Explicit Representation of Fundamental Units of Some Quadratic Fields

By Koshi TOMITA

Graduate School of Human Informatics, Nagoya University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 13, 1995)

1. Introduction. Explicit form of the fundamental unit of real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ is not well-known except for real quadratic fields of Richaud-Degert type.

In this paper, for all real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ such that d is a positive square-free integer congruent to 1 mod 4 and the period k_d in the continued fraction expansion of the quadratic irrational number $\omega_d = (1+\sqrt{d})/2$ in $\boldsymbol{Q}(\sqrt{d})$ is equal to 3, we describe explicitly T_d, U_d in the fundamental unit $\varepsilon_d = (T_d + U_d\sqrt{d})/2 (>1)$ of $\boldsymbol{Q}(\sqrt{d})$ and d itself by using two parameters l, r appearing in the continued fraction expansion of ω_d. Finally, as an application of this theorem, we provide a result on class number one problem for real quadratic fields and on Yokoi's invariant n_d.

For the set $I(d)$ of all quadratic irrational numbers in $\boldsymbol{Q}(\sqrt{d})$, we say that α in $I(d)$ is reduced if $\alpha > 1$, $-1 < \alpha' < 0$ (α' is the conjugate of α with respect to $\boldsymbol{Q}$), and denote by $R(d)$ the set of all reduced quadratic irrational numbers in $I(d)$. Then, it is well-known that any number α in $R(d)$ is purely periodic in the continued fraction expansion and the denominator of its modular automorphism is equal to the fundamental unit ε_d of $\boldsymbol{Q}(\sqrt{d})$, and that the norm of ε_d is $(-1)^{k_d}$ (see, for example, [2] p. 205, 215). Moreover the continued fraction with period k is generally denoted by $[a_0, \overline{a_1, \dots, a_k}]$, and $[x]$ means the greatest integer not greater than x.

Now, for any square-free positive integer d congruent to 1 mod 4, we put $d = a^2 + b$, $0 < b \le 2a$ ($a, b \in \boldsymbol{Z}$). Here, since $\sqrt{d} - 1 < a < \sqrt{d}$, both integers a and b are uniquely determined by d. Then, our main theorem is as follows:

Theorem. *For a square-free positive integer d congruent to 1 mod 4, we assume $k_d = 3$. Then, in the case that a is odd,*

$$\omega_d = [(a+1)/2, \overline{l, l, a}],$$

and

$$(T_d, U_d) = ((l^2+1)^2 r + l(l^2+3),\ l^2+1)$$

hold for two positive integers l, r such that $a = (l^2+1)r + l$.

Moreover in this case, it holds

$$d = (l^2+1)^2 r^2 + 2l(l^2+3)r + l^2 + 4.$$

In the case that a is even,

$$\omega_d = [a/2, \overline{1, 1, a-1}],\ (T_d, U_d) = (2a, 2)\ \textit{and}\ d = a^2 + 1$$

hold.

In order to prove this theorem, we need several lemmas.

Lemma 1. *For a square-free positive integer $d > 5$ congruent to 1 modulo 4, we put $\omega = (1+\sqrt{d})/2$, $q_0 = [\omega]$ and $\omega_R = q_0 - 1 + \omega$. Then $\omega \notin R(d)$, but $\omega_R \in R(d)$ holds. Moreover for the period k of ω_R, we get $\omega_R = [\overline{2q_0 - 1, q_1, \dots, q_{k-1}}]$ and $\omega = [q_0, \overline{q_1, \dots, q_{k-1}, 2q_0 - 1}]$. Furthermore, let $\omega_R = (P_k\omega_R + P_{k-1})/(Q_k\omega_R + Q_{k-1}) = [2q_0 - 1, q_1, \dots, q_{k-1}, \omega_R]$ be a modular automorphism of ω_R, then the fundamental unit ε_d of $\boldsymbol{Q}(\sqrt{d})$ is given by the following formula:*

$$\varepsilon_d = (T + U\sqrt{d})/2 > 1,$$
$$T = (2q_0 - 1)Q_k + 2Q_{k-1},\ U = Q_k,$$

where Q_i is determined by $Q_0 = 0$, $Q_1 = 1$, $Q_{i+1} = q_iQ_i + Q_{i-1}$, $(i \ge 1)$.

