Yamamoto, Y.
Osaka, J. Math.
8 (1971), 261-270

REAL QUADRATIC NUMBER FIELDS WITH LARGE FUNDAMENTAL UNITS

YOSHIHIKO YAMAMOTO

(Received December 4, 1970)

0. Introduction

There are many works on the determination or the estimation of the fundamental unit ε and the ideal class number h of real quadratic number fields F ([1], [3], [6] and [10], for example). The ε's which are treated in them have small orders of absolute value in comparison to their discriminants D, that is, $\varepsilon=O(\sqrt{D})$ or $\log\varepsilon=O(\log\sqrt{D})$. The aim of this note is to construct such F's with comparatively large ε's.

Let p and q be rational primes such that $p<q$. Then put

$$m_k=(p^k q+p+1)^2-4p \tag{0.1}$$

for $k=1, 2, \cdots$. Set $F_k=\boldsymbol{Q}(\sqrt{m_k})$ the quadratic number field obtained by adjoining $\sqrt{m_k}$ to the rational number field $\boldsymbol{Q}$ and denote by D_k, ε_k and h_k the discriminant, the fundamental unit and the ideal class number of F_k respectively. It holds $D_k\to\infty$ as $k\to\infty$, namely, $F_k (k=1, 2, \cdots)$ gives infinitely many real quadratic number fields. Then we can find a positive constant c_1 such that

$$\log\varepsilon_k>c_1(\log\sqrt{D_k})^3 \tag{0.2}$$

holds for sufficiently large D_k (Theorem 3.2).

It is known ([4]) that the following inequality holds for all real quadratic number fields;

$$h\log\varepsilon<\sqrt{D}(\log\sqrt{D}+1). \tag{0.3}$$

Combining (0.2) and (0.3), we get

$$h_k<c_2\frac{\sqrt{D_k}}{(\log\sqrt{D_k})^2} \qquad (c_2<c_1) \tag{0.4}$$

for sufficiently large D_k.

On the other hand, for imaginary quadratic number fields F's with $D<0$, it was shown by Hecke that

$$(0.5) \qquad h > c_3 \frac{\sqrt{|D|}}{\log \sqrt{|D|}}$$

if there exists a positive constant c_4 such that

$$(0.6) \qquad L(s,\chi) \neq 0 \quad \text{for } 1-\frac{c_4}{\log |D|} < s < 1,$$

where $L(s,\chi)$ is the Dirichlet L-funcioin attached to F. To be very broad, we can say that the order of the ideal class numbers of real quadratic number fields is smaller than that of imaginary ones under the assumption (0.6) is valid for all $D<0$.

NOTATIONS: We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ the ring of rational integers, the rational nubmer field and the real number field respectively.

1. Reduced quadratic irrationals

In the first place, we recall some fundamental properties of quadratic irrationals (see [2], [5], or [9]). Let α be a real quadratic irrational number with discriminant D, that is, α is a root of a quadratic equation

$$aX^2+bX+c=0$$

with rational integral coefficients a, b, c such that $a>0$, $(a, b, c)=1$ and $b^2-4ac=D$. In what follows, we give our attention to the case $D>0$ exclusively, so the quadratic irrationals are always to be understood to be real ones. We call a quadratic irrational α *reduced* if $\alpha>1$ and $0>\alpha'>-1$, where α' is the conjugate of α with respect to $\boldsymbol{Q}$. Let α and β be two quadratic irrationals, we say α and β are *equivalent* if we have

$$\alpha=\frac{a\beta+b}{c\beta+d}$$

with $a, b, c, d \in \boldsymbol{Z}$ satisfying $ad-bc=\pm 1$, then α and β have the same discriminant. We know that every quadratic irrational is equivalent to a reduced one.

Denote by $A^*=A^*(D)$ and $A=A(D)$ the set of all quadratic irrationals with discriminant D and the subset of A^* consisting of all reduced ones respectively.

