T. Azuhata
Nagoya Math. J.
Vol. 95 (1984), 125–135

ON THE FUNDAMENTAL UNITS AND THE CLASS NUMBERS OF REAL QUADRATIC FIELDS

TAKASHI AZUHATA

§0. Introduction

Let $\boldsymbol{Q}$ be the rational number field and $h(m)$ be the class number of the real quadratic field $\boldsymbol{Q}(\sqrt{m})$ with a positive square-free integer m. It is known that if $h(m) = 1$ holds, then m is one of the following four types with prime numbers $p \equiv 1$, $p_i \equiv 3 \pmod 4$ $(1 \leq i \leq 4)$: i) $m = p$, ii) $m = p_1$, iii) $m = 2$ or $m = 2p_2$, iv) $m = p_3 p_4$ (see Behrbohm and Rédei [1]). The sufficient conditions for $h(m) > 1$ with these m were given by several authors: in all cases by Hasse [2], in case i) by Ankeny, Chowla and Hasse [3] and by Lang [4], in case ii) by Takeuchi [5] and by Yokoi [6].

The principal aim of this paper is to extend the results of [3], [4], [5], [6] and a part of [2]. In Section 2, we show that the continued fractional expansion of a reduced quadratic irrational is given by the recurrence formula with rational integers. Further we shall give some types of reduced quadratic irrationals whose periods of the continued fractional expansions are small. In Section 3, using the results of Section 2, we shall give explicitly the fundamental units of $\boldsymbol{Q}(\sqrt{m})$ for several types of m. Finally in Section 4, the sufficient conditions for $h(m) > 1$ will be given for several types of m, using the results of Section 2.

§1. Reduced quadratic irrational

First we review the fundamental properties of quadratic irrationals (see Dirichlet [7] or Takagi [8]). Denote by $\boldsymbol{Z}$ the ring of rational integers and by $[\alpha]$ the greatest rational integer not exceeding α where α is a real number. Let m be a positive square-free integer and put

$$d(m) = \begin{cases} m\,, & \text{if } m \equiv 1 \pmod 4\,, \\ 4m\,, & \text{if } m \not\equiv 1 \pmod 4\,. \end{cases}$$

Received July 15, 1983.

Let α be a quadratic irrational with discriminant $d(m)$, that is, α is a root of quadratic equation $aX^2 + bX + c = 0$ with $a, b, c \in \boldsymbol{Z}, a > 0, (a, b, c) = 1$ and $b^2 - 4ac = d(m)$. Let $I(m)$ be the set of all quadratic irrationals with discriminant $d(m)$. An element α of $I(m)$ is called reduced if $\alpha > 1$, $0 > \alpha' > -1$ where α' is the conjugate of α with respect to $\boldsymbol{Q}$. Let $R(m)$ be the set of all reduced quadratic irrationals with discriminant $d(m)$. Then $R(m)$ is a finite set and an element α of $I(m)$ is in $R(m)$ if and only if the continued fractional expansion of α is purely periodic. For $\alpha \in R(m)$, let

$$\alpha_{i-1} = k_i + \frac{1}{\alpha_i}, \quad k_i = [\alpha_{i-1}] \quad (i \geq 1),$$

be the continued fractional expansion of $\alpha_0 = \alpha$. We say that the period of α is n if $\alpha_n = \alpha$, $\alpha_i \neq \alpha$ $(1 \leq i \leq n-1,\ n \geq 2)$.

LEMMA 1. *Let n be the period of $\alpha \in R(m)$ and*

$$\alpha = k_1 + \frac{1}{k_2} + \cdots + \frac{1}{k_n} + \frac{1}{\alpha} = \frac{r\alpha + s}{t\alpha + u}, \quad k_i, r, s, t, u \in \boldsymbol{Z}, \quad k_i \geq 1.$$

Then $t\alpha + u$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{m})$ with norm $(-1)^n$.

For two elements $\alpha, \beta \in R(m)$, we say that α and β are equivalent if one of the following mutually equivalent conditions is satisfied:

i) $\beta = \dfrac{r\alpha + s}{t\alpha + u}$ with $r, s, t, u \in \boldsymbol{Z}$, $ru - st = \pm 1$,

ii) $\alpha = k_1 + \dfrac{1}{k_2} + \cdots + \dfrac{1}{k_\lambda} + \dfrac{1}{\beta}$ with $k_i \in \boldsymbol{Z}$, $k_i \geq 1$,

iii) $\beta = \ell_1 + \dfrac{1}{\ell_2} + \cdots + \dfrac{1}{\ell_\mu} + \dfrac{1}{\alpha}$ with $\ell_i \in \boldsymbol{Z}$, $\ell_i \geq 1$.

