Ankeny–Artin–Chowla Conjecture and Continued Fraction Expansion

Ryūta Hashimoto

Graduate School of Human Informatics, Nagoya University, Nagoya 464-8601, Japan
E-mail: ryuta@math.human.nagoya-u.ac.jp

Communicated by D. Goss
Received April 27, 2000; published online May 24, 2001

For any prime $p$ congruent to 1 modulo 4, let $\left(t_p + u_p - p\right)/2$ be the fundamental unit of $\mathbb{Q}(-\sqrt{p})$. Then Ankeny, Artin, and Chowla conjectured that $u_p$ is not divisible by $p$. In this paper, we investigate a certain relation between the conjecture and the continued fraction expansion of $(1 + \sqrt{p})/2$. Consequently, we prove that the conjecture is true if $p$ is not “small” in some sense.

2001 Academic Press

Key Words: quadratic field; fundamental unit; continued fraction.

1. INTRODUCTION

For any prime $p$, let $t_p$ and $u_p$ be two positive integers such that $\left(t_p + u_p - p\right)/2$ is the fundamental unit of $\mathbb{Q}(-\sqrt{p})$. In [1], Ankeny, Artin, and Chowla proposed the following conjecture:

**Conjecture 1.1.** It holds that $u_p \not\equiv 0 \pmod{p}$ for any prime $p$ congruent to 1 modulo 4.

There are many papers on this conjecture. For example, Mordell [3] gives a criterion in terms of the cyclotomic field $\mathbb{Q}(\zeta_{2m(p)})$. Yokoi [8] gives another criterion in terms of some invariants related to the quadratic field $\mathbb{Q}(\sqrt{p})$. Numerically, van der Poorten et al. [7] checked that the conjecture is true for all primes $p < 10^4$.

In the present paper, we study a certain relation between the Ankeny–Artin–Chowla conjecture for $p$ and the continued fraction expansion of $(1 + \sqrt{p})/2$. Namely, in the next section, we first state the main theorem. In Section 3, we describe $p$ in terms of the partial quotients in the continued fraction expansion of $(1 + \sqrt{p})/2$, and prove the main theorem. In Section 4, we research integers “with fixed period.” In the final section, Section 5, we study a special case.
Notation 1.2. For any real number $x$, $\lceil x \rceil$ means the ceiling of $x$, that is, the least integer which is not less than $x$, while $\lfloor x \rfloor$ means the floor of $x$, that is, the greatest integer which is not greater than $x$.

2. MAIN THEOREM

We denote the continued fraction expansion of $(1 + \sqrt{p})/2$ by
\[
\frac{1 + \sqrt{p}}{2} = [c_0, c_1, ...] = [c_0, c_1, ..., c_{l_p}].
\]
where $l_p$ is the length of the period of the continued fraction expansion. Then it is known (cf. [4, Satz 3.30]) that the period is palindromic, that is, $c_k$'s satisfy
\[
c_{l_p-k} = c_k \quad \text{for} \quad 1 \leq k < l_p \quad \text{and} \quad c_{l_p} = 2c_0 - 1.
\]

Moreover, $l_p$ is odd (we note that this property follows Lemma 3.2 in Section 3). When $l_p$ is small, we have the following proposition:

Proposition 2.1. If $l_p = 1, 3, \text{or} 5$, then $u_p < p$, and Ankeny–Artin–Chowla conjecture is true.

It is easy to prove when $l_p = 1$ or 3. Tomita [6] proved Proposition 2.1 when $l_p = 5$ and $\lfloor \sqrt{p} \rfloor$ is even. However, his proof is also available when $l_p = 5$ and $\lfloor \sqrt{p} \rfloor$ is odd.

What happens when $l_p \geq 7$? A numerical example is given here.

