 INTRODUCTION

For a positive integer $n = df^2$ with the field discriminant d of K and $f \geqq 1$, K be a real quadratic field $Q(\sqrt{n})$ over the rationals $\boldsymbol{Q}$. In [3], Q. Mushtaq gave an interesting characterization between a set of totally negative irrational numbers $\kappa_j (0 \leqq j)$ and an ambiguous number κ under the action of $\kappa_j = {\kappa_0}^{A_j}$ of κ_0 by A_j of the projective linear transformation group $\mathrm{PSL}_2^+(\boldsymbol{Z})$ over the ring $\boldsymbol{Z}$ of rational integers, which means that every totally negative quadratic irrational number κ_0 attains an ambiguous number κ_m by a finitely many steps of modular transformations $\kappa_j = {\kappa_0}^{A_j}$ where A_j is equal to $XY = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ or $XY^2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ with $\mathrm{X} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathrm{Y} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$, which are generators of $\mathrm{PSL}_2^+(\boldsymbol{Z})$ [cf.5].

It is called that a number κ is totally negative, totally positive or ambiguous if κ and its conjugate number κ^σ with the embedding $\sigma : \xi = x + y\sqrt{n} \mapsto \xi^\sigma = x + y(-\sqrt{n})$ of K, with $x, y \in \boldsymbol{Q}$ have the same negative sign, the same positive one or the distinct one, respectively. In [3], it is claimed that every totally negative quadratic irrational number κ_j attains an ambiguous number κ after a finite steps of *'forward'* transformations $\kappa_j = \kappa_{j-1}^{\mathrm{YX}}$ with $-1 < \kappa_{j-1} < 0$ $(1 \leqq j)$. However, using this transformation, the sequence $\{\kappa_j\}_{0 \leqq j}$ of totally negative numbers modulo suitable parallel transformation $\kappa_{j-1}^{(\mathrm{Y}^2\mathrm{X})^u}$ with $u \leqq 0$, is bounded but never reach to an ambiguous number (Remark 3.2). On the contrary, in Section 2 we define the *'backward'* transformations $\kappa_j = \kappa_{j-1}^{\mathrm{XY}^2}$ $(1 \leqq j)$ for a totally negative number κ_{j-1} with $-1 < \kappa_{j-1} < 0$. Then in Section 3 we prove that any totally negative number can attain an ambiguous number by two ways (Theorem 3.1, Theorem 3.3). Let d be the field discriminant of a real quadratic field $\boldsymbol{Q}(\sqrt{n})$ and Ω_f be the set of all the ambiguous numbers belonging to the discriminant $n = df^2$. Since the group $\mathrm{PSL}_2^+(\boldsymbol{Z})$ acts to the set Ω_f, Ω_f is classified by the action of $\mathrm{PSL}_2^+(\boldsymbol{Z})$, namely for $\alpha, \beta \in \Omega_f$, it is defined that α and β are equivalent if and only if there exists $Z \in \mathrm{PSL}_2^+(\boldsymbol{Z})$ such that $\beta = \alpha^Z$, which is written by $\alpha \sim \beta$. Then the number of the equivalence classes $\Omega_f / \sim$, which is denoted by h_{Ω_f} is finite, because the number of elements in Ω_f is finite (Remark 3.3). In Section 4 we will discuss the relation of the ring class number $h_+(df^2)$, the class number h_{Ω_f} of the ambiguous numbers belonging to the discriminant df^2 and the class number h_+(resp. h) in the narrow(resp. wide) sense. Finally we prove that the ring class number $h_+(df^2)$ is unbounded as $f = \prod_{j=1}^{r} q_j$ goes to the infinity together with suitable prime factors q_j $(1 \leqq j \leqq r)$.

2 Lemma

Let $\mathrm{SL}_2(Z)$ be the modular group $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in Z, \ ad - bc = \pm 1\right\}$ over Z and $\mathrm{SL}_2^+(Z)$ be the subgroup $\{A \in \mathrm{SL}_2(Z);\ det(A) = 1\}$ of $\mathrm{SL}_2(Z)$ and $\mathrm{PSL}_2{}^+(Z)$ denotes the projective linear transformation group $\mathrm{SL}_2^+(Z)/\{\pm E\} =< \mathrm{X}, \mathrm{Y} : \mathrm{X}^2 = \mathrm{Y}^3 = -E > /\{\pm E\}$ being generated by $\mathrm{X} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathrm{Y} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ with $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which is denoted by G[cf.4], where we identify $A \in \mathrm{SL}_2^+(Z)$ and its class $A\{\pm E\}$ in G. Also, we identify the action $\alpha^A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} a\alpha + b \\ c\alpha + d \end{pmatrix} = A\alpha$ for an irrational number $\alpha \in K$ by $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and the ratio $\dfrac{a\alpha + b}{c\alpha + d}$. Here we denote $A\begin{pmatrix} \xi \\ 1 \end{pmatrix}$ by $A\xi$ for $A \in G$ and $\xi \in K$.

The following lemma is fundamental for the interpretation of the theorem of Q. Mushtaq.

Lemma 2.1 *Let* $\kappa = \frac{a+\sqrt{n}}{c} \in K$ *with* $c > 0$ *and* $\mathrm{X} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\mathrm{Y} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in G$. *Then we have*

(1) *The action* $\mathrm{Y}^2\mathrm{X}$ *makes a 'backward' transformation on a totally negative number* κ *with* $-1 < \kappa < 0$, *that is* $\kappa^{\mathrm{XY}^2} < \kappa$ *holds for* $-1 < \kappa < 0$.

(2) *The action* XY *makes a 'forward' transformation on a totally positive number* κ *with* $0 < \kappa < 1$, *that is* $\kappa < \kappa^{\mathrm{YX}}$ *holds for* $0 < \kappa < 1$.