LEMMA 2. *The number of the equivalent classes of $R(m)$ is equal to $h(m)$.*

For the proofs of Lemma 1 and 2, see [7] or [8].

§ 2. Continued fractional expansion

For a positive square-free integer m, we put $m = a^2 + b$ with $a, b \in \boldsymbol{Z}$, $0 < b \leq 2a$. We shall consider the properties of $R(m)$ according to the following cases:

I, $m \not\equiv 1 \pmod 4$,

II, $a \equiv 1 \pmod 2$, $b = 4d$ with $d \in Z$, $d \geq 1$,
III, $a \equiv 0 \pmod 2$, $b = 4d + 1$ with $d \in Z$, $d \geq 0$.

Let ω be an element of $R(m)$ and $sX^2 + tX + u$ be the minimal polynomial of ω with $s, t, u \in Z$, $s > 0$, $(s, t, u) = 1$. In case I, $\omega = (t' + \sqrt{m})/s$ with $t = 2t'$ from $t^2 - 4su = 4m$. In case II or III, $\omega = (t + \sqrt{m})/2s$ from $t^2 - 4su = m$. We notice that $t' + \sqrt{m} > s > \sqrt{m} - t' > 0$ in case I and $t + \sqrt{m} > 2s > \sqrt{m} - t > 0$ in case II or III. So if we put $\omega = (\sqrt{m} + a - r_0)/c_0$ with $c_0, r_0 \in Z$, we see that c_0 is even in case II or III, r_0 is even in case II and is odd in case III, and that $c_0 \mid b + 2ar_0 - r_0^2 = m - (a - r_0)^2$. Let

$$\omega_{i-1} = k_i + \frac{1}{\omega_i}, \quad k_i = [\omega_{i-1}] \quad (i \geq 1)$$

be the continued fractional expansion of $\omega_0 = \omega$ and put $\omega_i = (\sqrt{m} + a - r_i)/c_i$ with $c_i, r_i \in Z$.

PROPOSITION 1. *The integers k_i, c_i and r_i $(i \geq 1)$ are given by the following recurrence formula:*

2.1) $2a - r_{i-1} = c_{i-1}k_i + r_i$, $c_i = c_{i-2} + (r_i - r_{i-1})k_i$ $(i \geq 1)$, *where*

$$0 \leq r_i < c_{i-1}, \; c_{-1} = \frac{1}{c_0}(b + 2ar_0 - r_0^2)\,.$$

Proof. In the case $i = 1$, we see easily that

$$[\omega_0] = \left[\frac{1}{c_0}([\sqrt{m}] + a - r_0)\right] = \left[\frac{1}{c_0}(2a - r_0)\right].$$

So if we put $2a - r_0 = c_0k_1 + r_1$ and $c_1 = c_{-1} + (r_1 - r_0)k_1$ with $k_1, r_1 \in Z$, $0 \leq r_1 < c_0$, it follows from

$$\frac{1}{\omega_1} = \omega_0 - k_1 = \frac{1}{c_0}(\sqrt{m} - a + r_1) \quad \text{that} \quad \omega_1 = \frac{c_0(\sqrt{m} + a - r_1)}{b + 2ar_1 - r_1^2}\,.$$

Since $r_1 = 2a - c_0k_1 - r_0$, we see that

$$\begin{aligned} b + 2ar_1 - r_1^2 &= b + (c_0k_1 + r_0)(2a - c_0k_1 - r_0) \\ &= b + 2ar_0 - r_0^2 + c_0k_1(2a - c_0k_1 - 2r_0) \\ &= c_{-1}c_0 + c_0k_1(r_1 - r_0) = c_0c_1\,. \end{aligned}$$

Hence we have $\omega_1 = (\sqrt{m} + a - r_1)/c_1$. Exchanging suffixes 0, 1 for $i - 1$, i respectively, we get the assertion by the induction.

