On the units and the class numbers of certain composita of two quadratic fields

By Shin-ichi KATAYAMA,*) Claude LEVESQUE,**) and Toru NAKAHARA***)

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1999)

1. Preliminaries. Let k_1 be a real quadratic field and ε_1 (>1) be the fundamental unit of k_1. We shall fix a unit $\eta_1 = \varepsilon_1^{2i+1}$, which is an odd power of the fundamental unit ε_1 with $i \geq 0$. Then there exists some positive integer M such that η_1 is written in the form

$$\eta_1 = \frac{M + \sqrt{M^2 \pm 4}}{2}.$$

Let $\bar{\eta}_1$ be the field conjugate of η_1. Put $D = M^2 \pm 4$. Then D is not necessarily square-free, and we denote the square-free part of D by D_0. When we use the notation $\pm y$ or $\mp z$, $+y$ and $-z$ correspond to the upper case $D = M^2 + 4$, which will be called the *plus case*, and $-y$ and $+z$ correspond to the lower case $D = M^2 - 4$, which will be called the *minus case*.

Put

$$g_n = \eta_1^n + \bar{\eta}_1^n, \qquad h_n = \frac{\eta_1^n - \bar{\eta}_1^n}{\sqrt{D}}.$$

Then the sequences $\{g_n\}_{n\in\mathbf{N}}$ and $\{h_n\}_{n\in\mathbf{N}}$ are the non-degenerated second order linear recurrence sequences defined by

$$g_{n+2} = Mg_{n+1} \pm g_n, \quad h_{n+2} = Mh_{n+1} \pm h_n,$$

with the initial terms $g_0 = 2$, $g_1 = M$ and $h_0 = 0$, $h_1 = 1$.

The purpose of this note is to report our results on the class number h_K and the unit group E_K of the biquadratic field $K = \mathbf{Q}(\sqrt{D}, \sqrt{h_{2n+1}^2 - 1})$: see Theorems 1 and 2. Only sketches of proofs will be provided and details will be published elsewhere.

For any a, $b \in \mathbf{Z} \setminus \{0\}$, we put $a \sim b$ if and only if ab is a perfect square. So

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \sim \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \Longleftrightarrow a_1 \sim a_2 \text{ and } b_1 \sim b_2.$$

Moreover, $M^2 - D = \mp 4$ and $g_{2n+1}^2 - Dh_{2n+1}^2 = \mp 4$ imply

$$g_{2n+1}^2 - M^2 = D(h_{2n+1}^2 - 1).$$

Then we shall verify that $h_{2n+1}^2 - 1 \not\sim 1$ and $h_{2n+1}^2 - 1 \not\sim D$ except for finitely many indices n. So except for finitely many indices n, we will construct a family of real bicyclic biquadratic fields

$$K = \mathbf{Q}\left(\sqrt{D}, \sqrt{h_{2n+1}^2 - 1}\right) \quad (n \geq 1).$$

Then K has three subfields:

$$k_1 = \mathbf{Q}\left(\sqrt{D}\right), \quad k_2 = \mathbf{Q}\left(\sqrt{h_{2n+1}^2 - 1}\right),$$
$$k_3 = \mathbf{Q}\left(\sqrt{g_{2n+1}^2 - M^2}\right).$$

We have a unit η_2 in k_2 defined by

$$\eta_2 = h_{2n+1} + \sqrt{h_{2n+1}^2 - 1},$$

and we will denote by ε_2 the fundamental unit of k_2.

Concerning the recurrence sequence $\{g_n\}_{n\in\mathbf{N}}$, one can verify $M | g_{2n+1}$ by induction. So we also have a unit η_3 in $k_3 = \mathbf{Q}\left(\sqrt{(g_{2n+1}/M)^2 - 1}\right)$, namely

$$\eta_3 = g_{2n+1}/M + \sqrt{(g_{2n+1}/M)^2 - 1},$$

and we will denote by ε_3 the fundamental unit of k_3.

Let E be the group $\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$. Then the group index $[E_K : E]$ is called the unit index of K and is known to be $1, 2$ or 4 in general. Let us quote a result of Shorey-Stewart [14].

Lemma 1. *Let d be an integer > 1. Then there exists a constant C_1, which is effectively computable in terms of M and d such that for any $n \geq C_1$,*

$$g_n \not\sim d \quad \text{and} \quad h_n \not\sim d.$$

Let us list several properties of the above two linear recurrences $\{g_n\}_{n\in\mathbf{N}}$ and $\{h_n\}_{n\in\mathbf{N}}$.