Proof. (1) For any totally negative number $\kappa \in K$, by a suitable parallel transformation we may assume that $-1 < \kappa < 0$. By the transformation $\mathrm{Y}^2\mathrm{X} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$, $\kappa^{\mathrm{XY}^2} = (\mathrm{Y}^2\mathrm{X})\kappa = \frac{\kappa}{\kappa+1} < 0$ holds. Thus $0 < \frac{\kappa}{\kappa^{\mathrm{XY}^2}} = \kappa + 1 < 1$. Then we have $\kappa^{\mathrm{XY}^2} < \kappa < 0 \quad (-1 < \kappa < 0)$, which means a '*backward*' transformation.

(2) For any totally positive number $\kappa \in K$, by a suitable parallel transformation we may assume that $0 < \kappa < 1$. By the transformation $\mathrm{XY} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$, $\kappa^{\mathrm{YX}} = (\mathrm{XY})\kappa = \frac{\kappa}{1-\kappa} > 0$ holds. Thus $0 < \frac{\kappa}{\kappa^{\mathrm{YX}}} = \frac{\kappa}{\frac{\kappa}{1-\kappa}} = 1 - \kappa < 1$. Then we have $0 < \kappa < \kappa^{\mathrm{YX}} \quad (0 < \kappa < 1)$, which means a '*forward*' transformation. □

3 Backward and forward transformations

In this section, we prove the following theorem which gives a complete complement to the proof of Theorem 5 in [3].

Theorem 3.1 *Let $\kappa_0 = \frac{a+\sqrt{n}}{c}$ with $c > 0$ be a quadratic irrational number belonging to the discriminant n. Then there exist two kinds of sequences $\{\kappa_j\}_{0\leq j}$ as follows;*

(1) If κ_0 is totally negative, then the sequence $\{\kappa_j\}$ attains an ambiguous number κ_m with totally negative numbers κ_j $(1 \leqq j \leqq m-1)$ uniquely determined by the 'backward' transformations $\kappa_j = \kappa_{j-1}^{\mathrm{XY}^2}$.

(2) The sequence $\{\kappa_j\}_{0\leq j}$ is totally negative(resp. positive) forever by the parallel translations $\kappa_j = \kappa_0^{(\mathrm{XY})^{-j}}$ (resp. $\kappa_j = \kappa_0^{(\mathrm{XY})^j}$) *according as $j \to \infty$.*

Proof. (1) Let $\kappa \in K$ such that $\kappa = \frac{a+\sqrt{n}}{c}$ be any totally negative number belonging to the discriminant n with $c > 0$ and $a < 0$. Here, without loss of generality we can assume that $c > 0$ since if $c < 0$, we take $\kappa^\sigma = \frac{a-\sqrt{n}}{c} = \frac{-a+\sqrt{n}}{-c}$ with $-c > 0$. Then $N_K(\kappa) = \frac{a^2-n}{c^2} > 0$ holds, and hence by $b = \frac{a^2-n}{c}$, $b > 0$, where for $\xi \in K$, $N_K(\xi)$ means the norm $\xi\xi^\sigma$ of a number with respect to K/Q. For $s = \|[\kappa]\|$, we have $-1 < \kappa^{(XY)^{s-1}} < 0$, which we denote by $\kappa_0 = \frac{a_0+\sqrt{n}}{c_0}$ with $a_0 = a$ and $c_0 = c$. Here, $[\alpha]$ denotes the largest integer not exceeding a real number α. Using Lemma 2.1(1), we have $\kappa_1 = \kappa_0^{XY^2} = \frac{\kappa_0}{\kappa_0+1} < \kappa_0$. Now $\kappa_1 = \frac{\frac{a_0+\sqrt{n}}{c_0}}{\frac{a_0+c_0+\sqrt{n}}{c_0}} = \frac{a_0+b+\sqrt{n}}{b+2a_0+c_0}$, which we put $\frac{a_1+\sqrt{n}}{c_1}$, where ${a_1}^2 - n = (b+a_0)^2 - ({a_0}^2 - bc_0) = b^2 + 2ba_0 + bc_0 = b(b+2a_0+c_0) = bc_1$ holds with $c_1 = b + 2a_0 + c_0$ and $a_1 = b + a_0$. We denote irrational numbers $\kappa_j = \kappa_0^{(XY^2)^j}$ by $\kappa_j = \frac{a_j+\sqrt{n}}{c_j}$ $(0 \leqq j)$. Then it follows $c_j = j^2b + 2ja_0 + c_0$ and $a_j = jb + a_0$ $(0 \leqq j)$. Put $c_j = f(j)$, then for $\widetilde{j} = \frac{-a_0-\sqrt{n}}{b}$, $f(\widetilde{j}) = 0$ holds. Put $m = [\widetilde{j}] + 1$. Since $\widetilde{j} \notin Q$, then it follows that $f(m-1) > 0$ and $f(m) < 0$. As $a_0 < 0$, namely at m steps later, we have $c_{m-1} > 0$ and $c_m < 0$. Since ${a_m}^2 - n = bc_m$, and hence ${a_m}^2 + b|c_m| = n$, we have $|a_m| < \sqrt{n}$ by $b > 0$. Thus $\kappa_m = \frac{a_m+\sqrt{n}}{c_m} < 0$ and ${\kappa_m}^\sigma = \frac{a_m-\sqrt{n}}{c_m} > 0$. Therefore we attain to an ambiguous number κ_m from any totally negative numbers κ_j after a finitely many steps of '*backward*' transformations $\kappa_j^{XY^2}$ $(0 \leqq j \leqq m-1)$, which are uniquely determined by the initial value κ_0.