From now on, we denote by ω an element of $R(m)$, which is also an integer in $\boldsymbol{Q}(\sqrt{m})$, i.e. $\omega = \sqrt{m} + a$ in case I, $\omega = \frac{1}{2}(\sqrt{m} + a)$ in case II, and $\omega = \frac{1}{2}(\sqrt{m} + a - 1)$ in case III. By simple calculation, we have

2.2) $r_0 = r_1 = 0,\ c_0 = 1,\ c_1 = b,\ k_1 = 2a$ in case I,

2.3) $r_0 = r_1 = 0,\ c_0 = 2,\ c_1 = 2d,\ k_1 = a$ in case II,

2.4) $r_0 = r_1 = 1,\ c_0 = 2,\ c_1 = a + 2d,\ k_1 = a - 1$ in case III.

PROPOSITION 2. *Let n be the period of ω. If $n \geq 2$, we have the following relations*:

2.5) $k_i = k_{n+2-i}\ (2 \leq i \leq n),\ r_i = r_{n+1-i}\ (1 \leq i \leq n),$
$c_i = c_{n-i}\ (0 \leq i \leq n).$

Proof. It follows from $\omega_{i-1} = k_i + 1/\omega_i\ (1 \leq i \leq n)$ that

$$-\frac{1}{\omega_i'} = k_i + \frac{1}{-1/\omega_{i-1}'} \qquad (1 \leq i \leq n).$$

We notice that ω_i and $-1/\omega_i'$ are elements of $R(m)$ and are larger than one. We also notice that

$$\omega_n = \omega\,, \qquad -\frac{1}{\omega'} = \frac{c_0(\sqrt{m} + a - r_0)}{b + 2ar_0 - r_0^2} = \frac{1}{c_1}(\sqrt{m} + a - r_1) = \omega_1\,.$$

So we see that $k_i = k_{n+2-i}$ and $\omega_i = -1/\omega_{n+1-i}'\ (2 \leq i \leq n)$ by the uniqueness of the continued fractional expansion. Hence we have $r_i = r_{n+1-i}$, $c_i = c_{n-i}$ from

$$-\frac{1}{\omega_{n+1-i}'} = \frac{c_{n+1-i}(\sqrt{m} + a - r_{n+1-i})}{b + 2ar_{n+1-i} - r_{n+1-i}^2} = \frac{1}{c_{n-i}}(\sqrt{m} + a - r_{n+1-i})\,.$$

From 2.1)–2.5), we can determine the form of m when the period of ω is small as follows.

COROLLARY 1. *Let n be the period of ω. Then we have*

in case I, 2.6) *if $n = 1$, then $b = 1$, i.e. $m = a^2 + 1$ with odd a,*

2.7) *if $n = 2$, then $b \mid 2a$, $b > 1$ with $a^2 + b \not\equiv 1$ (mod 4),*

2.8) *if $n = 3$, then $a = 4k^2r + k + r$, $b = 4kr + 1$ with k, $r > 0$, $k \not\equiv r$ (mod 2),*

2.9) *if $n = 4$, then $a = \frac{1}{2}(kr + 1)(ek - r) + r$, $b = (ek - r)r + e$, $c_2 = kr + 1$ with $e, k, r, ek - r > 0$, $a^2 + b \not\equiv 1$ (mod 4),*

in case II, 2.10) *if $n = 1$, then $d = 1$, i.e. $m = a^2 + 4$ with odd $a \geq 3$,*

2.11) *if $n = 2$, then $d \mid a$ with odd a, $1 < d < \frac{1}{2}a$.*

2.12) *if* $n = 3$, *then* $a = k^2r + k + r$, $d = kr + 1$ *with* $k > 1$, $r > 0$, $a \equiv 1 \pmod 2$,

2.13) *if* $n = 4$, *then* $a = dk + r$, $d = (ek - r)r + e$, $c_2 = 2(kr + 1)$ *with* $k > 1$, e, r, $ek - r > 0$, $a \equiv 1 \pmod 2$,

in case III, 2.14) *if* $n = 1$, *then* $a = 2$, $d = 0$, *i.e.* $m = 5$,

2.15) *if* $n = 2$, *then* $a = 2(d + 1)$, *i.e.* $m = (2d + 3)^2 - 4$ *with* $d > 0$,

