42. *On Hasse's Argorithm to Calculate Fundamental Units of Real Cyclic Biquadratic Fields**)

By Ken-ichi YOSHINO

Department of Mathematics, Kanazawa Medical University

(Communicated by Shokichi IYANAGA, M. J. A., June 7, 1994)

1. Introduction. Let K be a real cyclic biquadratic field with conductor F and k the quadratic subfield of K with conductor f. Let E_K and E_k be the groups of units of K and k, respectively. Hasse [1] defined the unit index of K as $Q_K = [E_K : HE_k]$, where H is the group of relative units of K, i.e., $H = \{\eta \in E_K ; N_{K/k}(\eta) = \pm 1\}$. Then $Q_K = 1$ or 2. Let E be the relative fundamental unit of K, i.e., H is generated by ± 1, E and the conjugate of E and let ε be the fundamental unit of k. For a number A of K, A is uniquely written in the form $A = \frac{1}{2}\left(u + \frac{v\tau(\chi) + \overline{v\tau(\chi)}}{2}\right) = [u, v]$, where u, v are elements of k, $\boldsymbol{Q}(\sqrt{-1})$, respectively and $\tau(\chi)$ is the Gauss sum of a generator χ of the character group of K (cf. [1] §8). We call u and v the coordinates of A. If A is an integer of K, then u and v are integers of k and $\boldsymbol{Q}(\sqrt{-1})$, respectively. Let s be a generator of the Galois group of K over $\boldsymbol{Q}$. Let $A' = A^s$, $A'' = A^{s^2}$, $A''' = A^{s^3}$ be the conjugates of A. Let $a + bi$ be the basis number of K ("Basiszahl" von K in [1] p. 30).

If $Q_K = 2$, then there exists the unique positive unit E^* of K such that $E_K = \langle -1, E^*, E^{*\prime}, E^{*\prime\prime} \rangle$ and

(1) $$E^*E^{*\prime} = \pm E, \qquad N_{K/k}(E^*) = \pm \varepsilon.$$

E^* is called the fundamental unit of K. By using (1) Hasse described a method of calculating the coordinates of E^* from ε and E ([1], §12 B). We put $E = [(x_0 + x_1\sqrt{f})/2, y_0 + y_1 i]$ and $E^* = [(x_0^* + x_1^*\sqrt{f})/2, y_0^* + y_1^* i]$. Hasse's method is summarized as follows: To get the non-equivalent solutions (x_0^*, x_1^*), we examine the principal ideals (α) of k such that $N((\alpha)) = |x_0|$. And, to get the non-equivalent solutions (y_0^*, y_1^*), we examine the ideals $\boldsymbol{a}$ of k such that $N(\boldsymbol{a}) = |x_1|/G$ and $\boldsymbol{a} \in C_{\hat{\varphi}}^{-1}$, where $G = F/f$ and $C_{\hat{\varphi}}$ is the ideal class of k which is corresponding to the primitive quadratic form $\hat{\varphi}(y^*) = b(y_0^{*2} - y_1^{*2})/2 + ay_0^*y_1^*$ with determinant f. We note that if $Q_K = 2$ then G divides x_1. In this way we obtain a finite number of candidates $(x_0^*, x_1^*, y_0^*, y_1^*)$ for E^*. Among them there are solutions of (1). However, if we use Hasse's method to calculate the coordinates of E^* from ε and E, then the calculation is complicated in general, because the number of candidates for E^* is large.

In this note we shall modify Hasse's method and give a simple algorithm. That is, our method is based upon the following fact: $Q_K = 2$ if and only if

*) Partially supported by Grant-in-Aid for Scientific Research (No. 05640073), Ministry of Education, Science and Culture, Japan.

there exists a unit γ of K such that $\gamma^2 = \rho\varepsilon EE'$, where $\rho = sign(E')$. By our algorithm at most four candidates $(x_0^*, x_1^*, y_0^*, y_1^*)$ for E^* are easily obtained for any real cyclic biquadratic field K and one of them exactly gives the coordinates of E^*. The aim of this note is to prove the following algorithm, wherein (2), ..., (6) denote the equations in §2.

Algorithm. (i) *Calculate* $\rho\varepsilon EE' = [(t_0 + t_1\sqrt{f})/2, r_0 + r_1 i]$ *from* ε *and* $E = [(x_0 + x_1\sqrt{f})/2, y_0 + y_1 i]$.