Example 2.2. The least prime $p$ such that $p \equiv 1 \pmod{4}$ and $l_p \geq 7$ is 73. We have $(1 + \sqrt{73})/2 = [4, 1, 3, 2, 1, 1, 2, 3, 1, 7]$, $l_{73} = 9$, and $u_{73} = 250$. Consider the set $S(9; 1, 3, 2, 1)$ defined by
\[
S(9; 1, 3, 2, 1) := \left\{ d \in \mathbb{Z} \left| \begin{array}{c} d > 0, \quad d \equiv 1 \pmod{4}, \\ \frac{1 + \sqrt{d}}{2} = [c_0, 1, 3, 2, 1, 1, 2, 3, 1, 2c_0 - 1] \\ \text{where} \quad c_0 = \lfloor (1 + \sqrt{d})/2 \rfloor \end{array} \right. \right\}
\]
Then we have
\[
S(9; 1, 3, 2, 1) = \left\{ (q_8s + q_7r_s)^2 + 4q_7s + 4r_s \left| s \in \mathbb{Z}, \; s \geq -115 = \left\lfloor -\frac{q_7r_s}{q_8} \right\rfloor \right. \right\}
\]
\[
= \{ 73, 66845, 258617, ... \},
\]
where \( q_8 = 250, q_7 = 193, \) and \( r_7 = 149. \) We can prove the following fact: if a prime \( p \) belongs to \( S(9; 1, 3, 2, 1) \), then it holds that \( u_p < p \) unless \( p = 73. \) In particular, Ankeny–Artin–Chowla conjecture is true for all the primes belonging to \( S(9; 1, 3, 2, 1) \).

This example and others suggest the following: for primes \( p \) with a fixed period, it holds that \( u_p < p \) unless \( p \) is “small.” The main theorem in this paper shows that this suggestion is true.

For any given odd integer \( l \) and any given positive integers \( c_1, \ldots, c_l \), where \( l' = (l - 1)/2 \), we define the set \( S(l; c_1, \ldots, c_r) \) of positive integers by

\[
S(l; c_1, \ldots, c_r) := \left\{ d \in \mathbb{Z} \mid \begin{array}{l}
  d > 0, d \equiv 1 \pmod{4}, \\
  \frac{1 + \sqrt{d}}{2} = \left[ c_{l'}, c_{l'}, \ldots, c_{r}, \ldots, c_1, 2c_0 - 1 \right], \\
  \text{where } c_0 = \lfloor (1 + \sqrt{d})/2 \rfloor
\end{array} \right\}.
\]

(1)

**Remark 2.3.** It turns out that the set \( S(l; c_1, \ldots, c_r) \) is not empty. However, it is not certain whether \( S(l; c_1, \ldots, c_r) \) contains infinitely many primes. For details, see Section 4.

Now we are ready to state the main theorem in this paper.

**Main Theorem 2.4** [Theorem 3.4 in Section 3]. For any positive odd integer \( l \), put \( l' = (l - 1)/2 \). Assume that positive integers \( c_1, \ldots, c_r \) are given. Then, the Ankeny–Artin–Chowla conjecture holds for all the primes \( p \in S(l; c_1, \ldots, c_r) \) with one possible exception. Further, if the exception exists, then it is the least integer in \( S(l; c_1, \ldots, c_r) \).

We can prove that main theorem implies Proposition 2.1. But the proof is omitted in this paper.

**Remark 2.5.** It is certain that \( p \) belongs to \( S(l_p; \ldots) \). But the assertion that \( p \) belongs to \( S(l; \ldots) \) does not mean that \( l_p = l \), though it holds that \( l_p \leq l \) because \( l_p \mid l \). For example, take \( p = 5 \). Then we have \( 1 + \sqrt{5}/2 = \lfloor 1 \rfloor \) and \( l_5 = 1 \). Besides, the prime 5 belongs to not only \( S(1; \ldots) \) but also \( S(3; 1), S(5; 1, 1), \) etc. because

\[
\frac{1 + \sqrt{5}}{2} = \lfloor 1 \rfloor = \lfloor 1, 1, 1, \rfloor = \lfloor 1, 1, 1, 1, 1, \rfloor = \ldots.
\]
3. PROOF OF MAIN THEOREM

In this section, we obtain a description of \( p, q, r \) in terms of the partial quotients \( c_n \)'s of \( (1 + \sqrt{p})/2 \). Similar discussions can be seen in Perron [4, Section 30] and Friesen [2].