Lemma 1.1. *(a) A is a finite set.*

(b) For $\alpha\in A^*$, α is reduced (i.e. $\alpha\in A$) if and only if the continued fractional expansion of α is purely periodic.

Let $\alpha\in A$. Set

$$\alpha_1=\alpha,$$
(1.1)
$$\alpha_i=a_i+\frac{1}{\alpha_{i+1}} \qquad \text{for } i=1,\ 2,\cdots,$$

where a_i is the greatest rational integer not exceeding α_i. Then, from Lemma 1.1 (*b*), it holds $\alpha_{N+1}=\alpha_1$, where N is the (minimal) period of the continued fractional expansion of α, and moreover $\alpha_i(i=1,2,\cdots, N)$ form a coset of A with respect to the equivalence relation. Let

$$A=A_1\cup A_2\cup\cdots\cup A_h$$

be the equivalence class decomposition of A, then the number h of the cosets is equal to the ideal class number of the field $F=\boldsymbol{Q}(\sqrt{D})$ if D is the discriminant of F. We restrict ourselves to the case where D is the discriminant of a real quadratic number field F in the following.

From (1.1) we have, for $\alpha\in A$,

$$\alpha=a_1+\frac{1}{a_2}+\cdots+\frac{1}{a_N}+\frac{1}{\alpha}=\frac{a\alpha+b}{c\alpha+d}. \tag{1.2}$$

Then $ad-bc=(-1)^N$ and the fundamental unit ε of F is given by $c\alpha+d$.

Proposition 1.2 *If D is equal to the discriminant of a real quadratic number field F and ε is the fundamental unit of F, then*

$$\prod_{\alpha\in A_i}\alpha=\varepsilon \tag{1.3}$$

for any equivalence class $A_i(i=1,2,\cdots, h)$.

Corollary 1.3. *It holds that*

$$\prod_{\alpha\in A}\alpha=\varepsilon^h .$$

Proof of the Proposition 1.2. Let $\alpha\in A$ and define α_i by relation (1.1). Then the equivalence class containing α is given by $\{\alpha_1,\ \alpha_2,\cdots, \alpha_N\}$, where N is the period of the continued fractional expansion of α. From (1.2), the fundamental unit ε is given by

$$\varepsilon=c\alpha+d=[a_2,a_3,\cdots, a_N, \alpha] \tag{1.4}$$

where[ ] is defined in the following;

$$[\ \ ]=1,\quad [b_1]=b_1 \quad\text{and}$$

$$[b_1, b_2, \cdots, b_k]=[b_1, \cdots, b_{k-1}]b_k+[b_1, \cdots, b_{k-2}] \quad (k\geqq 2).$$

We claim

$$(1.5) \qquad \alpha_2\alpha_3\cdots\alpha_k=[a_2, a_3,\cdots, a_{k-1}, \alpha_k] \quad (k\geqq 2).$$

In fact, from (1.1), it holds

$$(1.6) \qquad \alpha_i\alpha_{i+1}=a_i\alpha_{i+1}+1 \quad (i\geqq 1).$$

So (1.5) is valid for $k=2$. Suppose (1.5) is valid for k.
Then

$$\begin{aligned}
&\alpha_2\alpha_3\cdots\alpha_{k+1}\\
&\quad=[a_2,\cdots, a_{k-1}, \alpha_k]\,\alpha_{k+1}\\
&\quad=[a_2,\cdots, a_{k-1}]\,\alpha_k\alpha_{k+1}+[a_2,\cdots, a_{k-2}]\alpha_{k+1}\\
&\quad=[a_2,\cdots, a_{k-1}]\,a_k\alpha_{k+1}+[a_2,\cdots, a_{k-1}]+[a_2,\cdots, a_{k-2}]\,\alpha_{k+1}\\
&\quad=[a_2,\cdots, a_k]\,\alpha_{k+1}+[a_2,\cdots, a_{k-1}]\\
&\quad=[a_2,\cdots, a_k, \alpha_{k+1}].
\end{aligned}$$

Therefore (1.5) is valid for all $k\geqq 2$. Our proposition follows from (1.4) and (1.5), using the relation $\alpha_{N+1}=\alpha_1=\alpha$.