2.16) *if* $n = 3$, *then* $d = 0$, *i.e.* $m = a^2 + 1$ *with even* $a \geq 4$,

2.17) *if* $n = 4$, *then* $a = ek + 2e - 1$, $d = \frac{1}{2}(ek - 1)$, $c_2 = 2e$ *with* $e > 1$, $k > 0$, $e \equiv k \equiv 1 \pmod 2$,

2.18) *if* $n = 5$, *then* $a = 2(d + e(k + 1) - 1)$, $d = \frac{1}{2}k(ek - 1)$, $c_2 = c_3 = 2(ek + e - 1)$ *with* e, $k > 0$, $k \equiv 0$ *or* $e \equiv k \equiv 1 \pmod 2$, $e(k + 1) \geq 3$.

Proof. We notice that the period of ω is n if and only if $(c_n, r_n) = (c_0, r_0)$ and $(c_i, r_i) \neq (c_0, r_0)$ $(1 \leq i \leq n - 1, n \geq 2)$. If $n = 1$, we have 2.6), 2.10) and 2.14) from $c_1 = c_0$.

In case I, if $n = 2$, 2.7) follows from $2a = bk_2$, $c_1 \neq 1$. If $n = 3$, we see that $a = \frac{1}{2}(k_2^2r_2 + k_2 + r_2)$, $b = 1 + k_2r_2$, $k_2, r_2 > 0$ from $2a = bk_2 + r_2$, $c_2 = 1 + k_2r_2 = c_1$, $(c_2, r_2) \neq (1, 0)$. Putting $k_2 = 2k$, $r_2 = 2r$, we have 2.8) from $m \not\equiv 1 \pmod 4$. If $n = 4$, it follows from $2a = bk_2 + r_2$, $c_2 = 1 + k_2r_2$, $2a - r_2 = bk_2 = (1 + k_2r_2)k_3 + r_2$, $(c_2, r_2) \neq (1, 0)$ that $b = k_3r_2 + (k_3 + r_2)/k_2$, $a = \frac{1}{2}(k_2r_2 + 1)k_3 + r_2, r_2 > 0$. So we have 2.9) with $k_3 + r_2 = ek_2$, $k_2 = k$, $r_2 = r$.

In case II, if $n = 2$, 2.11) follows from $2a = 2dk_2$, $c_1 \neq 2$. If $n = 3$, we have 2.12) from $2a = 2dk_2 + r_2$, $c_2 = 2 + k_2r_2 = c_1$, $(c_2, r_2) \neq (2, 0)$, $2d \leq a$, by putting $r_2 = 2r$, $k_2 = k$. If $n = 4$, 2.13) follows from $2a = 2dk_2 + r_2$, $c_2 = 2 + k_2r_2$, $2a - r_2 = 2dk_2 = (2 + k_2r_2)k_3 + r_2$, $(c_2, r_2) \neq (2, 0)$, $2d \leq a$ with $r_2 = 2r$, $k_2 = k$, $k_3 + r = ek$.

In case III, we notice that $k_2 = 1$ and $a = 2d + r_2 + 1$ if $n \geq 2$ since $2a - 1 = (a + 2d)k_2 + r_2$. 2.15) follows immediately from this. If $n = 3$, 2.16) follows from $a = 2d + r_2 + 1$, $c_2 = 1 + r_2$, $2a - r_2 = r_2 + 1 + 1$, $(c_2, r_2) \neq (2, 1)$, $r_2 \equiv 1 \pmod 2$. If $n = 4$, from $a = 2d + r_2 + 1$, $c_2 = 1 + r_2$, $2a - r_2 = (r_2 + 1)k_3 + r_2$, $(c_2, r_2) \neq (2, 1)$, we see that $a = \frac{1}{2}(r_2 + 1)k_3 + r_2$, $d = \frac{1}{2}(a - r_2 - 1) = \frac{1}{4}((r_2 + 1)k_3 - 2)$, $r_2 \geq 3$, $r_2 \equiv 1 \pmod 2$. Putting $r_2 + 1 = 2e$, $k_3 = k$, we have 2.17). If $n = 5$, it follows from $a = 2d + r_2 + 1$, $c_2 = 1 + r_2$, $2a - r_2 = a + 2d + 1 = (1 + r_2)k_3 + r_3$, $c_3 = a + 2d + (r_3 - r_2)k_3 = c_2$,

$(c_2, r_2) \neq (2, 1)$, $r_2 \equiv r_3 \equiv 1 \pmod 2$ that $a + 2d = (1 + r_2)k_3 + r_3 - 1 = 1 + r_2 + (r_2 - r_3)k_3$. So we see that $(1 + r_3)(1 + k_3) = r_2 + 3$, $4d = (r_2 - r_3)k_3 = (k_3(1 + r_3) - 2)k_3$. Hence we have 2.18) with $1 + r_3 = 2e$, $k_3 = k$.

