J.Math.Univ.Tokushima
Vol.35 (2001), 9-15

A Conjecture on Fundamental Units of Real Quadratic Fields

By

Shin-ichi KATAYAMA

Faculty of Integrated Arts and Sciences
The University of Tokushima
1-1, Minamijosanjima-cho
Tokushima-shi, 770-8502, JAPAN
e-mail address: *katayama@ias.tokushima-u.ac.jp*
(Received September 14, 2001)

Abstract

In our previous paper [6], we have investigated a certain family of real bicyclic biquadratic fields and proved that they have an explicit fundamental sytem of units assuming the ABC conjecture. In this paper we will generalize some results of [6] and state a conjecture on the fundamental units of a certain family of real quadratic fields and give numerical examples which support this conjecture.

2000 Mathematics Subject Classification. Primary 11R27; Secondary 11R11, 11B39

Introduction

The purpose of this paper is to generalize some of the results obtained in [6] and to give a conjecture on the fundamental units of a certain family of real quadratic fields related to Fibonacci numbers. We shall also give several numerical examples which support this conjecture.

Let k_1 be a fixed real quadratic field and let

$$\eta_1 = (M + \sqrt{M^2 - 4e})/2 \quad > \quad 1$$

be a fixed unit of k_1 with norm $N\eta_1 = e$, where M is a positive integer. Let $\bar{\eta}_1$

be the field conjugate of η_1 and put

$$g_n(M,e) = \eta_1^n + \bar{\eta}_1^n, \qquad h_n(M,e) = \frac{\eta_1^n - \bar{\eta}_1^n}{\sqrt{M^2-4e}}.$$

Then the sequences $\{g_n(M,e)\}_{n\in\mathbf{N}}$ and $\{h_n(M,e)\}_{n\in\mathbf{N}}$ are the non-degenerate binary recurrence sequences stisfying

$$g_{n+2}(M,e) = Mg_{n+1}(M,e) - eg_n(M,e),$$

$$h_{n+2}(M,e) = Mh_{n+1}(M,e) - eh_n(M,e),$$

with initial terms $g_0(M,e) = 2, g_1(M,e) = M$ and $h_0(M,e) = 0, h_1(M,e) = 1$. If there is no danger of confusion, we simply write $g_n(M,e)$ and $h_n(M,e)$ for g_n and h_n, respectively.

Firstly we shall remind the statement of the ABC conjecture and reproduce several propositions of [6] which we will need here.

The ABC **conjecture**. For any $\varepsilon > 0$, there exists a constant $K_0 > 0$ (depending only on ε) such that if a, b, c are non-zero relatively prime integers with $a + b + c = 0$, then

$$\max\{|a|, |b|, |c|\} \leq K_0 r^{1+\varepsilon},$$

where $r = rad(abc) = \prod_{p|abc} p$ (p: prime integer).

We note that any positive integer m can be written in the form $m = s(m)q^2(m)$, where $s(m)$ is the squarefree part of m. The following proposition is a corollary of a more general result of P. Ribenboim and G. Walsh [9, Theorem 2]:

Proposition 1. (*Assuming the ABC conjecture*).
For any $\varepsilon > 0$,

$$q(h_n) \leq h_n^{\varepsilon} \quad \textit{and} \quad q(g_n) \leq g_n^{\varepsilon}$$

except for finitely many indices n.

Since $h_n = s(h_n)q^2(h_n)$, we have $q(h_n) \leq h_n^{\varepsilon}$ if and only if $(q(h_n))^{1/\varepsilon - 2} \leq s(h_n)$. From the fact $1/\varepsilon - 2 \to \infty$ as $\varepsilon \to +0$, one sees that for any $m > 0$,

$$q^m(h_n) \leq s(h_n) \tag{1}$$

except for finitely many indices n under the ABC conjecture. Taking $m = 2$ in (1), we have $h_n = s(h_n)q^2(h_n) \leq s^2(h_n)$. The fact that $h_n \to \infty$ as $n \to \infty$ implies the following proposition.

Proposition 2. *(Assuming the ABC conjecture).*
For any constant $C > 0$,

$$C \leq s(h_n)$$

except for finitely many indices n.