(2) Let κ_0 be a totally negative (resp. positive) number in K, then the sequence $\{\kappa_j\}_{0 \leqq j}$ is totally negative(resp. positive) forever by the negative parallel translations $\kappa_j = \kappa_0^{(XY)^{-j}} = \kappa_0 - j$ (resp. positive ones $\kappa_j = \kappa_0^{(XY)^j} = \kappa_0 + j$). □

Remark 3.2 Let a totally negative number κ_0 and the '*forward*' transformation κ_0^{YX} with $-1 < \kappa_0 < 0$ be the same as in the Theorem 5 in [3]. Then

$0 > \kappa_0^{YX} = (XY)\kappa_0 = \frac{-\kappa_0}{\kappa_0-1}$. By $\frac{|\kappa_0|}{\left|\frac{-\kappa_0}{\kappa_0-1}\right|} = \frac{|\kappa_0-1|}{1} > 1$, we have $\kappa_0 < \frac{-\kappa_0}{\kappa_0-1}$ and $-1 < \frac{-\kappa_0}{\kappa_0-1} < 0$. Put $\kappa_1 = \kappa_0^{YX}$. Then by $1 < \frac{\kappa_0}{\kappa_1} = 1 - \kappa_0 < 2$, we have $\kappa_1 > \kappa_0$ and $\frac{1}{2} < \frac{1}{1-\kappa_0} < 1$. Then it holds that $0 > \frac{1}{2}\kappa_0 > \frac{\kappa_0}{1-\kappa_0} = \kappa_1$ and $\frac{{\kappa_0}^\sigma}{1-{\kappa_0}^\sigma} = {\kappa_1}^\sigma < 0$ then κ_1 is totally negative. By a suitable parallel transformation $\kappa_1^{(Y^2X)^u}$ with $u \leqq 0$, $-1 < \kappa_1^{(Y^2X)^u} < 0$ holds, whose number is denoted by κ_1 again. Put $\kappa_2 = \kappa_1^{YX}$. Then we have $\frac{1}{2}\kappa_1 > \kappa_2$ and hence for $n \geqq 1$ we obtain $0 > \frac{1}{2}\kappa_{n-1} > \kappa_n$. It holds that $\kappa_{n-1}^{YX} < 0$ as $n \to \infty$ and κ_n is totally negative. Thus we have the sequence $\{\kappa_j\}_{0 \leqq j}$ with an upper bound 0, thereby the sequence $\{\kappa_j\}_{0 \leqq j}$ never reaches an ambiguous number.

However, in the next theorem we show that any totally positive or negative number α_0 attains an ambiguous number using the alternative blocks of parallel and *'forward'* translations by way of the continued fraction expansion of α_0, whose method is based on [6].

Next theorem asserts that any quadratic irrational number α_0 attains a reduced number, and hence an ambiguous number after an even steps of continued fraction expansions of α.

Theorem 3.3 *Let α_0 be any quadratic irrational number, then α_0 attains an ambiguous number α_ℓ for $2 \mid \ell$ or $\alpha_{\ell+1}$ for $2 \nmid \ell$ by the continued fraction expansion,*

$$\alpha_0 = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots + \cfrac{1}{k_{j-1} + \frac{1}{\alpha_j}}}}} \quad \textit{with } \kappa_{j-1} = \begin{cases} \kappa_{\ell-1}, & 2 \mid \ell \\ \kappa_\ell, & 2 \nmid \ell \end{cases} \quad \textit{of } \alpha_0,$$

namely it holds that

$$\begin{aligned} \alpha_\ell &= (XY)^{k_{\ell-1}}(XY^2)^{k_{\ell-2}} \cdots (XY)^{k_1}(XY^2)^{k_0}\alpha_0 \\ &= \alpha_0^{(Y^2X)^{k_0}(YX)^{k_1} \cdots (Y^2X)^{k_{\ell-2}}(YX)^{k_{\ell-1}}} \quad \textit{for } 2 \mid \ell \end{aligned}$$

and

$$\begin{aligned} \alpha_{\ell+1} &= (XY)^{k_\ell}(XY^2)^{k_{\ell-1}} \cdots (XY)^{k_1}(XY^2)^{k_0}\alpha_0 \\ &= \alpha_0^{(Y^2X)^{k_0}(YX)^{k_1} \cdots (Y^2X)^{k_{\ell-1}}(YX)^{k_\ell}} \quad \textit{for } 2 \nmid \ell. \end{aligned}$$

Proof. Let α_0 be any quadratic irrational number. Then by the continued fraction expansion of α_0, we have $\alpha_0 = k_0 + \frac{1}{\alpha_1}$, where we identify $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and the ratio $\frac{\alpha}{\beta}$ of components α, β. It holds that

$\begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix} = \begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ 1 \end{pmatrix}$ and hence $\begin{pmatrix} \alpha_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix}$.

Put $M_0 = \begin{pmatrix} 0 & 1 \\ 1 & -k_0 \end{pmatrix}$, then $M_0 \notin \mathrm{SL}_2^+(\boldsymbol{Z})$. Next for $\alpha_1 = k_1 + \frac{1}{\alpha_2}$, put $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & -k_1 \end{pmatrix}$ with $M_1 \notin \mathrm{SL}_2^+(\boldsymbol{Z})$. By $|M_1M_0| = |M_1||M_0| = 1$, $M_1M_0 \in \mathrm{SL}_2^+(\boldsymbol{Z})$ holds. We have

$$\begin{pmatrix} \alpha_2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -k_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -k_0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -k_0 \\ -k_1 & 1 + k_1k_0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix} = \frac{\alpha_0 - k_0}{-k_1\alpha_0 + (1 + k_1k_0)} = M_1M_0\alpha_0. \quad (3.1)$$

On the other hand, we have by $\mathrm{XY}^2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$, $(\mathrm{XY}^2)^{k_0} = \begin{pmatrix} -1 & k_0 \\ 0 & -1 \end{pmatrix}$ and by

$\mathrm{XY} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$, $(\mathrm{XY})^{k_1} = \begin{pmatrix} -1 & 0 \\ k_1 & -1 \end{pmatrix}$ for any $k_0, k_1 \in \boldsymbol{Z}$. Then, we have

$$(\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0} = \begin{pmatrix} -1 & 0 \\ k_1 & -1 \end{pmatrix} \begin{pmatrix} -1 & k_0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -k_0 \\ -k_1 & k_1k_0 + 1 \end{pmatrix} \quad (3.2)$$

By (3.1) and (3.2), we obtain $M_1M_0 = (\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0}$. Continuing in this way on $M_j = \begin{pmatrix} 0 & 1 \\ 1 & -k_j \end{pmatrix}$, we have for $2 \mid \ell$,

$M_{\ell-1}M_{\ell-2} \cdots M_1M_0 = (\mathrm{XY})^{k_{\ell-1}}(\mathrm{XY}^2)^{k_{\ell-2}} \cdots (\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0}$.