§ 3. Application to fundamental units

The following lemma is a well-known result about the fundamental units of real quadratic fields (see Degert [9]).

LEMMA 3. *Let $\boldsymbol{Q}(\sqrt{d})$ be a real quadratic field with square-free integer d. Denote by ε_d the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$ and put $d = n^2 + r$ with $n, r \in \boldsymbol{Z}$, $-n < r \leq n$. If $4n \equiv 0 \pmod r$ holds, then ε_d is of the following form*:

$$\varepsilon_d = n + \sqrt{d} \text{ with } N\varepsilon_d = -\operatorname{sgn} r \text{ for } |r| = 1 \text{ (except for } d = 5),$$

$$\varepsilon_d = \tfrac{1}{2}(n + \sqrt{d}) \text{ with } N\varepsilon_d = -\operatorname{sgn} r \text{ for } |r| = 4,$$

$$\varepsilon_d = \frac{1}{|r|}[(2n^2 + r) + 2n\sqrt{d}] \text{ with } N\varepsilon_d = 1 \text{ for } |r| \neq 1, 4.$$

Using Lemma 1 in Section 1 and Corollary 1 in Section 2, we may give explicitly the fundamental units of $\boldsymbol{Q}(\sqrt{m})$ with several types of m. But we see that if the period of ω is small, then such units are also given by Lemma 3 above. So we show the cases which are not contained in the above.

THEOREM 1. *Let $m = a^2 + b$ be a square-free integer with $a, b \in \boldsymbol{Z}$, $0 < b \leq 2a$. Denote by ε_m the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{m})$. Then ε_m is given by the following form*:

3.1) *if* $a = 4k^2r + k + r$, $b = 4kr + 1$ *with* $k, r > 0$, $k \not\equiv r \pmod 2$, *then*
$\varepsilon_m = (4k^2 + 1)\omega + 2k$ *with* $\omega = \sqrt{m} + a$, $N\varepsilon_m = -1$,

3.2) *if* $a = \frac{1}{2}(kr + 1)(ek - r) + r$, $b = (ek - r)r + e$ *with* $e, k, r, ek - r > 0$, $a^2 + b \not\equiv 1 \pmod 4$, *then*
$\varepsilon_m = (k^2(ek - r) + 2k)\omega + k(ek - r) + 1$ *with* $\omega = \sqrt{m} + a$, $N\varepsilon_m = 1$,

3.3) *if* $a = k^2r + k + r$, $b = 4(kr + 1)$ *with* $k > 1$, $r > 0$, $a \equiv 1 \pmod 2$, *then*
$\varepsilon_m = (k^2 + 1)\omega + k$ *with* $\omega = \frac{1}{2}(\sqrt{m} + a)$, $N\varepsilon_m = -1$,

3.4) *if* $a = dk + r$, $b = 4d$ *with* $d = (ek - r)r + e$, $k > 1$, $e, r, ek - r > 0$, $a \equiv 1 \pmod 2$, *then*

$\varepsilon_m = (k^2(ek-r)+2k)\omega + k(ek-r)+1$ *with* $\omega = \frac{1}{2}(\sqrt{m}+a)$,
$N\varepsilon_m = 1$,

3.5) *if* $a = ek+2e-1$, $b = 2ek-1$ *with* $e>1$, $k>0$, $e \equiv k \equiv 1 \pmod 2$, *then*
$\varepsilon_m = (k+2)\omega + k+1$ *with* $\omega = \frac{1}{2}(\sqrt{m}+a-1)$, $N\varepsilon_m = 1$,

3.6) *if* $a = k(ek-1)+2e(k+1)-2$, $b = 2k(ek-1)+1$ *with* e, $k>0$, $k \equiv 0$ *or* $e \equiv k \equiv 1 \pmod 2$, $e(k+1) \geq 3$, *then*
$\varepsilon_m = (k^2+2k+2)\omega + k^2+k+1$ *with* $\omega = \frac{1}{2}(\sqrt{m}+a-1)$,
$N\varepsilon_m = -1$.

