JP Journal of Algebra, Number Theory and Applications
Volume 13, Number 1, 2009, Pages 41-47
Published Online: April 22, 2009
This paper is available online at http://www.pphmj.com

SOME RESULTS ON THE CLASS NUMBERS OF CERTAIN REAL QUADRATIC FIELDS

AYTEN PEKİN and AYDIN CARUS

Department of Mathematics
Faculty of Science and Arts
Trakya University
22030 Edirne, Turkey
e-mail: aytenpekin@trakya.edu.tr

Department of Computer Engineering
Faculty of Engineering and Architecture
Trakya University
22030 Edirne, Turkey
e-mail: aydinc@trakya.edu.tr

Abstract

In this paper, we revisit the relations between the fundamental units' coefficients of the real quadratic fields $K = Q(\sqrt{D})$ and convergents of the continued fraction expansions of W_D. Furthermore, we provide a theorem and obtain some new results on the class numbers of $K = Q(\sqrt{D})$ by using solvability of the equation $x^2 - Dy^2 = \sigma^2$ and the relations mentioned above.

2000 Mathematics Subject Classification: 11R11, 11R29, 11R27.

Keywords and phrases: real quadratic field, fundamental unit, class number, continued fraction expansion.

This research was partially supported by Scientific Research Project with the number TUBAP 123.

Communicated by Jannis A. Antoniadis

Received September 30, 2007; Revised February 10, 2008

1. Notations

D will denote a positive square free integer and $K = Q(\sqrt{D})$ the real quadratic field, the class number of K will be denoted by $h = h(D)$ throughout in this paper.

We let the fundamental unit of K be $\varepsilon_D = \dfrac{T_D + U_D\sqrt{D}}{\sigma}$ (>1), where

$$\sigma = \begin{cases} 2, & \text{if } D \equiv 1 \pmod 4, \\ 1, & \text{if } D \equiv 2, 3 \pmod 4). \end{cases}$$

Let $\{1, W_D\}$ be the integral base of the real quadratic field $K = Q(\sqrt{D})$, where

$$W_D = \begin{cases} \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \pmod 4 \end{cases}$$

is a quadratic irrational number. The continued fraction expansion of W_D has the form

$$W_D = \begin{cases} \langle a_0, \overline{a_1, a_2, \ldots, a_{k-1}, 2a_0 - 1}\rangle, & \text{if } D \equiv 1 \pmod 4, \\ \langle a_0, \overline{a_1, a_2, \ldots, a_{k-1}, 2a_0}\rangle, & \text{if } D \equiv 2, 3 \pmod 4, \end{cases}$$

where $k = k(D)$ denotes the length of shortest period of W_D.

2. Theorem

Let $D = a^2 \mp b$ be a square free integer with $0 < b \leq 2a$, $(a, b \in Z, b \mid 2a)$ and, p be a prime such that $\left(\dfrac{D}{p}\right) \neq -1$ and the class number $h(D)$ of $K = Q(\sqrt{D})$ be odd. Then

(i)

$$h(D) \geq \frac{\log\left(\dfrac{\sigma p_{k-1} - q_{k-1} - 2}{q_{k-1}{}^2}\right)}{\log p} = \frac{\log(\sigma p_{k-1} - q_{k-1} - 2) - 2\log q_{k-1}}{\log p},$$

if $D \equiv 1 \pmod 4$,

(ii)

$$h(D) \geq \frac{\log(p_{k-1} - 2) - 2\log q_{k-1}}{\log p}, \quad \textit{if} \quad D \equiv 2, 3 \pmod 4,$$

where p_{k-1} *and* q_{k-1} *are* $(k-1)$*-st convergents of the continued fraction of* W_D.

To prove this theorem, we need the following lemmas and propositions.

3. Lemmas and Propositions

Lemma 3.1. *Let* $D = a^2 + b$ *be a square free integer* $0 < b \leq 2a$ *and* $(a, b \in Z, b \mid 2a)$. *Then the continued fraction expansion of* W_D *is*

(i) *If* $D \equiv 1 \pmod 4$, *then*

$$W_D = \begin{cases} \left\langle \dfrac{a+1}{2}, \overline{\dfrac{4a}{b}, a} \right\rangle, & b \equiv 0 \pmod 4, \\ \left\langle \dfrac{a}{2}, \overline{1, 1, \dfrac{a-b}{b}, 1, 1, a-1} \right\rangle, & b \equiv 1 \pmod 4. \end{cases}$$