One can easily verify that for any positive integers x and y,

$$(2) \qquad \begin{array}{rcl} s(xy) = s(x)s(y)/(s(x), s(y))^2 & \geq & s(x)s(y)/(x, y)^2, \\ q(xy) = q(x)q(y)(s(x), s(y)) & \leq & q(x)q(y)(x, y). \end{array}$$

Combining the fact $h_{2n+1}^2 - 1 = h_{2n}h_{2n+2}$ with $(h_{2n}, h_{2n+2}) = M$ and Proposition 2, we have that for any $m > 0$,

$$s(h_{2n})s(h_{2n+2}) \geq M^{2m+4}$$

except for finitely many indices n. The inequality (1) imlplies $s(h_{2n}) \geq q^{2m}(h_{2n})$ and $s(h_{2n+2}) \geq q^{2m}(h_{2n+2})$ except for finitely many indices n. Using (2), we have

$$\begin{array}{rcl} s^2(h_{2n+1}^2 - 1) & = & s^2(h_{2n}h_{2n+2}) \\ & \geq & s^2(h_{2n})s^2(h_{2n+2})/M^4 \\ & \geq & q^{2m}(h_{2n})q^{2m}(h_{2n+2})s(h_{2n})s(h_{2n+2})/M^4 \\ & = & (Mq(h_{2n})q(h_{2n+2}))^{2m}s(h_{2n})s(h_{2n+2})/M^{2m+4} \\ & \geq & q^{2m}(h_{2n}h_{2n+2}) \\ & = & q^{2m}(h_{2n+1}^2 - 1). \end{array}$$

Thus assuming the ABC conjecture, we have for any $m > 0$,

$$s(h_{2n+1}^2 - 1) \geq q^m(h_{2n+1}^2 - 1)$$

except for finitely many indices n.

Similarly the fact $g_{2n+1}^2 - M^2 = (M^2 \pm 4)(h_{2n+1}^2 - 1)$ implies that for any $m > 0$,

$$s((g_{2n+1}/M)^2 - 1) \geq q^m((g_{2n+1}/M)^2 - 1)$$

except for finitely many indices n.

For the special case $m = 2$, we have

$$\begin{array}{rcl} s(h_{2n+1}^2 - 1) & \geq & q^2(h_{2n+1}^2 - 1), \\ s((g_{2n+1}/M)^2 - 1) & \geq & q^2((g_{2n+1}/M)^2 - 1), \end{array}$$

except for finitely many indices n. From the results of [5], we know that the units η_2 and η_3 are the odd powers of the fundamental units except for finitely many indices. Hence suppose

$$\eta_2 = ((t + \sqrt{t^2 - 4})/2)^{2l+1} \text{ for } l \geq 1.$$

Then $h_{2n+1}^2 - 1 = h_{2l+1}^2(t)(t^2-4)/4$ implies

$$\begin{array}{rcl} q^2(h_{2n+1}^2 - 1) & \geq & ((h_{2l+1}(t)/2)^2 \geq ((h_3(t)/2)^2 \\ & = & ((t^2-1)/2)^2 > t^2 - 4 \\ & \geq & s(t^2-4) \geq s(h_{2n+1}^2 - 1). \end{array}$$

Similarly we have the inequality $q^2((g_{2n+1}/M)^2 - 1) > s((g_{2n+1}/M)^2 - 1)$. Combining these inequalities, we have the following proposition, which is Theorem 1 of our previous paper [6].

Proposition 3 (*Assuming the ABC conjecture*).

$$\begin{array}{l} \eta_2 = h_{2n+1} + \sqrt{h_{2n+1}^2 - 1} \\ (resp.\ \eta_3 = g_{2n+1}/M + \sqrt{(g_{2n+1}/M)^2 - 1}) \end{array}$$

is the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{h_{2n+1}^2 - 1})$ (*resp.* $\boldsymbol{Q}(\sqrt{g_{2n+1}^2 - M^2})$), *except for finitely many indices n.*

Now we shall need the following elementary lemma.

Lemma 1. *For any $n \in N$, we have*

$$h_n^2 - e^{n-1} = h_{n-1} \cdot h_{n+1}.$$

Proof. Firstly one can easily verify $h_1^2 - e^0 = 1 - 1 = 0 = 0 \cdot M = h_0 \cdot h_2$ and
$h_2^2 - e = M^2 - e = 1 \cdot (M^2 - e) = h_1 \cdot h_3$, that is, the formula is true for the cases $n = 1$ and $n = 2$.