Proof. In general, for a real number α, if we put

$$\alpha = k_1 + \frac{1}{k_2} + \cdots + \frac{1}{k_n} + \frac{1}{\alpha_n} = \frac{p_n\alpha_n + p_{n-1}}{q_n\alpha_n + q_{n-1}},$$

it is known that $q_0 = 0$, $q_1 = 1$, $q_i = q_{i-1}k_i + q_{i-2}$ $(i \geq 2)$. Using the result of Corollary 1, the continued fractional expansion of ω in each case is given as follows:

3.1′) $\omega = 2a + \dfrac{1}{2k} + \dfrac{1}{2k} + \dfrac{1}{\omega}$,

3.2′) $\omega = 2a + \dfrac{1}{k} + \dfrac{1}{ek-r} + \dfrac{1}{k} + \dfrac{1}{\omega}$,

3.3′) $\omega = a + \dfrac{1}{k} + \dfrac{1}{k} + \dfrac{1}{\omega}$,

3.4′) $\omega = a + \dfrac{1}{k} + \dfrac{1}{ek-r} + \dfrac{1}{k} + \dfrac{1}{\omega}$,

3.5′) $\omega = a - 1 + \dfrac{1}{1} + \dfrac{1}{k} + \dfrac{1}{1} + \dfrac{1}{\omega}$,

3.6′) $\omega = a - 1 + \dfrac{1}{1} + \dfrac{1}{k} + \dfrac{1}{k} + \dfrac{1}{1} + \dfrac{1}{\omega}$.

From Lemma 1, we get ε_m by simple calculation.

§4. Application to class numbers

Now we show the various sufficient conditions for $h(m) > 1$ when m is one of the four types in Section 0, and when the period of ω is small, where ω is an element of $R(m)$ and is also an integer of $\boldsymbol{Q}(\sqrt{m})$.

THEOREM 2. *If one of the integers in the following condition* i) *is not prime, or there exists an odd prime q satisfying one of the following conditions* ii), iii), iv) *in each case of* 4.1)–4.8), *then* $h(m) > 1$ *holds*:

4.1) *if* $m = p = 9g^2 + 2$ *with odd* g *and prime* $p \equiv 3 \pmod 4$,

i) $6g + 1,\ 6g - 1$,

ii) $q < 3g,\ \left(\frac{p}{q}\right) = 1$,

iii) $q \mid g,\ q \equiv \pm 1 \pmod 8$,

iv) $q \mid 3g \pm 1,\ q \equiv \pm 1 \pmod{12}$,

4.2) *if* $m = 2p = 2(18g^2 + 1)$ *with odd* g *and prime* $p \equiv 3 \pmod 4$,

i) $12g + 1,\ 12g - 1$,

ii) $q \le 6g + 1,\ \left(\frac{2p}{q}\right) = 1$,

iii) $q \mid g,\ q \equiv \pm 1 \pmod 8$,

iv) $q \mid 6g \pm 1,\ q \equiv \pm 1 \pmod{12}$,

4.3) *if* $m = p = g^2 - 2$ *with odd* $g > 3$ *and prime* $p \equiv 3 \pmod 4$,

i) $2g - 3,\ 6g - 11$,

ii) $q \le g,\ \left(\frac{p}{q}\right) = 1$,

iii) $q \mid g,\ q \equiv 1$ *or* $3 \pmod 8$,

iv) $q \mid g \pm 1,\ q \equiv 1 \pmod 4$,

4.4) *if* $m = 2p = 2(8g^2 - 1)$ *with prime* $p \equiv 3 \pmod 4$,

i) $8g - 3,\ 24g - 11$,

ii) $q < 4g,\ \left(\frac{2p}{q}\right) = 1$,

iii) $q \mid g,\ q \equiv 1$ *or* $3 \pmod 8$,

iv) $q \mid 4g \pm 1,\ q \equiv 1 \pmod 4$,

4.5) *if* $m = p = g^2 + 4$ *with odd* g *and prime* $p \equiv 1 \pmod 4$,

i) $g,\ 2g - 3$,

ii) $q \le \frac{1}{2}(g + 1),\ \left(\frac{p}{q}\right) = 1$,

iii) $q \mid g \pm 1,\ q \equiv \pm 1 \pmod 5$,

4.6) *if* $m = p_1 p_2 = p_1(p_1 g^2 + 4)$ *with odd* g *and primes* $p_1 \equiv p_2 \equiv 3 \pmod 4$,