(ii) *If* $D \equiv 2, 3 \pmod 4$, *then*

$$W_D = \left\langle a, \overline{\frac{2a}{b}, 2a} \right\rangle.$$

Proof. We are going to give the proof only of part (ii) and the other cases are similar. From the following recurrences (see [5, pp. 41-42])

$$W_i = \frac{P_i + \sqrt{D}}{Q_i}, \quad P_{i+1} = a_i \cdot Q_i - P_i, \quad Q_{i+1} = \frac{(D - P_{i+1}^2)}{Q_i} \quad (i \geq 0)$$

we can obtain

$$a_0 = [W_0] = a, \ \text{ for } \ P_0 = 0, \ \ Q_0 = 1,$$

$$a_1 = [W_1] = \frac{2a}{b}, \ \text{ for } \ P_1 = a, \ \ Q_1 = b,$$

$$a_2 = [W_2] = 2a, \quad \text{for} \quad P_2 = a, \quad Q_2 = 1,$$

$$a_3 = [W_3] = \frac{2a}{b} = a_1, \quad \text{for} \quad P_3 = a = P_1, \quad Q_3 = b = Q_1,$$

$$a_4 = [W_4] = 2a = a_2, \quad \text{for} \quad P_4 = a = P_2, \quad Q_4 = 1 = Q_2,$$

$$\ldots.$$

Therefore, we have easily seen that the period length $k = k(D)$ is 2.

Lemma 3.2. *Let* $D = a^2 - b$ *be a square free integer* $0 < b \leq 2a$ *and* $(a, b \in Z, b|4a)$. *Then the continued fraction expansion of* W_D *is*

(i) *If* $D \equiv 1 \pmod 4$, *then*

$$W_D = \begin{cases} \left\langle \dfrac{a-1}{2}, \overline{1, \dfrac{4a-2b}{b}, 1, a-2} \right\rangle, & b \equiv 0 \pmod 4, \\ \left\langle \dfrac{a}{2}, \overline{2, \dfrac{a-b}{b}, 2, a-1} \right\rangle, & b \equiv 3 \pmod 4. \end{cases}$$

(ii) *If* $D \equiv 2, 3 \pmod 4$, *then*

$$W_D = \left\langle a-1, \overline{1, \frac{2a-2b}{b}, 1, 2a-2} \right\rangle.$$

Proposition 3.1. *Let* $D = a^2 + b$ *be a square free integer* $(0 < b \leq 2a$ *and* $a, b \in Z, b|2a)$.

(i) *If* $D \equiv 2, 3 \pmod 4$, *then the smallest solution of the equation* $x^2 - Dy^2 = \sigma^2$ *is*

$$(x, y) = \left(\frac{2a^2 + b}{b}, \frac{2a}{b}\right) = (T_D, U_D) = (a_0 Q_k + Q_{k-1}, Q_k) = (p_{k-1}, q_{k-1}).$$

(ii) *If* $D \equiv 1 \pmod 4$, *then the smallest solution of the equation* $x^2 - Dy^2 = \sigma^2$ *is*

$$(x, y) = \left(\frac{4a^2 + 2b}{b}, \frac{4a}{b}\right) = (T_D, U_D) = (a_k Q_k + 2Q_{k-1}, Q_k) = (\sigma p_{k-1} - q_{k-1}, q_{k-1}).$$

Proof. In this study, since the period of the continued fractions of all W_D is an even number, $N(\varepsilon_D) = 1$ holds.

(i) In order to prove this we can use the following recurrences (see [4, p. 136]):

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2} \quad (k \geq 2),$$

where $\{p_k\}$ and $\{q_k\}$ are sequences of integers.

By using special values; $p_{-1} = 1$, $p_{-2} = 0$, $q_{-1} = 0$, $q_{-2} = 1$, we can obtain $p_0 = a$, $p_1 = \dfrac{2a^2 + b}{b}$, $q_0 = 1$, $q_1 = \dfrac{2a}{b}$, where (p_1, q_1) is the smallest solution of the equation $x^2 - Dy^2 = \sigma^2$. Hence, $p_1 = T_D = a_2 Q_2 + Q_1$, $q_1 = U_D = Q_2$ from $Q_{i+1} = a_i Q_i + Q_{i-1}$ $(i \geq 0)$ for $Q_0 = 0$, $Q_1 = 1$.