If $|M_{\ell-1}M_{\ell-2} \cdots M_1M_0| = (-1)^\ell = -1$, then we can continue one step more by taking M_ℓ, so $M_\ell M_{\ell-1}M_{\ell-2} \cdots M_1M_0 \in \mathrm{SL}_2^+(\boldsymbol{Z})$ with $|M_\ell M_{\ell-1}M_{\ell-2} \cdots M_1M_0| = 1$ and

$M_\ell M_{\ell-1} \cdots M_1M_0 = (\mathrm{XY})^{k_\ell}(\mathrm{XY}^2)^{k_{\ell-1}} \cdots (\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0}$. In fact, if the reduced class $\mathfrak{R}$ containing $\alpha_{\ell-1}$ has at least 2 reduced numbers, there exists $\alpha_\ell = M_\ell\alpha_{\ell-1}$ by the continued fraction expansion, and if $\mathfrak{R}$ has only one reduced number, there exists the transformation $M_\ell = \begin{pmatrix} 0 & 1 \\ 1 & -[\alpha_\ell] \end{pmatrix}$ such that $\alpha_{\ell+1} = M_\ell\alpha_\ell$ which means the double period of the continued fraction expansion of α_ℓ. Here $[\alpha]$ denotes the largest integer less than or equal to α for a real number α. Thus we attain an ambiguous number;

$$\alpha_\ell = (\mathrm{XY})^{k_{\ell-1}}(\mathrm{XY}^2)^{k_{\ell-2}} \cdots (\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0}\,\alpha_0 \text{ if } 2 \mid \ell,$$

and

$$\alpha_{\ell+1} = (\mathrm{XY})^{k_\ell}(\mathrm{XY}^2)^{k_{\ell-1}} \cdots (\mathrm{XY})^{k_1}(\mathrm{XY}^2)^{k_0}\,\alpha_0 \text{ if } 2 \nmid \ell. \qquad \square$$

Remark 3.4 Let Ω_f be the set of ambiguous numbers belonging to the discriminant $n = f^2d$ in the ring $Z_f = \boldsymbol{Z}[1, f\omega]$, then $\sharp\left\{\frac{a+f\sqrt{d}}{c} \in \Omega_f\right\} \leqq 2f^2d(1+f\sqrt{d})^2$. Here for a set S, $\sharp S$ denotes the number of the elements in S. Because $\alpha = \frac{a+f\sqrt{d}}{c}$ be an ambiguous number, then by $N_K(\alpha) = \frac{a^2-f^2d}{c^2} = \frac{b}{c} < 0$, and hence $|a| < f\sqrt{d}$ holds, which implies that $\sharp\{a\} < 2f\sqrt{d}+1$. Since $bc = a^2 - f^2d$, the choices for $c > 0$ among the factors of $-f^2d, 1-f^2d, \cdots, [\sqrt{f^2d}] - f^2d$ are at most $f^2d(1+f\sqrt{d})$. So $\{(a,b,c)\} \leqq (2f\sqrt{d}+1)\cdot f^2d\cdot(1+f\sqrt{d}) < 2f^2d\cdot(1+f\sqrt{d})^2$, namely for a real quadratic field $\boldsymbol{Q}(\sqrt{n})$, the number of the ambiguous numbers belonging to the discriminant f^2d is finite.

Proposition 3.5 *Let $\mathfrak{R}_f$ be a reduced class belonging to the discriminant df^2 of a real quadratic field $K = \boldsymbol{Q}(\sqrt{n})$ with an integer $n = df^2$ and ε_f denotes the fundamental unit in $Z_f = \boldsymbol{Z}[1, f\omega]$, $\omega = \frac{d+\sqrt{d}}{2}$ of K. Then it holds that*

$$\sharp\mathfrak{R}_f = \begin{cases} 1 \,(\mathrm{mod}\ 2) \text{ if } N_K(\varepsilon_f) = -1, \\ 0 \,(\mathrm{mod}\ 2) \text{ if } N_K(\varepsilon_f) = 1. \end{cases}$$

Proof. Let $\alpha \in K$ be a reduced number belonging to the discriminant df^2 with $\alpha > 1$, $-1 < \alpha^\sigma < 0$. Then there exists a transformation M_j such that $\alpha = M_rM_{r-1}\cdots M_1\alpha$, where the transformation $M_rM_{r-1}\cdots M_1$ corresponds to the continued fraction expansion of α with length r. By
$M_rM_{r-1}\cdots M_1\alpha = \begin{pmatrix} P_r & P_{r-1} \\ Q_r & Q_{r-1} \end{pmatrix}\begin{pmatrix} \alpha \\ 1 \end{pmatrix}$
$= A\alpha = \frac{P_r\alpha+P_{r-1}}{Q_r\alpha+Q_{r-1}} \quad P_r, P_{r-1}, Q_r, Q_{r-1} \in \boldsymbol{Z}$ with $A = \begin{pmatrix} P_r & P_{r-1} \\ Q_r & Q_{r-1} \end{pmatrix}$, the denominator $Q_r\alpha + Q_{r-1}$ gives the fundamental unit ε_1 of K [cf.4]. As $\varepsilon_f \in Z_f = \boldsymbol{Z}[1, f\omega]$ with $\omega = \frac{d+\sqrt{d}}{2}$ is an algebraic number in K, there exists $f(x) = x^2 - Tr(A)x + N(A)$ such that $f(\varepsilon_f) = 0$, where $Tr(A) = P_r + Q_{r-1}$ and $N(A) = det(A)$. By $N_K(\varepsilon_f) = \varepsilon_f{\varepsilon_f}^\sigma = N(A) = det(A)$ and