We define \( \{ p_n \}, \{ q_n \}, \{ r_n \} \) by

\[
\begin{align*}
& p_{-1} = 1, \quad p_0 = c_0, \quad p_n = c_n p_{n-1} + p_{n-2} \quad (n \geq 1), \\
& q_{-1} = 0, \quad q_0 = 1, \quad q_n = c_n q_{n-1} + q_{n-2} \quad (n \geq 1), \\
& r_{-1} = 1, \quad r_0 = 0, \quad r_n = c_n r_{n-1} + r_{n-2} \quad (n \geq 1).
\end{align*}
\]

We notice that

\[
\frac{p_n}{q_n} = [c_0, c_1, ..., c_n], \quad \lim_{n \to \infty} \frac{p_n}{q_n} = \frac{1 + \sqrt{p}}{2},
\]

and

\[
\frac{q_n}{r_n} = [c_1, c_2, ..., c_n].
\]

We can easily prove the following assertions by induction on \( n \):

\[
\begin{align*}
q_n r_{n-1} - r_n q_{n-1} &= (-1)^n, \quad (3) \\
q_n r_{n-2} - r_n q_{n-2} &= (-1)^{n-1} c_n, \quad (4) \\
p_n - c_0 q_n &= r_n. \quad (5)
\end{align*}
\]

To obtain a description of \( p \) by \( c_n \)'s, we start with the following equation:

\[
\frac{1 + \sqrt{p}}{2} = [c_0, c_1, ..., c_{l_0-1}, [2c_0 - 1, r_{l_0-1}, ..., c_2]]
\]

\[
= [c_0, c_1, ..., c_{l_0-1}, c_0 - 1 + (1 + \sqrt{p})/2]
\]

\[
= \left[ \frac{(c_0 - 1 + (1 + \sqrt{p})/2) q_{l_0-1} + q_{l_0-2}}{(c_0 - 1 + (1 + \sqrt{p})/2) r_{l_0-1} + r_{l_0-2}} \right]
\]

\[
= c_0 + \frac{(c_0 - 1 + (1 + \sqrt{p})/2) r_{l_0-1} + r_{l_0-2}}{(c_0 - 1 + (1 + \sqrt{p})/2) q_{l_0-1} + q_{l_0-2}}.
\]
which implies
\[
q_{l_p-1} \left( \frac{1 + \sqrt{p}}{2} \right) - (q_{l_p-2} - q_{l_p-2} + r_{l_p-1}) \left( \frac{1 + \sqrt{p}}{2} \right) \\
- c_0 (c_0 - 1) q_{l_p-1} - c_0 q_{l_p-2} - (c_0 - 1) r_{l_p-1} - r_{l_p-2} = 0.
\]

On the other hand, it holds that
\[
\left( \frac{1 + \sqrt{p}}{2} \right)^2 - \left( \frac{1 + \sqrt{p}}{2} \right) - \frac{p-1}{4} = 0.
\]

Then we have
\[
\frac{q_{l_p-1} - q_{l_p-2} + r_{l_p-1}}{q_{l_p-1}} = 1 \tag{6}
\]

and
\[
\frac{c_0 (c_0 - 1) q_{l_p-1} + c_0 q_{l_p-2} + (c_0 - 1) r_{l_p-1} + r_{l_p-2}}{q_{l_p-1}} = \frac{p-1}{4}. \tag{7}
\]

By (6), we have
\[
q_{l_p-2} = r_{l_p-1}. \tag{8}
\]

By (7) and (8), we have
\[
\frac{p-1}{4} = c_0 (c_0 - 1) + \frac{(2c_0 - 1) q_{l_p-2} + r_{l_p-2}}{q_{l_p-1}}, \tag{9}
\]

which leads to
\[
\frac{p-(2c_0-1)^2}{4} q_{l_p-1} - (2c_0 - 1) q_{l_p-2} = r_{l_p-2}. \tag{10}
\]

By (3), (8), and the fact that \( l_p \) is odd, we have
\[
r_{l_p-2} q_{l_p-1} - q_{l_p-2}^2 = 1. \tag{11}
\]

