

A note on units of real quadratic fields *

Dongho Byeon and Sangyoon Lee

Abstract. For a positive square-free integer d , let t_d and u_d be positive integers such that $\epsilon_d = \frac{t_d + u_d\sqrt{d}}{\sigma}$ is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$, where $\sigma = 2$ if $d \equiv 1 \pmod{4}$ and $\sigma = 1$ otherwise. For a given positive integer l and a palindromic sequence of positive integers a_1, \dots, a_{l-1} , we define the set $S(l; a_1, \dots, a_{l-1}) := \{d \in \mathbb{Z} \mid d > 0, \sqrt{d} = [a_0, \overline{a_1, \dots, a_{l-1}}, 2a_0]\}$. We prove that $u_d < d$ for all square-free integer $d \in S(l; a_1, \dots, a_{l-1})$ with one possible exception and apply it to Ankeny-Artin-Chowla conjecture and Mordell conjecture.

1 Introduction

For a positive square-free integer d , let t_d and u_d be positive integers such that

$$\epsilon_d = \frac{t_d + u_d\sqrt{d}}{\sigma} > 1$$

is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$, where $\sigma = 2$ if $d \equiv 1 \pmod{4}$ and $\sigma = 1$ otherwise. The following two conjectures are well known.

Ankeny-Artin-Chowla conjecture *For any prime p congruent to 1 modulo 4, $u_p \not\equiv 0 \pmod{p}$.*

Mordell conjecture *For any prime p congruent to 3 modulo 4, $u_p \not\equiv 0 \pmod{p}$.*

*This work was supported by KRF-2008-313-C00012.

It is checked that Ankeny-Artin-Chowla conjecture is true for all primes $p < 2 \times 10^{11}$ in [6], [7] and Mordell conjecture is true for all primes $p < 10^7$ in [1]. In relation to three consecutive powerful numbers, Mollin and Walsh [5] conjectured that $u_d \not\equiv 0 \pmod{d}$ when $d \equiv 7 \pmod{8}$. But these conjectures are still open.

Let d be a non-square positive integer congruent to 1 modulo 4. We denote the continued fraction expansion of $(1 + \sqrt{d})/2$ by

$$\frac{1 + \sqrt{d}}{2} = [a'_0, a'_1, \dots] = [a'_0, \overline{a'_1, \dots, a'_{l'_d}}],$$

where l'_d is the length of the period of the continued fraction expansion. Then $a'_{l'_d} = 2a'_0 - 1$ and the sequence of positive integers $a'_1, \dots, a'_{l'_d-1}$ is palindromic, that is, $a'_{l'_d-t} = a'_t$ for $1 \leq t \leq l'_d - 1$. If p is a prime congruent to 1 modulo 4, then l'_p is odd. For a given positive integer l' and a palindromic sequence of positive integers $a'_1, \dots, a'_{l'-1}$, Hashimoto [2] defined the set $S'(l'; a'_1, \dots, a'_{l'-1})$ by

$$\begin{aligned} & S'(l'; a'_1, \dots, a'_{l'-1}) \\ & := \{d \in \mathbb{Z} \mid d > 0, d \equiv 1 \pmod{4} \text{ and } \frac{1 + \sqrt{d}}{2} = [a'_0, \overline{a'_1, \dots, a'_{l'-1}, 2a'_0 - 1}]\}. \end{aligned}$$

and proved the following theorem.

Theorem (Hashimoto) *For any positive odd integer l' and palindromic sequence of positive integers $a'_1, \dots, a'_{l'-1}$, $u_p < p$ and the Ankeny-Artin-Chowla conjecture holds for all primes $p \in S'(l'; a'_1, \dots, a'_{l'-1})$ with one possible exception. If the exception exists, then it is the least in $S'(l'; a'_1, \dots, a'_{l'-1})$.*

The aim of this note is to obtain a similar theorem for arbitrary positive square-free integers d . Let d be a positive integer. We denote the continued fraction expansion of \sqrt{d} by

$$\sqrt{d} = [a_0, a_1, \dots] = [a_0, \overline{a_1, \dots, a_{l_d}}],$$

where l_d is the length of the period of the continued fraction expansion. Then $a_{l_d} = 2a_0$ and the sequence of positive integers a_1, \dots, a_{l_d-1} is palindromic.