$(-1)^r = det(M_r M_{r-1} \cdots M_1) = det(A)$, if $N_K(\varepsilon_f) = +1$, then $r \equiv 0 \pmod 2$. If $N_K(\varepsilon_f) = -1$, then $r \equiv 1 \pmod 2$. □

Remark 3.6 In [3], Q. Mushtaq showed an ambiguous number whose length of the continued fraction expansion is equals to 6 for $n = 473$ with $d = 2^2 \cdot 473$. Let g be the transformation $(XY)^2(XY^2)^2(XY)(XY^2)^2(XY)^3(XY^2)^2 \in SL_2^+(Z)$. Then by $g\kappa = \kappa$, κ satisfies the quadratic equation $64\kappa^2 - 120\kappa - 62 = 0$ instead of $62\kappa^2 + 120\kappa - 64 = 0$ in [3] whose solution is κ^{-1}. Thus a fixed point $\kappa = \frac{30+\sqrt{1892}}{32} = \frac{15+\sqrt{473}}{16}$ by g satisfies $64\kappa^2 - 120\kappa - 62 = 0$.

4 BEHAVIOR OF THE RING CLASS NUMBERS

First we prepare the ring class number formula. Let $h_+(d)$ (resp. $h(d)$) be the class number in the narrow (resp. wide) sense of $K = Q(\sqrt{n})$. It is known that $h_+(d) = 2h(d)$ if $N_K(\varepsilon) = +1$ with the fundamental unit ε of K and $h_+(d) = h(d)$ if $N_K(\varepsilon) = -1$ or K is an imaginary quadratic field. Let Z_f be the ring $Z[1, f\omega]$ of conductor f with $\omega = \frac{d+\sqrt{d}}{2}$ in the ring Z_K of integers in K. By the definition of ring class number $h_+(df^2)$ (resp. $h(df^2)$) coincides with the order $\sharp(A_f/P_f)$ of the factor group A_f/P_f for the fractional ideal group A_f and the principal ideal subgroup P_f of A_f in the ring $Z_f = Z[1, f\omega]$ under the equivalence relation $\mathfrak{A} \sim \mathfrak{B}$ for $\mathfrak{A}, \mathfrak{B} \in A_f$ if there exists $\gamma \in Z_f$ such that $\mathfrak{B} = \gamma\mathfrak{A}$ with $N_K(\gamma) > 0$ (resp. $N_K(\gamma) \neq 0$.)

Theorem 4.1 [1] *Let $K = Q(\sqrt{n})$ be a quadratic field with the field discriminant d and the conductor f. Then the ring class number formula holds;*

$$\begin{cases} h_+(df^2) = h_+(d) f \prod_{p|f}(1 - \frac{(\frac{d}{p})}{p})/E_+ \\ h(df^2) = h(d) f \prod_{p|f}(1 - \frac{(\frac{d}{p})}{p})/E \end{cases}$$

with the products over the primes $p|f$. Here, if $d < 0$, $h(d) = h^+(d)$ and $E_+ = 1$ holds, except $E_+ = 2$ or 3 for $d = -4$ or -3, respectively. If $d > 0$, E_+ (resp. *E*) *denotes the exponent of the least power $\varepsilon_+^{E_+}$ of the totally positive fundamental unit ε_+ such that $\varepsilon_+^{E_+}$ (resp. the least one ε^E of the fundamental unit ε) belongs to the ring $Z_f = Z[1, f\omega]$ with $\omega = \frac{d+\sqrt{d}}{2}$ and $(\frac{d}{p})$ denotes the Kronecker symbol. Here it holds that for the unit ε_+, $\varepsilon_+ = \varepsilon$, if $N_K(\varepsilon) = +1$ and $\varepsilon_+ = \varepsilon^2$, if $N_K(\varepsilon) = -1$.*

Next we claim that the ambiguous class number is equal to the ring class number of conductor $f \geqq 1$. For the case of the conductor $f = 1$, on the class number $h(d)$ in the wide sense and $h_+(d)$ in the narrow sense, the relation

$$h(d) = \begin{cases} h_+(d), & \text{if} \quad d < 0 \quad \text{or} \quad N_K(\varepsilon) = -1, \\ \frac{h_+(d)}{2}, & \text{if} \quad d > 0 \quad \text{and} \quad N_K(\varepsilon) = +1. \end{cases}$$

is well known fact (see for example L.K. Hua [2] Chap. 26). For the case of $f \geqq 1$, the relation above is slightly generalized as follows.

Corollary 1 *Being the same notation as above, it holds that for $f \geqq 1$*

$$h_{\Omega_f} = h_+(d \cdot f^2)$$

and

$$h_{\Omega_f} \equiv \begin{cases} 0 \,(\mathrm{mod}\; h(d)), & \text{if} \quad N_K(\varepsilon^E) = -1, \\ 0 \,(\mathrm{mod}\; 2h(d)), & \text{if} \quad N_K(\varepsilon^E) = +1. \end{cases}$$

Proof. We denote the ambiguous class number h_{Ω_f} by k and the ring class number $h_+(df^2)$ in the narrow sense by m. Then we have $\Omega_f = \bigcup_{j=1}^k \Omega_{\alpha_j}$ such that $\Omega_{\alpha_i} \bigcap \Omega_{\alpha_j} = \emptyset$, where Ω_{α_j} denotes the ambiguous class with α_j, and $\mathfrak{R}_{df^2} = \bigcup_{j=1}^m \mathfrak{R}_{\beta_j}$ such that $\mathfrak{R}_{\beta_i} \bigcap \mathfrak{R}_{\beta_j} = \emptyset$, here $\mathfrak{R}_{\beta_j}$ denotes the reduced class in the narrow sence with β_j in the ring $Z_f = Z[1, f\omega]$. Let $\mathfrak{R}_j$ be a reduced class $\{\gamma = \gamma_1, \cdots, \gamma_s\}$ of length s. Then