(ii) *Calculate at most two integer solutions* (u_0, u_1) *of* (4) *such that* $u_0 \geq 0$ *for each integer solution* X *of* (3).

(iii) *For each* (u_0, u_1) *of* (ii), *calculate* v_0, v_1 *by* (5) *and, when they are integers, examine whether or not* (u_0, u_1, v_0, v_1) *satisfies the former two equations of* (2).

(iv) *For an integer solution* (u_0, u_1, v_0, v_1) *of* (2) *such that* $u_0 \geq 0$, *put* $\theta = [(u_0 + u_1\sqrt{f})/2, v_0 + v_1 i]$ *and calculate the coordinates of* $\theta E'''$.

(v) *By the values of cosine sums* Ω *and* Ω', *calculate the approximate value of* $\theta E'''$ *and determine* E^* *by* (6).

Using this algorithm, we shall also give a table of E and E^* for such a field K with conductor $F < 300$, wherein we correct some errors in Hasse's table.

2. Proof of Algorithm. From now on we consider a real cyclic biquadratic field K with $Q_K = 2$ and suppose that $E = [x, y] = [(x_0 + x_1\sqrt{f})/2, y_0 + y_1 i]$ is given. ε is easily calculated by the well known algorithm. We put $n(A) = N_{K/k}(A)$ for a number A of K. For the calculations of numbers of K, we need the following lemma which is shown in [1], §8. For $u = (u_0 + u_1\sqrt{f})/2$ and $v = v_0 + v_1 i$, we put $\varphi(v) = a(v_0^2 - v_1^2) - 2bv_0v_1$, $\hat{\varphi}(v) = b(v_0^2 - v_1^2)/2 + av_0v_1$ and $u \circ v = \{u_0(v_0 + v_1 i) + \sigma u_1(a - bi)\cdot(v_0 - v_1 i)\}/2$, where σ is the sign defined by [1], §7 (12). Let $N(u)$ and $N(v)$ be the norms of u and v, respectively and $G = F/f$.

Lemma 1. *For a number* $A = [u, v]$ *of* K, *we have*

(i) $A^2 = \left[\frac{1}{2}\left(u^2 + G\frac{N(v)f + \varphi(v)\sigma\sqrt{f}}{2}\right), u\circ v\right]$,

(ii) $A^{1+s} = \left[\frac{N(u) - G\hat{\varphi}(v)\sigma\sqrt{f}}{2}, \frac{1+i}{2}(u'\circ v)\right]$,

(iii) $n(A) = A^{1+s^2} = \frac{1}{4}\left(u^2 - G\frac{N(v)f + \varphi(v)\sigma\sqrt{f}}{2}\right)$.

Using $E = [(x_0 + x_1\sqrt{f})/2, y_0 + y_1 i]$, we first calculate the coordinates of $\rho\varepsilon EE'$ by Lemma 1 (ii), where $\rho = sign(E') = |E'|/E'$. Put $\rho\varepsilon EE' = [(t_0 + t_1\sqrt{f})/2, r_0 + r_1 i]$. Since $Q_K = 2$, there is an integer γ of K such that $\gamma^2 = \rho\varepsilon EE'$. In the following we calculate the coordinate $[u, v]$ of this unit γ.

Since $u = (u_0 + u_1\sqrt{f})/2$ and $v = v_0 + v_1 i$, we obtain by Lemma 1 (i)

$$(2)\quad \begin{aligned} u_0^2 + u_1^2 f + 2G(v_0^2 + v_1^2)f &= 4t_0, \\ u_0u_1 + \sigma G\{a(v_0^2 - v_1^2) - 2bv_0v_1\} &= 2t_1, \\ u_0v_0 + \sigma u_1(av_0 - bv_1) &= 2r_0, \\ u_0v_1 - \sigma u_1(av_1 + bv_0) &= 2r_1. \end{aligned}$$

We note that integers f, a, b, G, σ, t_j and $r_j (j=0, 1)$ are given. It is obvious that the number of the integer solutions (u_0, u_1, v_0, v_1) of (2) is exactly two, and that if we denote by (u_0, u_1, v_0, v_1) an integer solution of (2), the other one is given by $(-u_0, -u_1, -v_0, -v_1)$. Therefore we may find an integer solution (u_0, u_1, v_0, v_1) of (2) such that $u_0 \geq 0$.