For a given positive integer l and a palindromic sequence of positive integers a_1, \dots, a_{l-1} , we define the set $S(l; a_1, \dots, a_{l-1})$ by

$$S(l; a_1, \dots, a_{l-1}) := \{d \in \mathbb{Z} \mid d > 0, \sqrt{d} = [a_0, \overline{a_1, \dots, a_{l-1}, 2a_0}]\}.$$

Using Mc Laughlin's work [3] on the continued fraction, we obtain the following theorem similar to Hashimoto's.

Theorem 1.1 *For any positive integer l and palindromic sequence of positive integers a_1, \dots, a_{l-1} , $u_d < d$ for all square-free integer $d \in S(l; a_1, \dots, a_{l-1})$ with one possible exception. If the exception exists, then it is the least integer in $S(l; a_1, \dots, a_{l-1})$.*

We note that if p is a prime congruent to 1 modulo 4, then l_p is odd and if p is a prime congruent to 3 modulo 4, then l_p is even. Then from Theorem 1.1, we immediately have the following corollary on the Ankeny-Artin-Chowla conjecture and the Mordell conjecture.

Corollary 1.2 *(i) For any odd positive integer l and palindromic sequence of positive integers a_1, \dots, a_{l-1} , $u_p < p$ and the Ankeny-Artin-Chowla conjecture holds for all primes $p \in S(l; a_1, \dots, a_{l-1})$ with one possible exception. If the exception exists, then it is the least integer in $S(l; a_1, \dots, a_{l-1})$.
(ii) For any even positive integer l and palindromic sequence of positive integers a_1, \dots, a_{l-1} , $u_p < p$ and the Mordell conjecture holds for all primes $p \in S(l; a_1, \dots, a_{l-1})$ with one possible exception. If the exception exists, then it is the least integer in $S(l; a_1, \dots, a_{l-1})$.*

On the other hand, Hashimoto [2] and Tomita [8] show that if p is a prime congruent to 1 modulo 4 and the length of the period of the continued fraction expansion of $(1 + \sqrt{p})/2$ is 1, 3 or 5, then $u_p < p$. Similarly, we prove the following propositions.

Proposition 1.3 *For any positive square-free integer d such that $l_d \leq 4$, $u_d < d$. Specially Ankeny-Artin-Chowla conjecture and Mordell conjecture are true for any prime p such that $l_p \leq 4$.*

Proposition 1.4 *For any positive square-free integer d such that $l_d = 5$, $u_d \not\equiv 0 \pmod{d}$. Specially Ankeny-Artin-Chowla conjecture for any prime p such that $l_p = 5$.*

Remark We note that $l_d \leq 4$ is the best upper bound such that $u_d < d$ for all d with the length l_d . For examples, let d be a prime number 701, then we have $\sqrt{701} = [26, \overline{2, 10, 10, 2, 52}]$, $l_{701} = 5$, but $u_{701} = 890$. And let d be a prime number 19, then we have $\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$, $l_{19} = 6$, but $u_{19} = 39$. Moreover we can find infinitely many d such that $u_d > d$ and $l_d = 5$. For details, see Section 4.

2 Preliminaries

In [3, Section 2], Mc Laughlin gave an answer for the question; for which palindromic sequences of positive integers a_1, \dots, a_n , do there exist positive integers a_0 and d such that $\sqrt{d} = [a_0, \overline{a_1, \dots, a_n, 2a_0}]$? We need his following theorem.