$h_+(df^2) = 2m \leqq k = h_{\Omega_f}$ holds. If s is even, then there exists just two ambiguous classes; $\Omega_{\gamma_1} = \{\gamma_1, \gamma_3, \cdots, \gamma_{s-1}\}$ and $\Omega_{\gamma_2} = \{\gamma_2, \gamma_4, \cdots, \gamma_s\}$. If s is odd, $\mathfrak{R}_{\gamma_1} = \{\gamma = \gamma_1, \gamma_3, \cdots, \gamma_s, \gamma_2, \gamma_4, \cdots, \gamma_{s-1}\} = \Omega_{\gamma_1}$. Here, if γ_1 has a continued fraction expansion $[\bar{c}]$ of period length 1, then it holds that for $\Omega_{\gamma_1} = \{\gamma_1\}$ and $\Omega_{\gamma_3} = \{\gamma_1, \gamma_3\}$, $\Omega_{\gamma_1} = \Omega_{\gamma_3}$ holds because of $\gamma_1 = \gamma_2 = \gamma_3$. Then $h_+(df^2) = m \leqq k = h_{\Omega_f}$ holds. Conversely by Theorem 3.3, for any ambiguous class Ω_α, since α attains a reduced number β_α after an even steps later of continued fraction expansion, Ω_α corresponds to $\mathfrak{R}_{\beta_\alpha}$. Therefore we obtain $h_+(df^2) = h_{\Omega_f}$. The congruence relation follows from Theorem 4.1. □

Experiment 1 Let $d = 4 \cdot 7$ for $n = 7$. The fundamental unit ε is equal to $-34 + 3\omega$ for $\omega = \frac{28+\sqrt{28}}{2}$ with $N_d(\varepsilon) = +1$. For $f = 1$, the ambiguous class Ω_1 contains $14 + 14$ ambiguous numbers and the reduced class $\mathfrak{R}_d$ 4 reduced numbers. Then $h_{\Omega_1} = h_+(d) = 2h(d) = 2$ holds with $E_+ = 1$ by $\varepsilon \in Z_1$. Here $\eta_1 + \eta_2 + \cdots + \eta_r$ means that a disjoint union of r ambiguous/reduced classes with η_j ambiguous/reduced numbers contained in the jth class. For $f = 2$, $\Omega_2 = 36 + 36$ and $\mathfrak{R}_{d \cdot 2^2} = 4$. Thus $h_{\Omega_2} = h_+(d \cdot 2^2) = h_+(d) = 2h(d) = 2$ holds with $E_+ = 2$ by $\varepsilon \notin Z_2$ and $\varepsilon^2 = -545 + 48\omega \in Z_2$ whose relation satisfied by Proposition 4.2 (1). For $f = 3$, $\Omega_3 = 30 + 30 + 18 + 18$ and $\mathfrak{R}_{d \cdot 3^2} = 2 + 2$. In fact, by Corollary 1, $h_{\Omega_3} = h_+(d \cdot 3^2) = 2h_+(d) \equiv 0 \pmod{2h(d)}$ holds with $E_+ = 1$ by $\varepsilon \in Z_3$. For $f = 6$, $\Omega_6 = 76 + 76 + 28 + 28$ and $\mathfrak{R}_{d \cdot 6^2} = 4 + 6$. Then it holds $h_{\Omega_6} = h_+(d \cdot 6^2) = 2h_+(d) = 4h(d)$. In fact, $h_{\Omega_6} = h_+(d \cdot 6^2) \equiv 0 \pmod{2h(d)}$ holds with $E_+ = 2$ by $\varepsilon \notin Z_6$ and $\varepsilon^2 \in Z_6$.

Experiment 2 Let $d = 37$. The fundamental unit ε is equal to $-31 + 2\omega$ for $\omega = \frac{37+\sqrt{37}}{2}$ with $N_d(\varepsilon) = -1$ and totally positive fundamental unit ε_+ is equal to $\varepsilon^2 = -371 + 24\omega$ Now for $f = 1$, the ambiguous class Ω_1 contains 28 ambiguous numbers and the reduced class $\mathfrak{R}_d$ 3 reduced numbers. Then

$h_{\Omega_1} = h_+(d) = h(d) = 1$. with $E_+ = 1$ by $\varepsilon_+ \in Z_1$. For $f = 2$, Ω_2 has $48 + 24 + 24$ ambiguous numbers and $\mathfrak{R}_{d\cdot 2^2}$ $1 + 3 + 3$ reduced numbers. Thus $h_{\Omega_2} = h_+(d\cdot 2^2) = 3h_+(d)$, with $E_+ = 1$ as $\varepsilon_+ \in Z_2$ whose relation satisfied by Proposition 4.2 (3′). For $f = 3$, $\Omega_3 = 44 + 44$ and $\mathfrak{R}_{d\cdot 3^2} = 6$. In fact, by Colloraly 1, $h_{\Omega_3} = h_+(d\cdot 3^2) = 2h_+(d)$ holds with $E_+ = 1$ by $\varepsilon_+ \in Z_3$. For $f = 6$, $\Omega_6 = 80+80+32+32+32+32$ and $\mathfrak{R}_{d\cdot 6^2} = 4+4+2$. $h_{\Omega_6} = h_+(d\cdot 6^2) = 6h_+(d)$. In fact, $h_{\Omega_6} = h_+(d\cdot 6^2) \equiv 0 \pmod{2h(d)}$ holds with $E_+ = 1$ by $\varepsilon_+ \in Z_6$.

For the case of $f = 2$, we have an explicit relation of the ring class number $h_+(d\cdot 2^2)$ and the class number $h_+(d)$.