i) $p_1(g + 1) - 1$,

ii) $q \le \frac{1}{2}(p_1 g + 1),\ \left(\frac{p_1 p_2}{q}\right) = 1$,

4.7) *if* $m = p_1 p_2 = g^2 - 4$ *with odd* $g > 5$ *and primes* $p_1 \equiv p_2 \equiv 3 \pmod 4$,

i) $2g - 5$,

ii) $q \le \frac{1}{2}(g - 1),\ \left(\frac{p_1 p_2}{q}\right) = 1$,

iii) $q \mid g,\ q \equiv 1 \pmod 4$,

4.8) *if* $m = p = 4g^2 + 1$ *with prime* $p \equiv 1 \pmod 4$,

i) $g,\ 3g - 2$,

ii) $q < g,\ \left(\frac{p}{q}\right) = 1$,

iii) $q \mid g \pm 1,\ q \equiv \pm 1 \pmod 5$,

where (m/q) *is Kronecker's symbol.*

To prove this Theorem, we show the general conditions for $h(m) > 1$ according to the three cases in Section 2.

THEOREM 3. *Let* n *be the period of* ω *and* $R_1(m) = \{\omega_0, \omega_1, \cdots, \omega_{n-1}\}$ *be the equivalent class in* $R(m)$ *containing* $\omega_0 = \omega$, *and put* $\omega_i = (\sqrt{m} + a - r_i)/c_i$ $(0 \le i \le n - 1)$. *Then* $h(m) > 1$ *holds if and only if* $R(m) \ne R_1(m)$, *i.e. there exist integers* A *and* t *satisfying the following condition* 4.9):

4.9) *in case* I, $\quad A \mid t^2 - 2at - b\ (0 \le t < a),\ t < A \le 2a - t,$
$(A, t) \ne (c_i, r_i)\ (0 \le i \le n - 1),$

in case II, $\quad A \mid t^2 - at - d \ \left(0 \leq t < \dfrac{a}{2}\right),\ t < A \leq a - t,$

$(2A, 2t) \neq (c_i, r_i)\ (0 \leq i \leq n-1),$

in case III, $\quad A \mid t^2 - (a-1)t - \left(\dfrac{a}{2} + d\right) \left(0 \leq t < \dfrac{a}{2}\right),\ t < A < a - t,$

$(2A, 2t+1) \neq (c_i, r_i)\ (0 \leq i \leq n-1).$

Proof. From the equations:

$$m = (a-t)^2 - (t^2 - 2at - b) \qquad \text{in case I},$$
$$m = (a-2t)^2 - 4(t^2 - at - d) \qquad \text{in case II},$$
$$m = (a-2t-1)^2 - 4(t^2 - (a-1)t - (\tfrac{1}{2}a + d)) \qquad \text{in case III},$$

each element α of $R(m)$ may be written as follows:

$$\alpha = \frac{1}{A}(\sqrt{m} + a - t) \quad \text{with} \quad A \mid t^2 - 2at - b \quad (0 \leq t < a),$$
$$t < A \leq 2a - t \quad \text{in case I},$$
$$\alpha = \frac{1}{2A}(\sqrt{m} + a - 2t) \quad \text{with} \quad A \mid t^2 - at - d \quad \left(0 \leq t < \frac{a}{2}\right),$$
$$t < A \leq a - t \quad \text{in case II},$$
$$\alpha = \frac{1}{2A}(\sqrt{m} + a - 2t - 1) \quad \text{with} \quad A \mid t^2 - (a-1)t - \left(\frac{a}{2} + d\right)$$
$$\left(0 \leq t < \frac{a}{2}\right), \quad t < A < a - t \quad \text{in case III}.$$

So the existence of the integers A and t satisfying 4.9) means that $R(m) \neq R_1(m)$, which is the same thing as $h(m) > 1$ from Lemma 2. The converse is easy to verify.