Now, from $\rho\varepsilon EE' = [u, v]^2$, we have $N(\varepsilon)EE'^2E'' = N(\varepsilon)n(E)E'^2 = ([u, v]^{1+s})^2$, so that $\lambda\rho E' = [u, v]^{1+s}$, where $\lambda = sign([u, v]^{1+s})$. So it follows from Lemma 1 (ii) that $N(u) = \lambda\rho x_0$ and $\sigma G\widehat{\varphi}(v) = \lambda\rho x_1$. Noting that $N(v)^2 f = \varphi(v)^2 + 4\widehat{\varphi}(v)^2$, we can eliminate v_0 and v_1 in the first two equations in (2). Namely we get

$$16t_0^2 - 8t_0(u_0^2 + u_1^2 f) + (u_0^2 + u_1^2 f)^2 = 4f(2t_1 - u_0u_1)^2 + 16fx_1^2.$$

Since $u_0^2 - u_1^2 f = 4\lambda\rho x_0$, we have $t_0(u_0^2 + u_1^2 f) - 2ft_1u_0u_1 = 2(t_0^2 + x_0^2 - ft_1^2 - fx_1^2)$. Putting $X = (u_0^2 + u_1^2 f)/2$ and $Y = u_0u_1$, we obtain

$$\begin{cases} X^2 - fY^2 = 4x_0^2, \\ t_0X - ft_1Y = 4N(t) + 4N(x), \end{cases}$$

where $N(t)$ and $N(x)$ are the norms of $t = (t_0 + t_1\sqrt{f})/2$ and $x = (x_0 + x_1\sqrt{f})/2$, respectively. Thus we have

$$N(t)X^2 - 2t_0(N(t) + N(x))X + 4(N(t) + N(x))^2 + ft_1^2x_0^2 = 0.$$

We now give a lemma.

Lemma 2. *Under the above assumption and notation, we have*

$$N(t) + 2N(x) = -4N(\varepsilon) + x_0^2.$$

Therefore

$$(N(t) + N(x))^2 - N(t)x_0^2 = G^2\widehat{\varphi}(y)^2 f.$$

Proof. By Lemma 1 (ii) we have $4N(t) = N(\varepsilon)(N(x)^2 - G^2\widehat{\varphi}(y)^2 f)$. Since $Q_K = 2$, $N(\varepsilon) = n(E)$. So Lemma 1 (iii) shows that $GN(y)f = -8N(\varepsilon) + x_0^2 - 2N(x)$ and $\sigma G\varphi(y) = x_0x_1$. Hence it follows from these equations that

$$\begin{aligned} 16N(t) + 32N(x) &= N(\varepsilon)\{4N(x)^2 + 32N(\varepsilon)N(x) + G^2\varphi(y)^2 f - G^2N(y)^2f^2\} \\ &= N(\varepsilon)(-64 + 16N(\varepsilon)x_0^2), \end{aligned}$$

so that the first equation in Lemma 2 is obtained. The second equation is easily proved by the first one.

Now, by Lemma 2, the solutions of the above quadratic equation are given by

$$X = \{(N(t) + N(x))t_0 \pm F\widehat{\varphi}(y)t_1\}/N(t). \tag{3}$$

Since $Q_K = 2$, at least one of these solutions is an integer. Hence, to get u_0, u_1 which satisfy (2), we may calculate them by the following system of equations for each integer solution X of (3), because $u_0^2 - u_1^2 f = \pm 4x_0$.

$$\begin{cases} u_0^2 = X \pm 2x_0, \\ u_1^2 f = X \mp 2x_0. \end{cases} \tag{4}$$

Here (4) formally means two systems of equations. However, since f is not a square of an integer, we may regard (4) as a system of equations. Therefore we obtain at most four integer solutions (u_0, u_1) of (4), because $u_0 \geq 0$ and the number of integer solutions X is at most two.