Proposition 4.2 *Let K and $\varepsilon > 1$ be a real quadratic field $Q(\sqrt{d})$ with $d \equiv 0, 1 \pmod 4$ of the field discriminant d and the fundamental unit, respectively. Let $h_+(d\cdot 2^2)$ be the ring class number for $f = 2$ and $h_+(d)$ the class number in the narrow sense of K. Then it holds that*

$$\begin{array}{lll}
(1) & h_+(d\cdot 2^2) = h_+(d) & \text{if} \quad 2 \mid d \text{ and } \varepsilon \notin Z_2 \\
(1') & h_+(d\cdot 2^2) = 2h_+(d) & \text{if} \quad 2 \mid d \text{ and } \varepsilon \in Z_2 \\
(2) & h_+(d\cdot 2^2) = h_+(d) & \text{if} \quad d \equiv 1 \pmod 8 \\
(3) & h_+(d\cdot 2^2) = h_+(d) & \text{if} \quad d \equiv 5 \pmod 8 \text{ and } \varepsilon \notin Z_2 \\
(3') & h_+(d\cdot 2^2) = 3h_+(d) & \text{if} \quad d \equiv 5 \pmod 8 \text{ and } \varepsilon \in Z_2.
\end{array}$$

Proof. If $d \equiv 0 \pmod 4$, then

$$h_+(d\cdot 2^2) = h_+(d)2\Big(1 - \frac{(\frac{d}{2})}{2}\Big)/E_+ = h_+(d)\cdot 2\cdot(1-0)/2 = h_+(d)$$

holds. Because the value of Kronecker symbol is equal to 0 and on the fundamental unit $\varepsilon = u + v\sqrt{d} > 1$, if $2|v$, then $E_+ = 1$ and otherwise, $E_+ = 2$. Then $h_+(d\cdot 2^2) = \begin{cases} h_+(d)\cdot 2\cdot 1/1 = 2h_+(d) \\ h_+(d)\cdot 2\cdot 1/2 = h_+(d) \end{cases}$ Next, if $d \equiv 1 \pmod 4$, it is enough to prove the relation of the ring class number and the class number in the narrow sense. Then we have two cases; (a) $d \equiv 1 \pmod 8$ and (b) $d \equiv 5 \pmod 8$. In the case (a), if $\varepsilon = \frac{u+v\sqrt{d}}{2}$ with $u, v \in Z$, $2 \nmid uv$, then $\pm 4 = 4N_K(\varepsilon) = u^2 - v^2 d = 1 - 1 \equiv 0 \pmod 8$

which is a contradiction. Then $\varepsilon = u + v\sqrt{d}$ holds. If $2 \mid v$, then $4N_K(\varepsilon) = u^2 - v^2d = u^2 - 4 \equiv -3 \not\equiv \pm 1 \pmod 8$ which is a contradiction. So $2 \nmid v$, and hence $\varepsilon = u + v\sqrt{d} = u - vd + 2v\omega \in Z_2$ with $\omega = \frac{d+\sqrt{d}}{2}$. Thus $h_+(d \cdot 2^2) = h_+(d)2\Big(1 - \frac{(\frac{d}{2})}{2}\Big)/1 = h_+(d)2 \cdot \frac{2-1}{2}/1 = h_+(d)$. In the case (b), for the fundamental unit $\varepsilon = \frac{u+v\sqrt{d}}{2} > 1$, $\pm 4 = 4N_K(\varepsilon) = u^2 - v^2d \equiv u^2 - v^2 5 \pmod 8$ holds. If $(u,v) = 1$, and hence $2 \nmid u$ and $2 \nmid v$, then $\varepsilon^2 = \frac{\frac{u^2+v^2d}{2}+uv\sqrt{d}}{2} \notin Z_2$ because of $2 \nmid uv$. For $\varepsilon^3 = \frac{u_3+v_3\sqrt{d}}{2}$, we have $4u_3 = u^3 + uv^2d + 2v^2ud \equiv 1 \cdot u + 5 \cdot u + 10 \cdot u \equiv 0 \pmod 8$ and $4v_3 = u^2v + v^3d + 2u^2v \equiv v + 5 \cdot v + 2 \cdot v \equiv 0 \pmod 8$. Then $\varepsilon^3 \in Z_2$. If $(u,v) = 2$, then for $u = 2u'$ and $v = 2v'$, we have $\varepsilon = u' - v'd + 2\omega \in Z_2 = Z[1, 2\omega]$ and hence, $\varepsilon \in Z_2$ holds. By the value $\left(\frac{d}{2}\right) = -1$ of Kronecker symbol, we have

$$h_+(d \cdot 2^2) = h_+(d)2\Big(1 - \frac{(-1)}{2}\Big)/E_+ = h_+(d) \cdot 3/E_+.$$

Since $E_+ = 1$ or 3, we obtain $h_+(d \cdot 2^2) = \begin{cases} h_+(d) \text{ if } \varepsilon \notin Z_2 \\ 3h_+(d) \text{ if } \varepsilon \in Z_2 \end{cases}$ □

Finally we show that the ring class number $h_+(df^2)$ is unbounded, when f runs together with suitable prime factors. The behavior of the ratio $h_+(df^2)/h_+(d)$ is similar to Gauß' Genus Theory; $2^{t-1}|h_+(d)$ for the number t of prime discriminant which divide the field discriminants d.

Theorem 4.3 *Let K be a quadratic field with the field discriminant $d \equiv 1 \pmod 8$. Let $f = \prod_{j=1}^{r} q_j$ be the canonical decomposition of f such that $\left(\frac{d}{q_j}\right) = 1$ and $(s_1 \cdots s_{j-1}, s_j) = 1$ for $q_j = 2s_j + 1$ $(2 \leqq j \leqq r)$ hold. Then for the ratio of the ring class number $h_+(df^2)$ and the class number $h_+(d)$ in the narrow sense, it holds that*