Proposition 1. *For any index $n \geq 0$,*

(i) $h_{2n+1} + (\mp 1)^n = g_n h_{n+1}$,
(ii) $h_{2n+1} - (\mp 1)^n = g_{n+1} h_n$,
(iii) $g_{2n+1} + (\mp 1)^n M = g_n g_{n+1}$,

*) Department of Mathematical Sciences, Tokushima University, 1-1 Minamijosanjima-cho, Tokushima 770–8502.
**) Département de Mathématiques et de Statistique, Université Laval, Canada.
***) Department of Mathematics, Saga University, 1 Honjo-cho, Saga 840–8502.

(iv) $g_{2n+1} - (\mp 1)^n M = (M^2 \pm 4)h_n h_{n+1}$,
(v) $(h_n, h_{n+1}) = 1$ *and* $(g_n, g_{n+1}) = (M, 2)$,
(vi) $h_{n+2} \pm h_n = g_{n+1}$,
(vii) $(g_n, h_{n+1}) = \begin{cases} 1 & \textit{if } n \textit{ is even,} \\ M & \textit{if } n \textit{ is odd,} \end{cases}$
(viii) $(g_{n+1}, h_n) = \begin{cases} M & \textit{if } n \textit{ is even,} \\ 1 & \textit{if } n \textit{ is odd,} \end{cases}$
(ix) $(g_n, MD) = \begin{cases} (2, M) & \textit{if } n \textit{ is even,} \\ M & \textit{if } n \textit{ is odd.} \end{cases}$

Using the above lemma and proposition, we obtain the following theorem.

Theorem 1. *There exists a computable constant N_0 such that for all $n \geq N_0$, $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ is a fundamental system of units of K and $N\varepsilon_2 = N\varepsilon_3 = +1$. Moreover, the class number h_K of K verifies the identity*

$$h_K = \frac{1}{4} h_{k_1} h_{k_2} h_{k_3},$$

where h_{k_i} is the class number of the quadratic subfield k_i $(1 \leq i \leq 3)$.

Sketch of the proof. Let us note that

$$\sqrt{\frac{x + \sqrt{x^2 - r^2}}{r}} = \frac{x + r + \sqrt{x^2 - r^2}}{\sqrt{2r(x + r)}}.$$

Step 1. One can easily show

$$[K : \mathbf{Q}] = 4 \iff h_{2n+1}^2 - 1 \not\sim 1 \text{ and } h_{2n+1}^2 - 1 \not\sim D.$$

Since $h_{2n+1}^2 - 1 = h_{2n} h_{2n+2}$ with $(h_{2n}, h_{2n+2}) = M$, one sees that

$$h_{2n+1}^2 - 1 \sim 1 \iff \begin{pmatrix} h_{2n} \\ h_{2n+2} \end{pmatrix} \sim \begin{pmatrix} M \\ M \end{pmatrix}$$

and

$$h_{2n+1}^2 - 1 \sim D \iff \begin{pmatrix} h_{2n} \\ h_{2n+2} \end{pmatrix} \sim \begin{pmatrix} d_1 M \\ d_2 M \end{pmatrix},$$

where $d_1 d_2 = D_0$ with $(d_1, d_2) = 1$. From Lemma 1, one can easily verify that there exists a computable constant N_1 such that for $n \geq N_1$, $[K : \mathbf{Q}] = 4$.

Step 2. One can see

$$\eta_2 \in \langle \varepsilon_2^2 \rangle \iff h_{2n+1} + 1 \sim 2 \text{ or } h_{2n+1} - 1 \sim 2.$$

Then the above last conditions can be reduced to one of the following conditions:

$$\begin{pmatrix} g_n \\ h_{n+1} \end{pmatrix} \sim \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} M \\ 2M \end{pmatrix} \text{ or } \begin{pmatrix} 2M \\ M \end{pmatrix},$$

or

$$\begin{pmatrix} g_{n+1} \\ h_n \end{pmatrix} \sim \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} M \\ 2M \end{pmatrix} \text{ or } \begin{pmatrix} 2M \\ M \end{pmatrix}.$$

From Lemma 1, there exists a computable constant $N_2 \geq N_1$ such that for $n \geq N_2$, $\eta_2 \notin \langle \varepsilon_2^2 \rangle$. Similarly there exists a computable constant $N_3 \geq N_2$ such that for $n \geq N_3$, $\eta_3 \notin \langle \varepsilon_3^2 \rangle$.