Theorem 2.1 (Mc Laughlin) *Let l be a positive integer and a_1, \dots, a_{l-1} be a palindromic sequence of positive integers. Let P_i/Q_i be the i -th approximant of the continued fraction $[0, a_1, \dots, a_{l-1}]$. Then there exist positive integers a_0 and d such that*

$$\sqrt{d} = [a_0, \overline{a_1, \dots, a_{l-1}, 2a_0}] \quad (1)$$

if and only if $P_{l-2}Q_{l-2}$ is even. And if there exists a positive integer d satisfying (1), then

$$d = p(t) := \begin{cases} (\frac{Q_{l-2}P_{l-2}}{2} + tQ_{l-1})^2 + 2tP_{l-1} + P_{l-2}^2 & \text{if } l \text{ is odd,} \\ (\frac{-Q_{l-2}P_{l-2}}{2} + tQ_{l-1})^2 + 2tP_{l-1} - P_{l-2}^2 & \text{if } l \text{ is even,} \end{cases}$$

for some integer or half-integer t such that tQ_{l-1} is an integer and

$$t > \begin{cases} \frac{-Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is odd,} \\ \frac{Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is even.} \end{cases}$$

For the relation between the continued fraction expansion of \sqrt{d} and the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$, the following theorem is well-known (For example, see [4, Theorem 2.1.4]).

Theorem 2.2 *Let d be a positive square-free integer and ϵ_d the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. Let l_d be the length of the period of the continued fraction expansion of \sqrt{d} and P/Q the $(l_d - 1)$ -th approximant of it. Then*

$$\begin{aligned}\epsilon_d &= P + Q\sqrt{d} \text{ if } d \not\equiv 1 \pmod{4} \text{ or } d \equiv 1 \pmod{8}, \\ \epsilon_d &= P + Q\sqrt{d} \text{ or } \epsilon_d^3 = P + Q\sqrt{d} \text{ if } d \equiv 5 \pmod{8}.\end{aligned}$$

3 Proof of Theorem 1.1

Let l be a positive integer and a_1, \dots, a_{l-1} be a palindromic sequence of positive integers. Let P_i/Q_i be the i -th approximant of the continued fraction $[0, a_1, \dots, a_{l-1}]$. Suppose that $d \in S(l; a_1, \dots, a_{l-1})$. Then by Theorem 2.1,

$$d = \begin{cases} \left(\frac{Q_{l-2}P_{l-2}}{2} + tQ_{l-1}\right)^2 + 2tP_{l-1} + P_{l-2}^2 & \text{if } l \text{ is odd,} \\ \left(\frac{-Q_{l-2}P_{l-2}}{2} + tQ_{l-1}\right)^2 + 2tP_{l-1} - P_{l-2}^2 & \text{if } l \text{ is even.} \end{cases}$$

for some integer or half-integer t such that tQ_{l-1} is an integer and

$$t > \begin{cases} \frac{-Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is odd,} \\ \frac{Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is even.} \end{cases}$$

We can write

$$t = \begin{cases} \alpha + \frac{-Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is odd,} \\ \alpha + \frac{Q_{l-2}P_{l-2}}{2Q_{l-1}} & \text{if } l \text{ is even,} \end{cases}$$

for some positive $\alpha \in \mathbb{Q}$.

Then

$$d = \begin{cases} \alpha^2 Q_{l-1}^2 + 2\alpha P_{l-1} - \frac{Q_{l-2}P_{l-2}P_{l-1}}{Q_{l-1}} + P_{l-2}^2 & \text{if } l \text{ is odd,} \\ \alpha^2 Q_{l-1}^2 + 2\alpha P_{l-1} + \frac{Q_{l-2}P_{l-2}P_{l-1}}{Q_{l-1}} - P_{l-2}^2 & \text{if } l \text{ is even.} \end{cases}$$

Since

$$\begin{aligned}P_{l-1}Q_{l-2} + (-1)^{l-1} &= P_{l-2}Q_{l-1}, \\ d &= \begin{cases} \alpha^2 Q_{l-1}^2 + 2\alpha P_{l-1} - \frac{(P_{l-2}Q_{l-1}-1)P_{l-2}}{Q_{l-1}} + P_{l-2}^2 & \text{if } l \text{ is odd,} \\ \alpha^2 Q_{l-1}^2 + 2\alpha P_{l-1} + \frac{(P_{l-2}Q_{l-1}+1)P_{l-2}}{Q_{l-1}} - P_{l-2}^2 & \text{if } l \text{ is even.} \end{cases}\end{aligned}$$