Proof. Denote by Nm and Tr the norm and the trace respectively. Then $\omega_R = (2q_0 - 1 + \sqrt{d})/2$ belongs to $I(d)$, because ω_R is a root of the equation $X^2 - T_r(\omega_R)X + Nm(\omega_R) = 0$ and the discriminant of this equation is $Tr(\omega_R)^2 - 4Nm(\omega_R) = d$. Moreover since $\omega_R' = [\omega] - \omega > -1$ and $2q_0 - 1 < \sqrt{d}$, we get $0 > \omega_R' > -1$. Hence ω_R belongs to $R(d)$. Since $[\omega_R] = [[\omega] - 1 + \omega] = 2q_0 - 1$ and ω_R is purely periodic, ω_R and ω have expansions described in this Lemma respectively. Since $Q_k\omega_R + Q_{k-1}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{d})$ with norm $(-1)^k$ (see, for example, [2] p. 215), $\varepsilon_d = Q_k\{q_0 - 1 + (1+\sqrt{d})/2\} + Q_{k-1} = \{(2q_0 - 1)Q_k + 2Q_{k-1} + Q_k\sqrt{d}\}/2$. Thus, the proof of Lemma 1 was completed.

We apply the recurrence formula in [1] to ω_R, and get useful parameters essentially connected with partial quotients of the continued fraction expansion.

Lemma 2. *For a square-free positive integer d, we put* $d = a^2 + b (0 < b \leq 2a,\ a, b \in \boldsymbol{Z})$. *Moreover, let* $\omega_i = l_i + 1/\omega_{i+1}$ $(l_i = [\omega_i],\ i \geq 0)$ *be the continued fraction expansion of* $\omega = \omega_0$ *in* $R(d)$. *Then each* ω_i *is expressed in the form* $\omega_i = (a - r_i + \sqrt{d})/c_i$ $(c_i, r_i \in \boldsymbol{Z})$, *and* l_i, c_i, r_i *can be obtained from the following recurrence formula*:

$$\begin{cases} \omega_0 = (a - r_0 + \sqrt{d})/c_0, \\ 2a - r_i = c_i l_i + r_{i+1}, \\ c_{i+1} = c_{i-1} + (r_{i+1} - r_i) l_i \ (i \geq 0), \end{cases}$$

where $0 \leq r_{i+1} < c_i,\ c_{-1} = (b + 2ar_0 - r_0^2)/c_0$. *Moreover for the period* $k \geq 1$ *of* ω_0, *we get*

$l_i = l_{k-i} (1 \leq i \leq k-1)$,

$r_i = r_{k-i+1},\ c_i = c_{k-i}\ (1 \leq i \leq k)$.

For the proof of this lemma, see T. Azuhata [1] p. 127, 128.

Moreover, since $R(d) \ni \omega_i$ implies $-1/w_i' \in R(d)$, we obtain easily the following lemma:

Lemma 3. *Put* $\omega = \omega_R$ *in Lemma* 2. *Then*

$$\begin{cases} r_0 = r_1 = a - l_0 = a - 2q_0 + 1, \\ c_0 = 2,\ c_1 = c_{-1} = (b + 2ar_0 - r_0^2)/c_0, \\ l_0 = 2q_0 - 1,\ l_i = q_i (1 \leq i \leq k-1). \end{cases}$$

Proof. From Lemma 2, we obtain immediately $l_0 = 2q_0 - 1$, $c_0 = 2$ and $r_0 = a - l_0$, because $\omega_0 = [2q_0 - 1, q_1, \ldots] = [l_0, l_1, \ldots]$ and $a - r_0 = l_0$. Moreover $\omega_1 = 1/(\omega_0 - l_0) = c_0(l_0 + \sqrt{d})/(b + 2ar_0 - r_0^2) = (l_0 + \sqrt{d})/c_{-1}$ holds, and hence $c_1 = c_{-1}$, $r_1 = a - l_0$. Consequently we have $r_0 = r_1$.

2. The proof of main theorem.

We put $\omega = (1 + \sqrt{d})/2$ from now on and prove our main theorem.