On the other hand, the latter two equations in (2) give

$$(5)\qquad \begin{aligned}(u_0^2 - u_1^2 f)v_0 &= 2r_0(u_0 - \sigma a u_1) + 2\sigma b r_1 u_1,\\ (u_0^2 - u_1^2 f)v_1 &= 2r_1(u_0 + \sigma a u_1) + 2\sigma b r_0 u_1.\end{aligned}$$

Hence, for each (u_0, u_1) which is an integer solution of (4), we examine whether or not v_0 and v_1 computed by (5) are both rational integers. If this is the case, we next examine whether or not (u_0, u_1, v_0, v_1) satisfies the former two equations in (2). In this way we obtain an integer solution of (2), since $Q_K = 2$. We denote it by (u_0, u_1, v_0, v_1) and put $\theta = [(u_0 + u_1\sqrt{f})/2, v_0 + v_1 i]$. Then θ and $-\theta$ are exactly two solutions of $\gamma^2 = \rho\varepsilon EE'$. Next we calculate the coordinates of $\theta E'''$ by a formula in [1], p. 35 and calculate the approximate value of $\theta E'''$ by cosine sums Ω and Ω' defined in [1], §8. Then we can obtain

$$(6)\qquad E^* = \begin{cases} \theta E''' & \text{if } \theta E''' > 0,\\ -\theta E''' & \text{otherwise},\end{cases}$$

because $\theta E'''$ satisfies (1), i.e., $\theta E'''\theta' E = \pm E$ and $\theta E'''\theta'' E' = \pm\varepsilon$.

Therefore we complete the proof of our algorithm.

3. Table of E and E^*. In the appendix of [1], Hasse tabulated the coordinates of E, E^*, the class number h of K and Q_K for a real cyclic biquadratic field K with conductor $F < 100$. There are some errors in his table. Using our algorithm, we give a table of the fundamental unit E^* for a real cyclic biquadratic field K with conductor $F < 300$, wherein the symbol "†" denotes the correction of the error in Hasse's table. As to the values of Ω and Ω', we have $\{|\Omega|, |\Omega'|\} = \{\alpha, \beta\}$ and $4\Omega\Omega' = -2bG\sigma\sqrt{f}$ by [1], §8, where α and β are given by

$$\alpha = \sqrt{G(f + |a|\sqrt{f})/2}, \qquad \beta = \sqrt{G(f - |a|\sqrt{f})/2}.$$

So we can write the values of Ω and Ω' by α and β. Our table consists of the following: 1. the conductor F of K, 2. the conductor f of k, 3. the basis number $a + bi$ of K, 4. the fundamental unit ε of k, 5. the values of Ω and Ω', 6. the relative fundamental unit E of K, 7. the relative norm $n(E)$ of E, 8. the sign ρ of E', 9. the integer solution X of (3), 10. the coordinates of θ, 11. the coordinates of E^*, 12. the relative norm $n(E^*)$ of E^*, 13. $E^*E^{*\prime}$.

1	2	3	4	5	6	7	8
F	f	$a+bi$	ε	(Ω, Ω')	E	$n(E)$	ρ
16	8	$2+2i$	$1+\sqrt{2}$	$(\alpha, -\beta)$	$[2+2\sqrt{2}, 1-i]$	-1	$+1$
17	17	$1+4i$	$4+\sqrt{17}$	(β, α)	$[(1+\sqrt{17})/2, i]$	-1	-1
41	41	$5+4i$	$32+5\sqrt{41}$	$(-\beta, -\alpha)$	$[(5+\sqrt{41})/2, -i]$	-1	-1
73	73	$-3+8i$	$1068+125\sqrt{73}$	(α, β)	$[92+12\sqrt{73}, 18+14i]$	-1	† -1
80	8	$2+2i$	$1+\sqrt{2}$	(β, α)	$[14+10\sqrt{2}, 1+3i]$	-1	-1
85	17	$1+4i$	$4+\sqrt{17}$	$(\alpha, -\beta)$	$[76+20\sqrt{17}, 14-10i]$	-1	-1
89	89	$5+8i$	$500+53\sqrt{89}$	(β, α)	$[68+20\sqrt{89}, 2+30i]$	-1	-1
97	97	$9+4i$	$5604+569\sqrt{97}$	$(-\beta, -\alpha)$	† $[(9+\sqrt{97})/2, -i]$	-1	† -1
113	113	$-7+8i$	$776+73\sqrt{113}$	(α, β)	$[4264+400\sqrt{113}, 730+330i]$	-1	$+1$
137	137	$-11+4i$	$1744+149\sqrt{137}$	$(-\alpha, -\beta)$	$[(11+\sqrt{137})/2, -1]$	-1	$+1$