(ii) Since $D \equiv 1 \pmod 4$, we have $p_1 = \left(\dfrac{4a^2 + 2b}{b}, \dfrac{4a}{b}\right)$, $q_1 = \dfrac{4a}{b}$ and $Q_2 = a$. Thus we can easily see that $(T_D, U_D) = \left(\dfrac{4a^2 + 2b}{b}, \dfrac{4a}{b}\right)$ is the smallest solution of the equation $x^2 - Dy^2 = \sigma^2$ and

$$(T_D, U_D) = \left(\frac{4a^2 + 2b}{b}, \frac{4a}{b}\right)$$

$$= \begin{cases} (a_6 Q_6 + 2Q_5, Q_6) = (2p_5 - q_5, q_5), & \text{for } k = 6, b \equiv 1 \pmod 4, \\ (a_2 Q_2 + 2Q_1, Q_2) = (2p_1 - q_1, q_1), & \text{for } k = 2, b \equiv 0 \pmod 4. \end{cases}$$

Proposition 3.2. *Let* $D = a^2 - b$ *be a square free integer* $(0 < b \leq 2a$ *and* $a, b \in Z$, $b \mid 2a)$.

(i) *If* $D \equiv 2, 3 \pmod 4$, *then the smallest solution of the equation* $x^2 - Dy^2 = \sigma^2$ *is*

$$(x, y) = \left(\frac{2a^2 - b}{b}, \frac{2a}{b}\right) = (T_D, U_D) = (a_0 Q_k + Q_{k-1}, Q_k) = (p_{k-1}, q_{k-1}).$$

(ii) *If* $D \equiv 1 \pmod 4$, *then the smallest solution of the equation* $x^2 - Dy^2 = \sigma^2$ *is*

$$(x, y) = \left(\frac{4a^2 - 2b}{b}, \frac{4a}{b}\right) = (T_D, U_D) = (a_k Q_k + 2Q_{k-1}, Q_k) = (\sigma p_{k-1} - q_{k-1}, q_{k-1}).$$

Proof. It can be proved as in the proof of Proposition 3.1.

Lemma 3.3 (Davenport, Ankeny, Hasse, Ichimura)**.** *Let* $K = Q(\sqrt{D})$ *be a real quadratic field with the fundamental unit* $\varepsilon_D = \dfrac{T_D + U_D\sqrt{D}}{\sigma}$. *If the Pell's equation* $x^2 - Dy^2 = \mp\sigma^2 m$ *(m not square) is solvable, then the following inequality holds*:

$$\begin{cases} m \geq \dfrac{T_D - 2}{U_D^2}, & \text{for } N(\varepsilon_D) = 1, \\ m \geq \dfrac{T_D}{U_D^2}, & \text{for } N(\varepsilon_D) = -1. \end{cases}$$

Proof of the Theorem. From the assertion of the Theorem, p is a prime such that $\left(\dfrac{D}{p}\right) \neq -1$ and $h(D)$ is odd. Therefore, if P is a prime above p and e is the order of P in the class group of $Q(\sqrt{D})$, then e divides $h(D)$ (e is odd) and $N(P^e) = \sigma^2 p^e = u^2 - Dv^2$ $(u, v \in Z)$ holds. Hence, from Lemma 3.3, Propositions 3.1 and 3.2, we have

$$p^{h(D)} \geq p^e \geq \begin{cases} \dfrac{\sigma p_{k-1} - q_{k-1} - 2}{q_{k-1}^2}, & \text{if } D \equiv 1 \pmod 4, \\ \dfrac{p_{k-1} - 2}{q_{k-1}^2}, & \text{if } D \equiv 2, 3 \pmod 4 \end{cases}$$

for $N(\varepsilon_D) = 1$, which implies

$$h(D) \geq \begin{cases} \dfrac{\log(\sigma p_{k-1} - q_{k-1} - 2) - 2\log q_{k-1}}{\log p}, & \text{if } D \equiv 1 \pmod 4, \\ \dfrac{\log(p_{k-1} - 2) - 2\log q_{k-1}}{\log p}, & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

References

[1] N. C. Ankeny, S. Chowla and H. Hasse, On the class-number of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math. 217 (1965), 217-220.

[2] H. Hasse, Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper, Elem. Math. 20 (1965), 49-59 (in German).

[3] S. Louboutin, Continued fractions and real quadratic fields, J. Number Theory 30 (1998), 167-176.

[4] N. H. McCoy, The Theory of Numbers, The Macmillan Co., New York, 1965.

[5] R. A. Mollin, Quadratics, CRS Press, Boca Raton, New York, London, Tokyo, 1996.

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