COROLLARY 2. *Under the same notations as in Theorem* 3, *if there exists an odd prime* q *satisfying the following condition* 4.10), *then* $h(m) > 1$ *holds*:

4.10) *in case* I, $\quad q \leq a + 1,\ q \neq c_i\ (0 \leq i \leq n-1),\ \left(\dfrac{m}{q}\right) = 1,$

in case II, $\quad q \leq \dfrac{1}{2}(a+1),\ 2q \neq c_i\ (0 \leq i \leq n-1),\ \left(\dfrac{m}{q}\right) = 1,$

in case III, $\quad q \leq \dfrac{a}{2},\ 2q \neq c_i\ (0 \leq i \leq n-1),\ \left(\dfrac{m}{q}\right) = 1.$

We use the following simple lemma without proof.

LEMMA 4. *Let q be an odd prime and $f(X) = X^2 + uX + v$ with u, $v \in Z$. Then the polynomial $f(X)$ is reducible modulo q if $((u^2 - 4v)/q) = 1$ holds.*

Proof of Corollary 2. Assume that there exists an odd prime q satisfying 4.10). In case I, from Lemma 4, we see that $t^2 - 2at - b \equiv (t - u) \times (t - v) \pmod{q}$ with u, $v \in Z$, $0 \leq u$, $v < q$, since $((4a^2 + 4b)/q) = (4m/q) = 1$. We may assume that $0 \leq u < v < q$, $u \leq q - 2 \leq a - 1$ since $u = v$ means that $m \equiv 0 \pmod{q}$. So we see that

$$q \,|\, u^2 - 2au - b\,, \quad 0 \leq u \leq a - 1\,, \quad u < q \leq 2a - u\,, \quad q \neq c_i\,.$$

Hence we have $h(m) > 1$ by Theorem 3. In case II and III, we have $h(m) > 1$ in the same way.

Proof of Theorem 2. Using Theorem 3 and Corollary 2, our assertion follows from Corollary 1 in Section 2: 4.1) (resp. 4.2)) from 2.7) with $a = 3g$ (resp. $a = 6g$), $b = 2$, $c_0 = 1$, $c_1 = 2$; 4.3) (resp. 4.4)) from 2.9) with $k = r = 1$, $a = e = g - 1$, $b = 2g - 3$ (resp. $a = e = 4g - 1$, $b = 8g - 3$), $c_0 = 1$, $c_1 = c_3 = 2g - 3$ (resp. $c_1 = c_3 = 8g - 3$), $c_2 = 2$; 4.5) from 2.10) with $c_0 = 2$; 4.6) from 2.11) with $a = p_1 g$, $d = p_1$, $c_0 = 2$, $c_1 = 2p_1$; 4.7) from 2.15) with $d = \frac{1}{2}(g - 3)$, $c_0 = 2$, $c_1 = 2g - 4$; 4.8) from 2.17) with $a = 2g$, $c_0 = 2$, $c_1 = c_2 = 2g$.

If one of the integers in i) is not prime, from 4.9) with $t = 0$, 1 or 2, we have $R(m) \neq R_1(m)$. The condition ii) in each case is the same thing as 4.10), and iii), iv) are the special cases of ii). This completes the proof.

ACKNOWLEDGEMENT. The author wishes to thank Professor I. Yamaguchi for his kind advice and encouragement.

REFERENCES

[1] H. Behrbohm and L. Rédei, Der Euklidische Algorithmus in quadratischen Körpern, J. Reine Angew. Math., **174** (1936), 192–205.

[2] H. Hasse, Über mehrklassige, aber eingeschlechtige reellquadratischer Zahlkörper, Elem. Math., **29** (1965), 49–59.

[3] 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.

[4] S. D. Lang, Note on the class-number of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., **290** (1977), 70–72.

[5] H. Takeuchi, On the class-number of the maximal real subfield of a cyclotomic field, Canad. J. Math., **33** (1981), 55–58.

[6] H. Yokoi, On the Diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field, Nagoya Math. J., **91** (1983), 151–161.

[7] P. G. L. Dirichlet, Vorlesungen über Zahlentheorie, F. Vieweg & Shon, Braunschweig, 1894.
[8] T. Takagi, Shoto Seisuron Kogi (in Japanese), Kyoritsu, Tokyo, 1931.
[9] G. Degert, Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 92–97.

Department of Mathematics
Science University of Tokyo
26 Wakamiya, Shinjuku-ku
Tokyo, Japan