REMARK. Relation (1.3) is used also in [5].

2. Reduced ideals

Let $F=\boldsymbol{Q}(\sqrt{D})$ be the real quadratic number field with discriminant D. Put $\omega=\dfrac{D+\sqrt{D}}{2}$, then 1 and ω form *a* $\boldsymbol{Z}$-basis of the ring $\mathfrak{o}$ of all algebraic integers in F. Let $\xi_1, \xi_2, \cdots, \xi_n$ be elements of F, we denote by $[\xi_1, \xi_2, \cdots, \xi_n]$ and by $(\xi_1, \xi_2, \ldots, \xi_n)$ respectively the modules in F generated by the elements over $\boldsymbol{Z}$ and over $\mathfrak{o}$. So $\mathfrak{o}=[1, \omega]=(1)$. Every integral ideal $\mathfrak{a}$ has the (unique) canonical basis of the following form: $\mathfrak{a}=[a, b+c\omega]$ where $a, b, c\in\boldsymbol{Z}$ satisfying (i) $a>0$, $c>0$ and $ac=N(\mathfrak{a})$ (the absolute norm of $\mathfrak{a}$), (ii) $a\equiv b\equiv 0 \pmod c$ and $N(b+c\omega)\equiv 0 \pmod{ac}$ and (iii) $-a<b+c\omega'<0$ (ω' is the conjugate of ω). Then we define α by

$$\alpha=\alpha(\mathfrak{a})=\frac{b+c\omega}{a}$$

and call α *the quadratic irrational associated with the ideal* $\mathfrak{a}$. An integral ideal $\mathfrak{a}$ is called *reduced* if $c=1$ and $\alpha(\mathfrak{a})$ is a reduced quadratic irrational.

Proposition 2.1. *The map* $\mathfrak{a}\rightarrow\alpha(\mathfrak{a})$ *gives a bijection of the set of all reduced ideals to the set* $A=A(D)$ *of all reduced quadratic irrationals with discriminant* D. *And it induces a bijection of the ideal class group of* F *to the set* $\{A_1, A_2,\cdots, A_h\}$ *of the equivalence classes of* A.

Proposition 2.2. *An integral ideal* $\mathfrak{a}$ *is reduced if* (i) $N(\mathfrak{a})<\frac{\sqrt{D}}{2}$ *and* (ii) *the conjugate ideal* $\mathfrak{a}'$ *is relatively prime to* $\mathfrak{a}$.

For the proof of Proposition 2.1, see [2], [5] or [9]. Proposition 2.2 is easily seen by checking the definition of reduced quadratic irrationals.

3. Lower bounds of regulators

In this section we estimate the values of the regulators of a certain type of real quadratic number fields.

Theorem 3.1. *Let* p_i $(i=1, 2, \cdots, n)$ *be rational primes satisfying* $p_1<p_2<\cdots<p_n$. *Assume that there exist infinitely many real quadratic number fields* F *satisfying the following condition* (*):

(*) *Every* p_i *is decomposed in* F *into the product of two principal prime ideals* $\mathfrak{p}_i$ *and* $\mathfrak{p}_i'$.

Then there exists a positive constant c_0 *depending only on n and* $p_1, p_2, \cdots, p_n$ *such that*

$$\log \varepsilon>c_0 (\log\sqrt{D})^{n+1}$$

holds for sufficiently large D, *where* D *and* ε *are the discriminant and the fundamental unit or* F.