So we have

$$d = \alpha^2 Q_{l-1}^2 + 2\alpha P_{l-1} + \frac{P_{l-2}}{Q_{l-1}}.$$

If Q_{l-1} is odd and d is not the least element of $S(l; a_1, \dots, a_{l-1})$, then $\alpha \geq 1$ and

$$d \geq Q_{l-1}^2 + 2P_{l-1} + \frac{P_{l-2}}{Q_{l-1}} > 2Q_{l-1}.$$

If Q_{l-1} is even and d is not the least element of $S(l; a_1, \dots, a_{l-1})$, then $\alpha \geq 1/2$ and

$$d \geq \frac{1}{4}Q_{l-1}^2 + P_{l-1} + \frac{P_{l-2}}{Q_{l-1}}.$$

So we have that $d > 2Q_{l-1}$ for even $Q_{l-1} \geq 8$. We note that Theorem 2.2 implies that $u_d \leq 2Q_{l-1}$ (for some $d \equiv 1 \pmod{4}$, u_d can be equal to $2Q_{l-1}$). Thus we proved that if d is not the least element in $S(l; a_1, \dots, a_{l-1})$, then

$$d > 2Q_{l-1} \geq u_d$$

except for the case Q_{l-1} is even and less than 8. If $Q_{l-1} = 6$, then $d \in S(4; 1, 4, 1)$ or $S(2; 6)$. If $Q_{l-1} = 4$, then $d \in S(4; 1, 2, 1)$ or $S(2; 4)$. If $Q_{l-1} = 2$, then $d \in S(3; 1, 1)$ or $S(2; 2)$. For all such d , we can easily check that $d > u_d$. Thus we completely proved Theorem 1.2. \square

4 Proof of Proposition 1.3 and 1.4

To prove Proposition 1.3 and 1.4, we need the following lemma, which can be obtained from Theorem 2.1 and the fact that it is permitted to substitute a_0 for $(\frac{\pm Q_{l-2}P_{l-2}}{2} + tQ_{l-1})$.

Lemma 4.1 *Let d be a square-free integer such that $\sqrt{d} = [a_0, \overline{a_1, \dots, a_{l-1}}, 2a_0]$ for some positive integer a_0 and some palindromic sequence of positive integers a_1, \dots, a_{l-1} . Let P_i/Q_i be the i -th approximant of the continued fraction $[0, a_1, \dots, a_{l-1}]$. Then we can write $d = a_0^2 + b$ where $b = \frac{2a_0P_{l-1} + P_{l-2}}{Q_{l-1}}$.*

Proof of Proposition 1.3 We give a proof only for the case $l_d = 4$. The other cases can be proved in a similar way. Let d be a positive square-free integer

with $l_d = 4$. Then $\sqrt{d} = [a_0, \overline{m, n, m, 2a_0}]$, for some positive integer a_0 , m , and n and the approximants of the continued fraction $[0, m, n, m]$ are

$$\frac{P_0}{Q_0} = \frac{0}{1}, \frac{P_1}{Q_1} = \frac{1}{m}, \frac{P_2}{Q_2} = \frac{n}{mn+1}, \frac{P_3}{Q_3} = \frac{mn+1}{m^2n+2m}.$$

By Lemma 4.1, we can write $d = a_0^2 + b$, where $b = \frac{2a_0(mn+1)+n}{m^2n+2m}$. Let $2a_0 = mk + r$ where k, r are non-negative integers with $0 \leq r < m$. Then we have $b = k + G$, where $G = (r(mn+1) + n - km)/(m^2n+2m) < 1$.