Because of (11), any integer solution \((p, c_0)\) of the Eq. (10) must satisfy
\[
\frac{p-(2c_0-1)^2}{4} = r_{l_p-2}^2 + q_{l_p-2}s, \tag{12}
\]

\[
2c_0 - 1 = q_{l_p-2} r_{l_p-2} + q_{l_p-1}s. \tag{13}
\]
for some integer $s$. Since $(p - (2c_0 - 1)^2)/4 > 0$ and $2c_0 - 1 > 0$, (12) and (13) lead to
\[
s > -\frac{q_{2l-2}r_{2l-2}}{q_{2l-1}}.
\] (14)

Notice that $q_{2l-1}$, $q_{2l-2}$, $r_{2l-2}$ are polynomials of $c_1, ..., c_{2l-1}$. Then we can discuss the elements of $S(l; c_1, ..., c_r)$ as above. Moreover, (12), (13), and (14) lead to the proposition on $S(l; c_1, ..., c_r)$ as follows:

**Proposition 3.1.** For any odd integer $l$, put $l' = (l - 1)/2$. Assume that positive integers $c_1, ..., c_r$ are given. Then, on the set $S(l; c_1, ..., c_r)$ defined by (1), we have
\[
S(l; c_1, ..., c_r) = \left\{ (q_{l-1}s + q_{l-2}r_{l-2})^2 + 4q_{l-2}s^2 + 4r_{l-2}^2) \right\} \\
s \in \mathbb{Z}, \quad s > -\frac{q_{l-2}r_{l-2}}{q_{l-1}}, \quad q_{l-1}s + q_{l-2}r_{l-2} \text{ is odd,}
\]
where $q_{l-1}$, $q_{l-2}$, and $r_{l-2}$ are defined by (2) and $c_k = c_{2k+1} = 1$ for $l' + 1 \leq k \leq 2l'$. In particular, if $p \in S(l; c_1, ..., c_r)$ and $p \neq \min S(l; c_1, ..., c_r)$, then
\[
p = (q_{l-1}s + q_{l-2}r_{l-2})^2 + 4q_{l-2}s^2 + 4r_{l-2}^2, \\
\text{where } s \in \mathbb{Z} \quad \text{and} \quad s > -(q_{l-2}r_{l-2})/q_{l-1} + 1.
\]

Next, we obtain a description of $t_p$ and $u_p$ by $c_s$'s. The following lemma is well-known:

**Lemma 3.2.** Let $d$ be a positive non-square integer such that $d \equiv 1 \pmod{4}$. Assume that the continued fraction expansion of $(1 + \sqrt{d})/2$ is as follows:
\[
\frac{1 + \sqrt{d}}{2} = [c_0, c_1, ...] = [c_0, c_1, ..., c_{l_d}],
\]
where $l_d$ is the length of the period of the continued fraction expansion of $(1 + \sqrt{d})/2$. Define $\{p_n\}$ and $\{q_n\}$ by (2).
1. (cf. [4, Satz 3.35]) All the positive integer solutions of \( X^2 - XY - ((d-1)/4) Y^2 = \pm 1 \) have the form \((X, Y) = (p_{m_1-1}, q_{m_1-1})\). Further, it holds that

\[
p_{m_1-1}^2 - p_{m_1-1} q_{m_1-1} - \frac{d-1}{4} q_{m_1-1}^2 = (-1)^{m_1}.
\]

In particular, the diophantine equation \( X^2 - XY - ((d-1)/4) Y^2 = -1 \) is solvable if and only if \( l_d \) is odd.

2. The diophantine equation \( X^2 - XY - ((d-1)/4) Y^2 = 1 \) is solvable if and only if \( X^2 - dY^2 = -4 \) is solvable.