Step 3. Let $n \geq N_3$. Then in the minus case one sees that

$$\begin{aligned} \sqrt{\varepsilon_1} \in E_K &\iff \sqrt{\eta_1} \in E_K \\ &\iff M + 2 \sim h_{2n+1}^2 - 1 \text{ or} \\ &\qquad M - 2 \sim h_{2n+1}^2 - 1. \end{aligned}$$

It is obvious that $\sqrt{\varepsilon_1} \notin E_K$ in the plus case. So in the same way as in Step 1, we can show that there exists a computable constant $N_4 \geq N_3$ such that for $n \geq N_4$, $\sqrt{\varepsilon_1} \notin E_K$. In the same way as above, one can see that there exists an effectively computable constant $N_0 \geq N_4$ such that, for $n \geq N_0$, $\sqrt{\varepsilon_2} \notin E_K$ and $\sqrt{\varepsilon_3} \notin E_K$ and $\sqrt{\varepsilon_1 \varepsilon_2} \notin E_K$ and $\sqrt{\varepsilon_2 \varepsilon_3} \notin E_K$ and $\sqrt{\varepsilon_1 \varepsilon_3} \notin E_K$ and $\sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3} \notin E_K$. In short, $E_K = E$ for $n \geq N_0$. □

2. The case of an odd integer M. In this section, we shall restrict ourselves to the case where M is odd, i.e. $D = M^2 \pm 4$ is odd. We will see that the constant N_0 in Theorem 1 can be taken to be 7; we will also exhibit fundamental systems of units for $1 \leq n \leq 6$. First we quote the following results of Cohn [3, 4] and Ribenboim–MacDaniel [12].

Lemma 2. *If $M = 1$ in the plus case and $r > 0$, then*

$$\begin{aligned} g_r \sim M &\iff r = 1 \text{ or } 3, \\ g_r \sim 2M &\iff r = 6. \end{aligned}$$

If $M = 3$ in the plus case and $r > 0$, then $g_r \not\sim 2$, $g_r \not\sim 2M$, and

$$\begin{aligned} g_r \sim 1 &\iff r = 3, \\ g_r \sim M &\iff r = 1. \end{aligned}$$

If $M = 3$ in the minus case and $r > 0$, then $g_r \not\sim 1$, $g_r \not\sim 2M$, and

$$\begin{aligned} g_r \sim 2 &\iff r = 3, \\ g_r \sim M &\iff r = 1. \end{aligned}$$

If $M = 5$ in the plus case and $r > 0$, then $g_r \not\sim 1$, $g_r \not\sim 2M$, and

$$\begin{aligned} g_r \sim 2 &\iff r = 6, \\ g_r \sim M &\iff r = 1. \end{aligned}$$

If $M = 27$ in the minus case and $r > 0$, then $g_r \not\sim 1$, $g_r \not\sim 2M$, and

$$\begin{aligned} g_r \sim M &\iff r = 1, \\ g_r \sim 2 &\iff r = 3. \end{aligned}$$

Elsewhere $g_r \not\sim 2$, $g_r \not\sim 2M$, *and*

$$g_r \sim 1 \iff r = 1 \ (\textit{and } M \sim 1),$$
$$g_r \sim M \iff r = 1.$$

Using this lemma, one can get the following result.

Theorem 2. *Let* M (*and* $D = M^2 \pm 4$) *be odd. Then the unit group* E_K *of* K *is given by*

$$E_K = \begin{cases} \langle -1, \varepsilon_1, \sqrt{\varepsilon_2}, \varepsilon_3 \rangle \\ \quad \textit{if } n = 5 \textit{ with } M = 1 \textit{ in the plus case}, \\ \langle -1, \varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3} \rangle \\ \quad \textit{if } n = 2 \textit{ with } M \textit{ such that } M^2 = 2x^2 \mp 1, \\ \langle -1, \varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3} \rangle \\ \quad \textit{if} \begin{cases} n = 1 \textit{ for any } M, \\ n = 6 \textit{ with } M = 1 \textit{ in the plus case}, \end{cases} \\ \langle -1, \varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_1\varepsilon_3} \rangle \\ \quad \textit{if } n = 2 \textit{ with } M = 5 \textit{ in the minus case}, \\ \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle \\ \quad \textit{otherwise}. \end{cases}$$

The fact $\sqrt{\varepsilon_1\varepsilon_3} \notin E_K$ except for $n = 2$ with $M = 5$ in the minus case can be shown in the following way. First we see

$$\sqrt{\varepsilon_1\varepsilon_3} \in E_K$$
$$\iff \begin{cases} g_n g_{n+1} \sim 2M(M+2) \text{or } 2M(M-2) \\ \text{or} \\ h_n h_{n+1} \sim 2M(M+2) \text{ or } 2M(M-2). \end{cases}$$