Proof. In the case of even a, we can put $d = a^2 + 4m + 1$ for a positive integer m satisfying $0 \leq 4m < 2a$. Since $q_0 = [\omega] = [([\sqrt{d}] + 1)/2] = [(a+1)/2] = a/2$ and $\omega_R = (a - 1 + \sqrt{d})/2$, it follows from Lemma 3 that $r_0 = r_1 = a - 2q_0 + 1 = 1$, $c_0 = 2$, $c_1 = (4m + 1 + 2ar_0 - r_0^2)/2 = a + 2m$ and $l_0 = a - 1$. Let $[\overline{a - 1, l_1, l_2}]$ be the continued fraction expansion of ω_R. Then, by Lemma 2 we have $2a - r_1 = (a + 2m) l_1 + r_2$ because of $c_1 = a + 2m$. Hence, we get $(2 - l_1) a = 2ml_1 + r_1 + r_2 > 0$, which implies $l_1 = 1$. So, we have $a = 2m + r_2 + 1$. Moreover, it follows from Lemma 2 and Lemma 3 that $c_2 = r_2 + 1$, $2a - r_2 = c_2 l_2 + r_3$, $l_2 = l_1 = 1$ and $r_3 = r_1 = 1$ respectively, and hence $a = r_2 + 1$ holds. Therefore, $m = 0$ follows from $r_2 + 1 = 2m + r_2 + 1$. Thus we get $d = a^2 + 1$. Since $\omega = [a/2, \overline{1, 1, a - 1}]$ by Lemma 1, $Q_2 = 1$ and $Q_3 = 2$ are obtained, from which we have $T = 2a$ and $U = 2$ immediately.

In the case of odd a, we can put $d = a^2 + 4m$ for a positive integer m satisfying $0 < 4m \leq 2a$. In the same way, since $q_0 = (a+1)/2$ and $\omega_R = (a + \sqrt{d})/2$, we get $r_0 = r_1 = a - 2q_0 + 1 = 0$, $c_0 = 2$, $c_1 = 2m$ and $l_0 = a$. Let $\omega_R = [\overline{a, l_1, l_2}]$ be the continued fraction expansion of ω_R. Then, by Lemma 2 we have $2a = 2ml_1 + r_2$, $c_2 = c_0 + (r_2 - r_1) l_1 = 2 + r_2 l_1 = c_1$, and hence $2a = (2 + r_2 l_1) l_1 + r_2$. Here, since r_2 is even, we can put $r_2 = 2r$ for an integer r. If we put $l_1 = 1$ again, then $a = r(l^2 + 1) + l$ holds. On the other hand, $2m = 2rl + 2$ implies $m = rl + 1$. Since a is odd, it does not happen that both r and l are even. Since $\omega = [(a+1)/2, \overline{l, l, a}]$ implies $Q_2 = l$ and $Q_3 = l^2 + 1$ by Lemma 1, we obtain $T = r(l^2 + 1)^2 + l(l^2 + 3)$, $U = l^2 + 1$ respectively. Moreover, we can also get immediately $d = (l^2 + 1)^2 r^2 + 2l(l^2 + 3) r + l^2 + 4$ because of $b = 4(rl + 1)$. Thus the theorem was proved completely.

Next we apply above theorem to Yokoi's invariant n_d.

Corollary. *Let d be a square-free positive integer congruent to* 1 *modulo* 4 *and assume* $k_d = 3$. *Then it always holds* $n_d = [T_d / U_d^2] \neq 0$. *In this case, there exist exactly the following* 11 *real quadratic fields* $\boldsymbol{Q}(\sqrt{d})$ *with class number one*: $d =$

$$17, 37, 61, 101, 197, 317, 461, 557, 667, 773, 1877.$$

Proof. Under the same notation as main theorem, in the case that a is even, Corollary is clear from $n_d = q_0 \neq 0$. In the other case, we get easily $U_d^2 - l(l^2 + 3) = l^3(l - 1) + l(2l - 3) + 1$, and so $U_d^2 > l(l^2 + 3)$ because of $l > 1$. Hence $n_d = r \neq 0$ holds. Therefore, by H. Yokoi [3], there exists only a finite number of d such that the class number of the real quadratic field $\boldsymbol{Q}(\sqrt{d})$ is one and $k_d = 3$. The tables I, III in [3] show that such d are exactly eleven primes described in this Corollary.

References

[1] T. Azuhata: On the fundamental unit and the class numbers of real quadratic fields. Nagoya Math. J., **95**, 125–135 (1984).

[2] T. Takagi: Shotō Seisūron Kōgi. 2nd ed., Kyōritsu, Tokyo (1971) (in Japanese).

[3] H. Yokoi: The fundamental unit and class number one problem of real quadratic fields with prime discriminant. Nagoya Math. J., **120**, 51–59 (1990).
[4] H. Yokoi: The fundamental unit and bounds for class numbers of real quadratic fields. Nagoya Math. J., **124**, 181–197 (1991).
[5] H. Yokoi: New invariants and class number problem in quadratic fields. Nagoya Math. J., **132**, 175–197 (1993).