3. If \( d = p \) is prime, then the diophantine equation \( X^2 - p Y^2 = -4 \) is solvable.

We obtain \((t_p, u_p)\) as the least positive integer solution of \( X^2 - p Y^2 = -4 \). Then Lemma 3.2 leads to

\[
t_p = 2p_{j_1-1} - q_{j_1-1} \quad \text{and} \quad u_p = q_{j_1-1}.
\]

By (5), (8), and (13), we have

\[
2p_{j_1-1} - q_{j_1-1} = q_{j_1-1}^2 + q_{j_1-1} q_{j_1-2} r_{j_1-2} + 2q_{j_1-2}.
\]

Hence we obtain

**Proposition 3.3.** For any prime \( p \) congruent to 1 modulo 4, \( t_p \) and \( u_p \) can be written in terms of the continued fraction expansion of \((1 + \sqrt{p})/2\), namely,

\[
t_p = q_{j_1-1}^2 s + q_{j_1-1} q_{j_1-2} r_{j_1-2} + 2q_{j_1-2}, \quad u_p = q_{j_1-1}.
\]

We are now ready to state and prove the following theorem:

**Theorem 3.4.** Notations are as in Proposition 3.1.

It holds that \( u_p < p \) for all the primes \( p \in S(l; c_1, \ldots, c_l) \) with one possible exception. Further, if the exception \( p \) exists, then \( p \) can be written as follows:

\[
p = (q_{j_1-1} s + q_{j_1-2} r_{j_1-2})^2 + 4q_{j_1-2} s + 4r_{j_1-2}^2,
\]

where \( s = \left\lfloor \frac{q_{j_1-2} r_{j_1-2}}{q_{j_1-1}} \right\rfloor \).
Proof. Suppose that $p \in S(l; c_1, ..., c_r)$ and $p \neq \min S(l; c_1, ..., c_r)$. By Proposition 3.1, we have
\[
s > \frac{q_{l-2}r_{l-2}}{q_{l-1}} + 1.
\]
Hence (11) implies
\[
p > q_{l-1}^2 + 4q_{l-2} + \frac{4r_{l-2}(\frac{q_{l-3}^2 + q_{l-1}r_{l-2}}{q_{l-1}})}{q_{l-1}}
\]
\[
= q_{l-1}^2 + 4q_{l-2} + \frac{4r_{l-2}}{q_{l-1}} > q_{l-1}.
\]
Since $l_p \leq l$, we have $p > q_{l-1} \geq q_{l-1}^2 = u_p$.

Therefore we have $u_p < p$ for all the primes $p \in S(l; c_1, ..., c_r)$ except $p = \min S(l; c_1, ..., c_r)$. Thus we complete the proof.

As a corollary of Theorem 3.4, we easily obtain the following:

**Corollary 3.5.** Notations are as in Proposition 3.1.
If the minimum of $S(l; c_1, ..., c_r)$ is not prime, then it holds that $u_p < p$ for all the primes $p$ belonging to $S(l; c_1, ..., c_r)$.

### 4. Integers with Fixed Period

In this section, we investigate some properties of $S(l; c_1, ..., c_r)$.

**Proposition 4.1.** In the situation of Proposition 3.1, $S(l; c_1, ..., c_r)$ is not empty. Moreover, either of the following two assertions holds:

1. $q_{l-1}, q_{l-2} - r_{l-2}$, and $s$ are all odd;
2. $q_{l-1}$ is even, and both $q_{l-2}$ and $r_{l-2}$ are odd.

**Proof.** By (9), $S(l; c_1, ..., c_r)$ is not empty if and only if
\[
(2x - 1) q_{l-2} + r_{l-2} \equiv 0 \pmod{q_{l-1}}
\]
(15) is solvable. By (3), $q_{l-1}$ and $q_{l-2}$ are coprime. So (15) is solvable if and only if it holds that $\gcd(q_{l-1}, 2) | (q_{l-2} - r_{l-2})$. 

In the case when \( q_{l-1} \) is odd, (15) is always solvable. In addition, \( q_{l-2} - r_{l-2} \) is odd because of (11), and \( s \) is odd because of (13).

In the case when \( q_{l-1} \) is even, (15) is solvable if and only if \( q_{l-2} - r_{l-2} \) is even. Because of (13), both \( q_{l-2} \) and \( r_{l-2} \) are odd, which implies that (15) is solvable.