By Lemma 2, one sees that the possible index $n = 2$ and M must satisfy the conditions $M+1 \sim 6$, and $M-1 \sim 1$ and $M-2 \sim 3$. Put $M-1 = x^2$, $M-2 = 3y^2$ and $M+1 = 6z^2$. Then the existence of such an integer M is equivalent to the existence of integer solutions of the following simultaneous Fermat-Pell equations

$$\begin{cases} x^2 - 3y^2 = 1, \\ y^2 - 2z^2 = -1. \end{cases}$$

Let us rather consider the following equivalent equations

$$(1) \qquad \begin{cases} x^2 - 3y^2 = 1, \\ w^2 - 2y^2 = 2, \end{cases}$$

where $w = 2z$. With the help of a result of Rickert (see (1.7) in [13]), we will show that these equations have only one positive integer solution: $(x, y, w) = (2, 1, 2)$.

Lemma 3 (Rickert)**.** *Let* u, v *be non-zero integers. All integer solutions* x, y, z *of the following simultaneous Fermat-Pell equations*

$$\begin{cases} x^2 - 3y^2 = u \\ z^2 - 2y^2 = v \end{cases}$$

satisfy

$$\max\{|x|, |y|, |z|\} \le (10^7 \max\{|u|, |v|\})^{12}.$$

Then to find the positive integer solutions of (1) is equivalent to finding all non-negative integers m, n for which

$$\begin{cases} x = r_n = ((2+\sqrt{3})^n + (2-\sqrt{3})^n)/2, \\ y = s_n = ((2+\sqrt{3})^n - (2-\sqrt{3})^n)/(2\sqrt{3}), \\ y = p_m = ((1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1})/2, \\ w = q_m = ((1+\sqrt{2})^{2m+1} - (1-\sqrt{2})^{2m+1})/\sqrt{2}. \end{cases}$$

From Lemma 3, we see that $(1+\sqrt{2})^{2m} < p_m \le (10^7 \times 2)^{12}$ for $m \ge 1$ implies $m < (42\log(10) + 6\log(2))/\log(1+\sqrt{2}) = 114.443\cdots < 115$. We have checked that for $0 \le m \le 114$, $p_m = s_n$ only for $m = 0$, $n = 1$, i.e., the simultaneous Fermat-Pell equations (1) have only the positive integer solution $(x, y, w) = (2, 1, 2)$.

Acknowledgement. We would like to express our warmest thanks to Prof. I. Wakabayashi, who suggested us to use Rickert's result to simplify our first proof for solving the above Fermat-Pell equations.

References

[1] A. Baker and H. Davenport: The equations $3x^2 - 2 = y^2$, and $8x^2 - 7 = z^2$. Quart. J. Math. Oxford, (2), **20**, 127–137 (1969).
[2] R. T. Bumby: The diophantine equation $3x^4 - 2y^2 = 1$. Math. Scand., **21**, 144–148 (1967).
[3] J. H. E. Cohn: Eight diophantine equation. Proc. London Math. Soc., **16**, 153–166 (1966).
[4] J. H. E. Cohn: Squares in some recurrent sequences. Pacific J. Math., **41**, 631–646 (1972).
[5] S. Katayama and S.-G. Katayama: Fibonacci, Lucas and Pell numbers and class numbers of bicyclic biquadratic. Math. Japon., **42**, 121–126 (1995).
[6] C. Levesque: Systèmes fondamentaux d'unités de certains corps de degré 4 et de degré 8 sur $\boldsymbol{Q}$. Canad. J. Math., **XXXIV**, nr. 5, 1059–1090 (1982).
[7] W. Ljunggren: Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper. Oslo Vid. Akad. Strifter, **1**, nr. 12 (1936).
[8] K. Nakamula and A. Pethő: Squares in binary recurrence sequences (preprint).

[9] A. Pethő: Perfect powers in second order linear recurrences. J. Number Theory, **15**, 5–13 (1982).
[10] A. Pethő: Full cubes in the Fibonacci sequence. Publ. Math. Debrecen, **30**, 1–2, 117–127 (1983).
[11] P. Ribenboim: The Book of Prime Number Records, 2nd ed., Springer-Verlag, New York (1989).
[12] P. Ribenboim and W. L. McDaniel: The square terms in Lucas sequences. J. Number Theory, **58**, 104–123 (1996).
[13] J. H. Rickert: Simultaneous rational approximations and related Diophantine equations. Math. Proc. Cambridge Philos. Soc., **113**, 461–472 (1993).
[14] T. N. Shorey and C. L. Stewart: On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrences. Math. Scand., **52**, 24–36 (1983).