Case 1 $G = 0$ Since $r(mn+1) + n = km$,

$$2a_0 = mk + r = n(rm+1) + 2r.$$

If $r = 0$, then $2a_0 = n$ and $l_d < 4$. So we assume that $r \neq 0$. If $r \geq 3$ or $n \geq 8$, then

$$d > a_0^2 = \left(\frac{n(rm+1) + 2r}{2}\right)^2 = \frac{n^2r^2}{4}m^2 + \left(\frac{n^2r}{2} + nr^2\right)m + \frac{n^2}{4} + nr + r^2 \geq 2Q_3.$$

By Theorem 2.2, $u_d \leq 2Q_4$. Thus we have if $r \geq 3$ or $n \geq 8$, then

$$d > u_d.$$

Suppose $r < 3$ and $n < 8$. Since $m|(n+r)$, $m \leq 9$. For the finite number of d with $0 < m \leq 9$, $0 < n < 8$ and $0 < r < 3$, we can easily check that $d > u_d$.

Case 2 $G \leq -1$ Since $r(mn+1) + m^2n + 2m + n \leq km$,

$$2a_0 = mk + r \geq r(mn+2) + m^2n + 2m + n,$$

and we have

$$d > a_0^2 \geq \left(\frac{m^2n + 2m + n}{2}\right)^2 = m^2 + m^3n + mn + (m^2n + n)^2/4.$$

So $d > 2Q_3 \geq u_d$ except for $m = n = 1$. If $m = n = 1$, since $l_d = 4$, $d > 6 = 2Q_3 \geq u_d$. \square

Proof of Proposition 1.4 Let d be a positive square-free integer with $l_d = 5$. Then $\sqrt{d} = [a_0; \overline{m, n, n, m, 2a_0}]$, for some positive integer a_0 , m , and n and the approximants of the continued fraction $[0, m, n, n, m]$ are

$$\begin{aligned}\frac{P_0}{Q_0} &= \frac{0}{1}, \quad \frac{P_1}{Q_1} = \frac{1}{m}, \quad \frac{P_2}{Q_2} = \frac{n}{mn+1}, \\ \frac{P_3}{Q_3} &= \frac{n^2+1}{mn^2+m+n}, \quad \frac{P_4}{Q_4} = \frac{mn^2+m+n}{m^2n^2+m^2+2mn+1}.\end{aligned}$$

By Lemma 4.1, we can write $d = a_0^2 + b$, where $b = \frac{2a_0(mn^2+m+n)+n^2+1}{m^2n^2+m^2+2mn+1}$. Let $2a_0 = mk + r$ where k, r are non-negative integer with $0 \leq r < m$. Then we have $b = k + H$, where $H = \frac{r(mn^2+m+n)+n^2+1-k(mn+1)}{m^2n^2+m^2+2mn+1} < 1$. We give a proof only for the case $H = 0$. For the case $H \leq -1$, by the similar method in the proof of Proposition 1.3, we can show that $d > 2Q_4$ except for $d = 701$. Thus Theorem 2.2 implies that $d > u_d$ and $u_d \not\equiv 0 \pmod{d}$ except for $d = 701$. If $d = 701$, then $Q_4 = 445$ and $u_{701} = 2Q_4 = 890$. So $u_{701} \not\equiv 0 \pmod{701}$.

Case $H = 0$ Since $r(mn^2 + m + n) + n^2 + 1 = k(mn + 1)$,

$$k = rn + \frac{rm + n^2 + 1}{mn + 1},$$

and we have

$$2a_0 = mk + r = r(mn + 1) + m\left(\frac{rm + n^2 + 1}{mn + 1}\right).$$

We note that $(mn + 1) \mid (rm + n^2 + 1)$ and let $rm + n^2 + 1 = h(mn + 1)$ for some positive integer h . If r is odd, then both m and k are odd. Then the equation

$$r(mn^2 + m + n) + n^2 + 1 = k(mn + 1)$$

implies

$$(n + 1 + n) + n + 1 \equiv n + 1 \pmod{2},$$

which cannot hold. So r should be even. If $r = 0$, then the inequality

$$n(n - km) = k - 1 \geq 0$$

implies that $n \geq km$. If $n > km$, then $n(n - km) > km \geq k > k - 1$. So n should be equal to km . This implies that $k = 1$ and $m = n$. So $2a_0 = m$