Proof. Consider the ideals $\mathfrak{a}$ of the form

$$\mathfrak{a}=\prod_{i=1}^{n}\mathfrak{p}_i^{e_i}\mathfrak{p}_i'^{f_i}$$

Then $\mathfrak{a}$ is a principal integral ideal and reduced if (a) $N(\mathfrak{a})=p_1^{e_1+f_1}\cdots p_n^{e_n+f_n}<\frac{\sqrt{D}}{2}$ and (b) $e_1f_1=\cdots=e_nf_n=0$ (Proposition 2.2). Let $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_t$ be the set of all reduced ideals obtained as above. Then the quadratic irrationals $\alpha_1, \alpha_2, \cdots, \alpha_t$ associated with them build a subset of the equivalence class A_1, say, corresponding to the principal ideal class. So we get, from Proposition 1.2,

$$\varepsilon=\prod_{\alpha\in A_1}\alpha>\prod_{i=1}^{t}\alpha_i\,.$$

On the other hand, we have

$$\alpha_i=\frac{b_i+\omega}{N(\mathfrak{a}_i)}>\left(\frac{\sqrt{D}}{2}\right)(p_1^{e_1+f_1}\cdots p_n^{e_n+f_n})^{-1},$$

where $\mathfrak{a}_i=[N(\mathfrak{a}_i), b_i+\omega]$ is the canonical basis of $\mathfrak{a}_i$. Hence we get the following inequality

$$\varepsilon > \Pi' \frac{\sqrt{D}/2}{p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}} = \varepsilon_0. \tag{3.1}$$

The product in (3.1) is taken over all integers e_i and f_i satisfying

$$(a') \qquad (e_1+f_1)\log p_1 + \cdots + (e_n+f_n)\log p_n < \log\left(\frac{\sqrt{D}}{2}\right),$$

$$(b') \qquad e_i \geqq 0, f_i \geqq 0 \text{ and } e_i f_i = 0 \quad (i=1, 2, \cdots, n).$$

We have

$$\Pi' \frac{\sqrt{D}}{2} = \left(\frac{\sqrt{D}}{2}\right)^t \tag{3.2}$$

The number t equals to the cardinal of the set of $2n$-tuples $(e_1, f_1, \cdots, e_n, f_n)$ satisfying (a') and (b'). Then it holds

$$t = \frac{2^n V}{P} + O\left(\left(\log \frac{\sqrt{D}}{2}\right)^{n-1}\right), \tag{3.3}$$

where V is the volume of the n-simplex Δ in the n-dimensional euclidean space $\boldsymbol{R}^n$;

$$\Delta = \left\{ (x_1, \cdots, x_n) \in \boldsymbol{R}^n : \begin{array}{l} x_1 \geqq 0, \cdots, x_n \geqq 0, \\ x_1 + \cdots + x_n \leqq \log \frac{\sqrt{D}}{2} \end{array} \right\}.$$

and $\qquad P = (\log p_1)(\log p_2) \cdots (\log p_n)$.

We have

$$V = \int_\Delta dx_1 \cdots dx_n = \frac{1}{n!}\left(\log \frac{\sqrt{D}}{2}\right)^n.$$

For the product of all denominators in the right side of (3.1), we have

$$\begin{aligned} &\log \Pi' (p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}) \\ &= \Sigma' [(e_1+f_1)\log p_1 + \cdots + (e_n+f_n)\log p_n] \\ &= \frac{2^n}{P}\int_\Delta (x_1 + \cdots + x_n)\, dx_1 \cdots dx_n + O\left(\left(\log \frac{\sqrt{D}}{2}\right)^n\right) \\ &= \frac{2^n n}{(n+1)!P} (\log \sqrt{D})^{n+1} + O((\log \sqrt{D})^n). \end{aligned} \tag{3.4}$$

From (3.3) and (3.4), we get

$$\log \varepsilon_0 = \log \left(\frac{\sqrt{D}}{2}\right)^t - \log \Pi' (p_1^{e_1+f_1} \cdots p_n^{e_n+f_n})$$

$$= \frac{2^n}{(n+1)!P} (\log \sqrt{D})^{n+1} + O((\log \sqrt{D})^n).$$

Our theorem follows from this and (3.1).