Assume the formula is true for $n-1$, that is, $h_{n-1}^2 - e^{n-2} = h_{n-2} \cdot h_n$. Then we have

$$\begin{array}{rcl} h_{n+1}^2 - e^n & = & (Mh_n - eh_{n-1})^2 - e^n \\ & = & M^2h_n^2 - 2Meh_nh_{n-1} + (h_{n-1}^2 - e^{n-2}) \\ & = & M^2h_n^2 - 2Meh_nh_{n-1} + h_n \cdot h_{n-2} \\ & = & h_n(M(Mh_n - eh_{n-1}) - e(Mh_{n-1} - eh_{n-2})) \\ & = & h_n(Mh_{n+1} - eh_n) \\ & = & h_n \cdot h_{n+2}, \end{array}$$

which completes the proof.

Combining these, we shall generalize some part of Proposition 3 as follows.

Theorem. (Assuming the *ABC* conjecture).
For any $n \geq 2$, $\eta_2 = h_n + \sqrt{h_n^2 - e^{n-1}}$ is the fundamental unit of the real

quadratic field $\boldsymbol{Q}(\sqrt{h_n^2 - e^{n-1}})$ *except for finitely many indices* n.

Proof. Because of Proposition 3, we may consider only the case $n = 2l$. From Lemma 1, we see $h_{2l}^2 - e^{2l-1} = h_{2l-1}h_{2l+1}$ with $(h_{2l-1}, h_{2l+1}) = (h_{2l-1}, h_{2l-3}) = \cdots = (h_3, h_1) = 1$. Thus we have

$$q(h_{2l}^2 - e^{2l-1}) = q(h_{2l-1})q(h_{2l+1})$$

and

$$s(h_{2l}^2 - e^{2l-1}) = s(h_{2l-1})s(h_{2l+1}).$$

From (2), we have

$$s(h_{2l}^2 - e^{2l-1}) > q^2(h_{2l}^2 - e^{2l-1})$$

except for finitely many indices n, which completes the proof.

A conjecture and some numerical edidence

We shall write the results of Theorem in another statement as follows:

Assuming the ABC conjecture, for any M *there exists a positive integer* $N(M, e)$ *such that*

$$h_n + \sqrt{h_n^2 + e^{n-1}}$$

is the fundamental unit of the real quadratic fields $\boldsymbol{Q}(\sqrt{h_n^2 - e^{n-1}})$ *for any* $n \geq N(M, e)$.

It is worth noting that since the statement of the *ABC* conjecture is ineffective, the results of Proposition 3 and Theorem are also ineffective. So it is difficult to determine $N(M, e)$ in general. But in [11], G. Walsh proved the following result using Cohn's results [3]:

Proposition 4. *For the case* $M = 2$, $e = -1$ *and* $n \geq 2$, *the unit*

$$h_n(2, -1) + \sqrt{h_n^2(2, -1) + (-1)^n}$$

is the fundamental unit of $\boldsymbol{Q}(\sqrt{h_n^2(2, -1) + (-1)^n})$ *except for* $n = 2$ *and* $n = 6$. *For* $n = 2$ *and* 6, $h_n(2, -1) + \sqrt{h_n^2(2, -1) + (-1)^n}$ *is the third power of the fundamental unit.*

Remark. From the above proposition, we know $N(2, -1) = 7$. Let F_n be the nth usual Fibonacci number. In [2], Y.J. Choie claimed that $N(1, -1) = 2$. However she used the fact that $F_n^2 + (-1)^n$ is squarefree, but it is not always of the case. Hence all her results on fundamental units and class numbers are not proved for the real quadratic fields though some results are true for some orders of the real quadratic fields.

Thus, except for the case $N(2,-1)$ we don't know any $N(M,e)$, but we would like to state the following conjecture:

Conjecture. *For any $n \geq 2$, $F_n + \sqrt{F_n + (-1)^n}$ is the fundamental unit of the real quadratic fields $\boldsymbol{Q}(\sqrt{F_n^2 + (-1)^n})$.*

Here we shall give several numerical data which support the above conjecture. We have checked the conjecture holds for any n, $2 \leq n \leq 701$ with two different methods. We verified $s(F_n) > q^2(F_n)$ for all n, $13 \leq n \leq 702$ using the tables of [1] and [12]. From the proof of Proposition 3 and Theorem, it means that we have verified $F_n + \sqrt{F_n^n + (-1)^n}$ is the fundamental unit for any n, $14 \leq n \leq 701$. We have stopped at $n = 702$, because F_{703} is the first Fibonacci number which is not completely factorized so far. We shall quote here the data to see the cases $n = 700$ and 701:

$F(699) = 2 \cdot 139801 \cdot 13953397457 \cdot 245701220509 \cdot 25047390419633 \cdot 6314840895836$
$93149557829547141 \cdot 35655216831967549432456554975771249921292070066844$
166830

$F(700) = 3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 29 \cdot 41 \cdot 71 \cdot 101 \cdot 151 \cdot 281 \cdot 401 \cdot 701 \cdot 911 \cdot 2801$
$\cdot 3001 \cdot 28001 \cdot 54601 \cdot 141961 \cdot 56701 \cdot 57601 \cdot 7517651 \cdot 51636551 \cdot 12317523121$
$\cdot 2487737663570611401 \cdot 1723120373020118908301 \cdot 7358192362316341243805801$

$F(701) = 42061 \cdot 96737 \cdot 242836213 \cdot 274479353 \cdot 830256889720677 8357 \cdot 526094433$
$9485659754393 \cdot 119475615424178586033394749749743625883464495972432550$
$1434163348353044982847 2737$

$F(702) = 2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 79 \cdot 109 \cdot 233 \cdot 521 \cdot 859 \cdot 5779 \cdot 29717 \cdot 135721 \cdot 2623373$
$\cdot 8023861 \cdot 65597689 \cdot 39589685693 \cdot 1052645985555841 \cdot 657903216797404903717440$
$98034257 \cdot 21104087776648187459376854003284008649$

We also verified that $F_n + \sqrt{F_n^2 + (-1)^n}$ is actually the fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{F_n^2 + (-1)^n}) = \boldsymbol{Q}(\sqrt{s(F_n^2 + (-1)^n)})$ for any n, $2 \leq n \leq 225$ by using UBASIC86.

Acknowledgement. Several parts of this paper were obtained during the author's stay at Université Laval as a visiting researcher. The author expresses his heartily thanks for their kind hospitality to the staff of Département de Mathématiques et de Statistique. He is very grateful to Professor Claude Levesque for helpful discussions and many remarks which improved this paper.

References

[1] J. Brillhart, P. L. Montgomery and R. D. Silverman, Tables of Fibonacci and Lucas factorizations, *Math. Comp.*, **50** (1988), 251–260 and S1–S15.

[2] Y.J. Choie, Rational Period functions, class numbers, and diophantine equations, *J. Number Theory*, **42** (1992), 158–188.

[3] J.H.E. Cohn, The diophantine equation $x^4 - Dy^2 = 1$, II, *Acta Arith.*, **78** (1997), 401-403.

[4] S.–I. Katayama and S.–G. Katayama, Fibonacci, Lucas and Pell numbers and class numbers of bicyclic biquadratic fields, *Math. Jap.*, **42** (1995), 121–126.

[5] S.–I. Katayama, C. Levesque and T. Nakahara, On the unit group and the class number of certain composita of two real quadratic fields, to appear in *Man. Mathematica.*

[6] S.–I. Katayama, The abc conjecture and the fundamental system of units of certain bicyclic biquadratic fields, *Proc. Japan Acad.*, **75A** (1999), 198–199.

[7] S. Lang, Old and new conjectured diophantine inequalities, *Bull. Amer. Math. Soc.*, **30** (1990), 37–75.

[8] P. Ribenboim, The New Book of Prime Number Records, Springer–Verlag, New York, 1995.

[9] P. Ribenboim and G. Walsh, The ABC conjecture and the powerfull part of terms in binary recurring sequences, *J. Number Theory*, **74** (1999), 134–147.

[10] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge Univ. Press, Cambridge, 1986.

[11] G. Walsh, On integer solutions to $x^2 - dy^2 = 1, z^2 - 2dy^2 = 1$, *Acta Arith.*, **82** (1997), 67–76.

Further refences on the web:

[12] B. Kelly, Small tables of Fibonacci factorizations $n \leq 1000$,
http://www.home.att.net/~blair.kelly/mathematics/fibonacci/f1000.txt

[13] A. Nitaj, The ABC Conjecture Home Page,
http://www.math.unicaen.fr/~nitaj/abc.html