193	193	$-7+12i$	$1764132 + 126985\sqrt{193}$	(α, β)	$[(903+63\sqrt{193})/2, 56+31i]$	-1	$+1$
208	8	$2+2i$	$1+\sqrt{2}$	$(-\beta, -\alpha)$	$[62+26\sqrt{2}, -1-7i]$	-1	-1
233	233	$13+8i$	$23156+1517\sqrt{233}$	$(-\beta, -\alpha)$	$[101876+6676\sqrt{233}, -3634-12846i]$	-1	-1
241	241	$-15+4i$	$71011068 + 4574225\sqrt{241}$	$(-\alpha, -\beta)$	$[(15+\sqrt{241})/2, -1]$	-1	$+1$
257	257	$1+16i$	$16+\sqrt{257}$	(β, α)	$[191176+11752\sqrt{257}, 16338+17138i]$	-1	$+1$
272	136	$-6+10i$	$35+6\sqrt{34}$	(α, β)	$[610+108\sqrt{34}, 66+36i]$	$+1$	-1
272	136	$10-6i$	$35+6\sqrt{34}$	$(\beta, -\alpha)$	$[66+12\sqrt{34}, 2-8i]$	$+1$	-1
281	281	$5+16i$	$1063532 + 63445\sqrt{281}$	$(-\beta, -\alpha)$	$[43380+2588\sqrt{281}, -3066-4170i]$	-1	$+1$

9	10	11	12	13
X	θ	E^*	$n(E^*)$	$E^*E^{*\prime}$
8	$[2, 1]$	$[2+2\sqrt{2}, 1]$	$+\varepsilon$	$-E$
66	$[4+\sqrt{17}, 1+i]$	$[1, 1+i]$	$-\varepsilon$	$+E$
666	$[13+2\sqrt{41}, -1-3i]$	$[6+\sqrt{41}, -1-3i]$	$-\varepsilon$	$-E$
4418036	$[1051+123\sqrt{73}, 202+140i]$	$[93+11\sqrt{73}, 20+14i]$	$-\varepsilon$	$-E$
88	$[6+2\sqrt{2}, i]$	† $[2+4\sqrt{2}, i]$	† $-\varepsilon$	† $-E$
8532	$[47+11\sqrt{17}, 8-6i]$	$[1+3\sqrt{17}, 2]$	$-\varepsilon$	$-E$
30980628	$[2783+295\sqrt{89}, 286+516i]$	$[15+\sqrt{89}, 4+6i]$	$-\varepsilon$	† $+E$
155218	$[197+20\sqrt{97}, -7-33i]$	† $[128+13\sqrt{97}, -7-33i]$	$-\varepsilon$	$-E$
158928292	$[6303+593\sqrt{113}, 1080+490i]$	$[529+49\sqrt{113}, 90+40i]$	$+\varepsilon$	$+E$
26874	$[82+7\sqrt{137}, -17-3i]$	$[117+10\sqrt{137}, -17-3i]$	$+\varepsilon$	$-E$
43784723698	$[104624+7531\sqrt{193}, 13063+7503i]$	$[7613+548\sqrt{193}, 921+529i]$	$+\varepsilon$	$-E$
1048	$[18-10\sqrt{2}, 2-i]$	$[38+28\sqrt{2}, -2-5i]$	$-\varepsilon$	$-E$
271347635604	$[260455+17063\sqrt{233}, -9294-32836i]$	$[9063+593\sqrt{233}, -324-1142i]$	$-\varepsilon$	$+E$
1636687906	$[20228+1303\sqrt{241}, -2999-393i]$	$[26329+1696\sqrt{241}, -2999-393i]$	$+\varepsilon$	$-E$
33764767812	$[91877+5731\sqrt{257}, 7848+8354i]$	$[-2835+181\sqrt{257}, -258+248i]$	$+\varepsilon$	$-E$
4616	$[42+4\sqrt{34}, 3+3i]$	$[654+112\sqrt{34}, 69+39i]$	$-\varepsilon$	$+E$
2440	$[26+4\sqrt{34}, 1-3i]$	$[94+16\sqrt{34}, 3-11i]$	$-\varepsilon$	$+E$
59390491284	$[121851+7269\sqrt{281}, -8612-11714i]$	$[378627+22587\sqrt{281}, -26758-36396i]$	$+\varepsilon$	$-E$

Reference

[1] Hasse, H.: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. Abh. Deutsch. Akad. Wiss. Berlin, Math. Nat. Kl., 1948, Nr. 2, 3–95 (1950).