Theorem 3.2. *For the case $n=2$, the assumption of Theorem 3.1 is satisfied by the following F's : $F=\boldsymbol{Q}(\sqrt{m_k})$*

$$m_k = (p^k q+p+1)^2 - 4p \qquad (k=1,2,\cdots),$$

where we set $p=p_1$ and $q=p_2$.

Proof. We see easily that $m_k \equiv 1 \pmod{p}$, $m_k \equiv (p-1)^2 \pmod{q}$ and $m_k \equiv 1 \pmod{4}$ ($m_k \equiv 1 \pmod{8}$ if $p=2$). Hence each of p and q is decomposed into the product of two distinct prime ideals in F (if m_k is not a square). Set $p=\mathfrak{p}\mathfrak{p}'$ and $q=\mathfrak{q}\mathfrak{q}'$. From the definition of m_k, it holds

$$(p^k q+p+1)^2 - m_k = 4p \tag{3.5}$$

$$(p^k q+p-1)^2 - m_k = -4p^k q. \tag{3.6}$$

From (3.5), $\mathfrak{p}$ and $\mathfrak{p}'$ are both principal (set $\mathfrak{p}=(\frac{p^k q+p+1+\sqrt{m_k}}{2})$, for example). From (3.6), either $\mathfrak{p}^k\mathfrak{q}$ or $\mathfrak{p}'^k\mathfrak{q}$ is principal. Since $\mathfrak{p}^k$ and $\mathfrak{p}'^k$ are principal, both $\mathfrak{q}$ and $\mathfrak{q}'$ are also principal. So the condition (*) in Theorem 3.1 is satisfied. Finally, the infiniteness of the number of F's given above is as follows. Set $k=2j$ (we consider the case where k is even), then

$$m_k = m_{2j} = (p^{2j} q+p+1)^2 - 4p = q^2 p^{4j} + 2q(p+1)p^{2j} + (p-1)^2.$$

Since the diophantine equation

$$Dy^2 = q^2 x^4 + 2q(p+1)x^2 + (p-1)^2$$

has only a finite number of rational integral solutions (x, y) for a fixed integer D (Siegel's theorem), $\boldsymbol{Q}(\sqrt{m_{2j}})$ represents infinitely many real quadratic number fields F for $j=1,2,\ldots$. This completes the proof.

4. Some examples

(I) The case $n=1$.

Set $F_k=\boldsymbol{Q}(\sqrt{k^2\pm 4p})$, for a given prime number $p_1=p$. Then it can easily be seen that F_k satisfies the condition (*) in Theorem 3.1. Hence we get the lower bound for the fundamental unit ε_k of F_k;

$$\log \varepsilon_k > c_0 (\log \sqrt{D_k})^2$$

if the discriminant D_k of F_k is sufficiently large.

Here is an interesting example where we can determine the fundamental units. Let $F=\boldsymbol{Q}(\sqrt{d})$, where

$$d=d_k=(2^k+3)^2-8\ .$$

Since $d\equiv 1 \pmod 8$, the discriminant of F is equal to d if d is square-free. Suppose d is square-free. Set

$$\alpha=\alpha_1=\frac{2^k+1+\sqrt{d}}{2}.$$

Then α is the reduced quadratic irrational with discriminant d associated with the ideal (1) in F. Calculating the continued fractional expansion (1.1) and (1.2), we see that all the reduced quadratic irrationals equivalent to α are given by

$$\alpha_{2i}=\frac{2^k+1+\sqrt{d}}{2^{k-i+2}} \qquad (i=1, 2,\cdots, k),$$

$$\alpha_{2i+1}=\frac{2^k-1+\sqrt{d}}{2^{k+i}} \qquad (i=1, 2,\cdots, k).$$

From Proposition 1.2, we get

$$\begin{aligned}\varepsilon&=\alpha_1\ \alpha_2\cdots\alpha_{2k}\ \alpha_{2k+1}\\ &=\frac{(2^k+1+\sqrt{d})^{k+1}(2^k-1+\sqrt{d})^k}{2\,(2^2\,2^3\cdots 2^{k+1})^2}\\ &=\left(\frac{2^k+3+\sqrt{d}}{4}\right)^k\ \left(\frac{2^k+1+\sqrt{d}}{2}\right).\end{aligned}$$