Proposition 4.1 and the discussion to prove Theorem 3.4 in the previous section easily lead to the following theorem:

**Theorem 4.2.** In the situation of Proposition 3.1, assume that \( q_{l-1} \) is odd and \( \sqrt{-q_{l-2}r_{l-2}/q_{l-1}} \) is even. Then it holds that \( u_p < p \) for all the primes \( p \) belonging to \( S(l; c_1, ..., c_p) \).

Next, we ask how many primes \( S(l; c_1, ..., c_p) \) contains. Proposition 3.1 shows that we can answer this question if we know how many primes a quadratic polynomial represents. But it is unknown (e.g. [5, Chap. 6, Section II]).

5. CASES WHEN ALMOST ALL THE PARTIAL QUOTIENTS ARE EQUAL

It is still not easy to prove the Ankeny–Artin–Chowla conjecture completely for an arbitrary \( l_p \). But we can prove the conjecture for special cases. In this section, we consider the case when almost all the partial quotients of the continued fraction expansion of \( (1+\sqrt{p})/2 \) are equal.

As a corollary of Theorems 3.4 and 4.2, we have the following:

**Corollary 5.1.** Let \( p \) be a prime which is congruent to 1 modulo 4. Suppose that the continued fraction expansion of \( (1+\sqrt{p})/2 \) is

\[
\frac{1+\sqrt{p}}{2} = [c_0, c, ..., c, 2c_0 - 1],
\]

that is to say, \( c_k = c \) (for \( l_p \mid k \)) where \( c \) is a constant positive integer. Then it holds that \( p > u_p \). In particular, the Ankeny–Artin–Chowla conjecture is true for \( p \).

**Proof.** Corollary 5.1 is true for any prime \( p \) such that \( l_p = 1 \) because of Proposition 2.1. So, we assume that \( l_p > 1 \).

We can check that

\[
r_n = q_{n-1} \quad \text{for} \quad 0 \leq n < l_p.
\]

Then (4) leads to that

\[
q_{k-2}r_{k-2} - q_{k-1}r_{k-3} = r_{k-1}q_{k-3} - q_{k-2}r_{k-3} = c.
\]

151 ON ANKENY–ARTIN–CHOWLA CONJECTURE
So it holds that
\[
\left\lfloor \frac{q_{l_p-2}^{2} r_{l_p-2}}{q_{l_p-1}} \right\rfloor = \left\lfloor \frac{q_{l_p-1} r_{l_p-3} + c}{q_{l_p-1}} \right\rfloor = \left\lfloor -\frac{r_{l_p-3} - c}{q_{l_p-1}} \right\rfloor = -r_{l_p-3}.
\]

Suppose that \( c \) is even. By (2), \( q_n \) is odd and \( r_n \) is even if \( n \) is even and \( n \equiv l_p - 1 \). In particular, \( q_{l_p-1} \) is odd and \( r_{l_p-3} \) is even. Hence Theorem 4.2 implies that \( u_p < p \).

Suppose that \( c \) is odd. By Theorem 3.4, we have only to consider the case when
\[
p = (q_{l_p-1} s + q_{l_p-2} r_{l_p-2})^2 + 4q_{l_p-2} s + 4r_{l_p-2}^2,
\]
where
\[
s = \left\lfloor -\frac{q_{l_p-2} r_{l_p-2}}{q_{l_p-1}} \right\rfloor.
\]

By (17), (16), and (3), we have
\[
p = (-q_{l_p-1} r_{l_p-3} + q_{l_p-2} r_{l_p-2})^2 - 4q_{l_p-2} r_{l_p-3} + 4r_{l_p-2}^2 = c^2 + 4,
\]
which implies that \( p \) belongs to \( S(1) \), contradicting the assertion that \( l_p > 1 \). Hence we complete the proof.

ACKNOWLEDGMENTS

The author thanks Professor Hideo Yokoi for his suggestion to improve the earlier statement of the main theorem. Thanks are also due to the referees for their many comments to make this paper readable.

REFERENCES

6. K. Tomita, Explicit representation of fundamental units of some real quadratic fields, II, 
7. A. J. van der Poorten, 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.*, in 
   press. [Posted on March 15, 2000, PII S 0025-5718(00)01234-5]
8. H. Yokoi, The fundamental unit and bounds for class numbers of real quadratic fields, 