$$2^{r-1} \,\Big|\, \frac{h_+(df^2)}{h_+(d)}.$$

Proof. Let $\prod_{j=1}^{t} p_j$ be the canonical decomposition of the prime factors of the discriminant d. Since the half of prime numbers in the set P of all the prime numbers are completely decomposed in $K = \boldsymbol{Q}(\sqrt{n})$ except for t (resp. $t+1$) ramified primes when $n \equiv 1 \pmod{4}$ (resp. $n \equiv 3 \pmod{4}$,) we select such a prime factor q of f, we use the ring class number formula, $h_+(dq^2) = h_+(d)q\left(1 - \left(\frac{d}{q}\right)/q\right)/E_+$. By the choice of a divisor q of f, we have $q \cong \mathfrak{Q}\mathfrak{Q}^{\sigma}$, where $\mathfrak{Q}$ is a prime divisor of q in K and for a number α and an ideal $\mathfrak{A}$ of K, $\alpha \cong \mathfrak{A}$ means that the both sides are equal to each other as ideals. Then it holds that
$\mathrm{N}_K((q)) = q^2 = \mathrm{N}_K(\mathfrak{Q})\mathrm{N}_K(\mathfrak{Q}^{\sigma}) = \mathrm{N}_K(\mathfrak{Q})^2$, and hence $q = \mathrm{N}_K(\mathfrak{Q})$, where N_K denotes the norm of an ideal with respect to K over $\boldsymbol{Q}$, and (α) denotes the principal ideal αZ_K for an integer α in K. Thus for any residue class $\overline{\varepsilon} = \varepsilon + \mathfrak{Q} \in Z_K/\mathfrak{Q}^{\times}$, $\overline{\varepsilon}^{\mathrm{N}_K(\mathfrak{Q})-1} = \overline{1}$ holds, where $Z_K/\mathfrak{Q}^{\times}$ means the multiplicative group of the residue class field $Z_K/\mathfrak{Q}$, which is isomorphic to $\boldsymbol{Z}/q\boldsymbol{Z}$. Then $\varepsilon^{q-1+1} \equiv \varepsilon \pmod{\mathfrak{Q}}$. Also $\varepsilon^{\mathrm{N}_K(\mathfrak{Q}^{\sigma})} \equiv \varepsilon \pmod{\mathfrak{Q}^{\sigma}}$, namely $\varepsilon^{q} \equiv \varepsilon \pmod{\mathfrak{Q}^{\sigma}}$ holds. Then by $(\mathfrak{Q}, \mathfrak{Q}^{\sigma}) = 1$, $(\varepsilon, \mathfrak{Q}\mathfrak{Q}^{\sigma}) = 1$ and $\mathfrak{Q}\mathfrak{Q}^{\sigma} \cong q$, $\varepsilon^{q-1} \equiv 1 \pmod{q}$ follows. Then, we obtain
$\frac{u_{q-1}+v_{q-1}\sqrt{d}}{2} \equiv 1 \pmod{q}$, which implies $\varepsilon^{q-1} \in Z_q$. Since $d \equiv 1 \pmod{8}$. Then for the fundamental unit $\varepsilon = \frac{u+v\sqrt{d}}{2}$ of K, if $2 \nmid v$, then
$\pm 4 = u^2 - v^2 d \equiv \left\{ \begin{matrix} 0 \\ 4 \\ 1 \end{matrix} \right\} - 1 \cdot 1 \equiv \left\{ \begin{matrix} -1 \\ 3 \\ 0 \end{matrix} \right\} \pmod{8}$ holds, which is a contradiction. Then by $\varepsilon^1 = u + v\sqrt{d} = u - v + 2v\omega \in Z_f = \boldsymbol{Z}[1, f\omega]$, $E_+ | s_1$ holds for $q_1 = 2s_1 + 1$. Let $q_j = 2s_j \pm 1$ be primes with an odd $s_j = 2t_j \prod_{i=1}^{j-1} s_i + 1$ using Dirichlet's Theorem on Arithmetic progression. Then the choice of prime numbers q_j of f,
$\mathrm{lcm}[\varphi(q_1), \cdots, \varphi(q_r)] = 2\prod_{j=1}^{r} s_j = \frac{1}{2^{r-1}} \prod_{j=1}^{r} \varphi(s_j)$ follows, where φ denotes the Euler function. Then by $E_+ | \mathrm{lcm}[\varphi(q_1), \cdots, \varphi(q_r)]$,
$h^+(d)f\left(\prod_{j=1}^{r} \frac{q_j - 1}{q_j}\right) \frac{2^{r-1}}{\prod_{j=1}^{r} \varphi(q_j)} | h_+(df^2)$, that is, $2^{r-1} \left| \frac{h_+(df^2)}{h_+(d)} \right.$. Therefore

we furnished the proof. □

Acknowledgements The authors would like to express their gratitude to a referee for her/his valuable notices in section 4 ,
Prof. Syed Husnine[NUCES, Lahore Campus] and Ms. Aisha AHMAD[Univ. of Peshawar] his comment and her computation on the ambiguous and the reduced numbers in $Q(\sqrt{n})$ by C++ program, respectively. The first author is supported by PhD scholar fund from the Ministry of Education and Research, the Islamic Republic of Pakistan, through PN II-Ideas, Grant No 17-5-6(Ps-088)/HEC/Sch/2010. The second author is partially supported by grant (♯20540019) from the Japan Society for the Promotion of Science.

References

[1] H. Cohn, *Introduction to the construction of class fields*, Dover Publications, INC. New York, 1994.

[2] L. K. Hua, *Introduction to number theory*, English translation by P.Shiu, Springer-Verlag, Berlin· Heidelberg· New York, 1982.

[3] Q. Mushtaq, *Modular group acting on real quadratic fields* , Bull. Austral. Math. Soc., **37** (1988), 303-309.

[4] T. Ono, *An Introduction to Algebraic Number Theory*, Plenum Press New York and London, 1990.

[5] J. P. Serre, *A cource in arthemetic*, Springer-Verlag, Berlin· Heidelberg· New York, 1973,
French original edition; *Cours d' Arthmétique*, press Universitaire de France, Paris, 1970-1977.

[6] D. Tomonou, *Modular group which acts on real quadratic fields*, (In Japanese) 24 pages, M. Phil thesis, Saga University, Japan, 2006.