and $l_d < 5$. Thus we assume that r is a positive even integer. If $r \geq 2$, then we have

$$d > a_0^2 = \frac{r^2 m^2 n^2}{4} + \frac{r^2 mn}{2} + \frac{rm^2 nh}{2} + \frac{r^2}{4} + \frac{rmh}{2} + \frac{m^2 h^2}{4} \geq Q_4,$$

where $h = \frac{rm+n^2+1}{mn+1}$. By Theorem 2.2, $u_d \leq 2Q_4$. So if $u_d \equiv 0 \pmod{d}$, then $d = u_d$. If $d \not\equiv 1 \pmod{4}$, then $d = u_d = Q_4$. But it is impossible because $d > Q_4$. If $d \equiv 1 \pmod{4}$ and $u_d = 2Q_4$, then $d = u_d = 2Q_4$. But it is impossible because $d \equiv 1 \pmod{4}$. If $d \equiv 5 \pmod{8}$ and $\epsilon_d^3 = P_4 + Q_4\sqrt{d}$, then $d = u_d = \frac{8}{3t_d^2 + u_d^2 d} Q_4 \leq Q_4$ because $3t_d^2 + u_d^2 d \geq 8$. But it is impossible because $d > Q_4$. So $u_d \not\equiv 0 \pmod{d}$. \square

Remark In the proof of the case $H = 0$ of Proposition 1.4, let $r = 2$, $h = 2$ and $n + 1 = 2m$. Then we have

$$\begin{aligned} a_0 &= \frac{(n+1)^2}{2} + 1, \\ d &= \frac{(n+1)^4}{4} + (n+1)^2 + 1 + 2(n+1), \\ 2Q_4 &= \frac{(n+1)^2 n^2}{2} + \frac{(n+1)^2}{2} + 2n(n+1) + 2, \\ \sqrt{d} &= [(n+1)^2/2 + 1, (n+1)/2, n, n, (n+1)/2, (n+1)^2 + 2], \\ Q_4 &< d < 2Q_4. \end{aligned}$$

If $n \equiv -1 \pmod{8}$, then $d \equiv 1 \pmod{8}$ and $u_d = 2Q_4$ by Theorem 2.2. Thus there are infinitely many d such that $u_d > d$ and $l_d = 5$.

Acknowledgement The authors would like to thank the referee for his careful reading and many valuable suggestions.

References

- [1] B. D. Beach, H. C. Williams and C. R. Zarnke, *Some computer results on units in quadratic and cubic fields*, Proc. 25th Summer meeting Can. Math. Congress, Lakehead Univ. (1971), 609–648.
- [2] R. Hashimoto, *Ankeny-Artin-Chowla conjecture and continued fraction*, J. Number Theory **90** (2001), 143–153.

- [3] J. Mc Laughlin, *Multi-variable polynomial solutions to Pell's equation and fundamental units in real quadratic fields*, Pacific J. Math. **210** (2003), 335–349.
- [4] R. A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.
- [5] R. A. Mollin and P. G. Walsh, *A note on powerful numbers, quadratic fields and the Pellian*, C. R. Rep. Acad. Sci. Canada **8** (1986), 109–114.
- [6] A. J. Van Der Poorten, H. J. J. te Riele and H. C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000*, Math. Comp. **70** (2001), 1311–1328.
- [7] A. J. Van Der Poorten, H. J. J. te Riele and H. C. Williams, *Corrigenda and addition to "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than 100 000 000 000"*, Math. Comp. **72** (2003), 521–523.
- [8] K. Tomita, *Explicit representaion of fundamental units of some real quadratic fields, II* J. Number Theory **63** (1997), 275–285.

Department of Mathematics, Seoul National University
 Seoul 151-747, Korea
 E-mail: dhbyeon@math.snu.ac.kr

Department of Mathematics, Seoul National University
 Seoul 151-747, Korea