In fact,

$d_1 = 17,\quad h=1,\quad \varepsilon=4+\sqrt{17}.$

$d_2 = 41,\quad h=1,\quad \varepsilon=32+5\sqrt{41}.$

$d_3 = 113,\quad h=1,\quad \varepsilon=776+73\sqrt{113}.$

$d_4 = 353,\quad h=1,\quad \varepsilon=71264+3793\sqrt{353}.$

$d_5 = 1217,\quad h=1,\quad \varepsilon=276\,28256+7\,91969\sqrt{1217}.$

where h is the ideal class number of F. For the values of $h=h_k$ $(k\leqq 12)$ c.f. [8].

(II) The case $n=2$ (c.f. Theorem 3.2).

Set

$$m=m_k=(p^k q+p+1)^2-4p \qquad (p<q).$$

Let $F=\boldsymbol{Q}(\sqrt{m})$ and h be the ideal class number of F.

(a) $p=2$, $q=3$.

$m_1=73$, $h=1$,

$\varepsilon=1068+125\sqrt{73}$.

$m_2=217=7\cdot 31$, $h=1$,

$\varepsilon=38\ 44063+2\ 60952\sqrt{217}$.

$m_3=721=7\cdot 103$, $h=1$,

$\varepsilon=18\ 63217\ 69432\ 92415+69389\ 85301\ 22112\sqrt{721}$.

$m_4=2593$, $h=1$,

$\varepsilon=2290\ 04858\ 04690\ 92256\ 48456+44\ 97212\ 78935\ 82134\ 31953\sqrt{2593}$.

(b) $p=2$, $q=5$.

$m_1=161=7\cdot 23$, $h=1$,

$\varepsilon=11775+928\sqrt{161}$.

$m_2=521$, $h=1$,

$\varepsilon=1383\ 77240+56\ 24309\sqrt{521}$

$m_3=1841=7\cdot 263$, $h=1$,

$\varepsilon=221\ 70854\ 28203\ 33535+5\ 16720\ 31146\ 43592\sqrt{1841}$.

OSAKA UNIVERSITY

References

[1] G. Degert: *Über die Bestimmung der Grundeinheit gewisser reel-quadratischer Zahlkörper*, Abh. math. Sem. Univ. Hamburg **22** (1958), 92-97.

[2] P. G. L. Dirichlet: Vorlesungen über Zahlentheorie, F. Vieweg & Son, Braunschweig, 1894.

[3] H. Hasse: *Über mehrklassige, aber eingeschlechtige reelquadratische Zahlkorper*, Elem. Math **20** (1965), 49-59.

[4] L. K. Hua: *On the least solution of Pell's equation*, Bull. Amer. Math. Soc. **48** (1942), 731-735.

[5] E. L. Ince: Cycles of Reduced Ideals in Quadratic Fields, Mathematical Tables vol. IV, University Press, Cambridge, 1968.

[6] M. Newman: *Bounds for class numbers*, Proc. Symposia in Pure Math. vol. VIII, A. M. S., 1965, 70-77.

[7] C. Richaud: *Sur la resolution des equations* $x^2-Ay^2=1$, Atti Accad. pontif. Nuovi Lincei (1866), 177-182.

[8] D. Shanks: *On Gauss's class number problems*, Math. Comp. **23** (1969), 151-163.

[9] T. Takagi: Shoto Seisuron Kogi (in Japanese), Kyoritsu, Tokyo, 1931.

[10] H. Yokoi: *On the fundamental unit of real quadratic fields with norm* 1, J. Number Theory **2** (1970), 106-115.

[11] H. Yokoi: *Units and class numbers of real quadratic fields*, Nagoya Math. J. **37** (1970), 61-65.