Remark on Ankeny, Artin and Chowla conjecture

ALEKSANDER GRYCZUK

Abstract. In this paper we give two new criteria connected with well-known and still open conjecture of Ankeny, Artin and Chowla.

Introduction

In the paper [2] Ankeny, Artin and Chowla conjectured that, if $p \equiv 1 \pmod{4}$ is a prime and $\varepsilon = 1/2(T + U \sqrt{p}) > 1$ is the fundamental unit of the quadratic number field $K = \mathbb{Q}(\sqrt{p})$ then $p|U$. It was shown by Mordell [5] in the case $p \equiv 5 \pmod{8}$ and by Ankeny and Chowla [3] for the remaining primes $p \equiv 1 \pmod{4}$ that $p | U$ if and only if $p|B_{2n-1}$, where $B_{2n}$ is $2n$-th Bernoulli number. Another criterion has been given by T. Agoh in [1]. Beach, Williams and Zarnke [4] verified the conjecture of Ankeny, Artin and Chowla for all primes $p < 6270713$. Sheingorn [6], [7] gave interesting connections between the fundamental solution $\langle x_0, y_0 \rangle$ of the non-Pellian equation

\begin{equation}
    x^2 - py^2 = -1, \quad p \equiv 1 \pmod{4}, \quad p \text{ is a prime}
\end{equation}

and the manner of the reflection lines on the modular surface and also of the $\sqrt{p}$ Riemann surface. We prove the following two theorems:

**Theorem 1.** Let $p \equiv 1 \pmod{4}$ be a prime and $p = b^2 + c^2$. Moreover, let $\sqrt{p} = [q_0; q_1, q_2, \ldots, q_s]$ be the representation of $\sqrt{p}$ as a simple continued fraction and let $\langle x_0, y_0 \rangle$ be the fundamental solution of (1). Then $p | y_0$ if and only if $p | cQ_r + bQ_{r-1}$ and $p | Q_r - cQ_{r-1}$, where $r = \frac{s-1}{2}$ and $P_n/Q_n$ is $n$-th convergent of $\sqrt{p}$.

**Theorem 2.** Assume that the assumptions of the Theorem 1 are satisfied. Then $p | y_0$ if and only if $p | 4bQ_rQ_{r-1} - (-1)^{r+1}$, where $r = \frac{s-1}{2}$ and $P_n/Q_n$ is $n$-th convergent of $\sqrt{p}$.

Basic Lemmas

**Lemma 1.** Let $\sqrt{d} = [q_0; q_1, \ldots, q_s]$ be the representation of $\sqrt{d}$ as a simple continued fraction. Then

\begin{equation}
    q_n = \left[ \frac{q_0 + b_n}{c_n} \right], \quad b_n + b_{n+1} = c_nq_n, \quad d = b_{n+1}^2 + c_nc_{n+1}
\end{equation}
(3) if \( s = 2r + 1 \) then minimal number \( k \), for which \( c_{k+1} = c_k \) is \( k = \frac{s-1}{2} \).

(4) \( dQ_{n-1} = b_n P_{n-1} + c_n P_{n-2} \)

(6) \( P_{n-1} = b_n Q_{n-1} + c_n Q_{n-2} \)

(7) \( P_{n-1}^2 - dQ_{n-1}^2 = (-1)^n c_n \)

where \( P_n/Q_n \) is the \( n \)-th convergent of \( \sqrt{d} \).

This Lemma is a collection of well-known results of the theory of continued fractions.

From Lemma 1 we can deduce for the case \( d = p \equiv 1 \pmod{4} \) and \( r = \frac{s-1}{2} \) the following:

**Lemma 2.** Let \( p \equiv 1 \pmod{4} \) be a prime and let \( \sqrt{p} = [q_0; q_1, \ldots, q_s] \), where \( s = 2r + 1 \) then

(8) \( p = b_{r+1}^2 + c_r^2 = b^2 + c^2; \quad b_{r+1} = b, \quad c_r = c \)

(9) \( pQ_r = bP_r + cP_{r-1} \)

(10) \( P_r = bQ_r + cQ_{r-1} \)

(11) \( P_{r-1} = cQ_r - bQ_{r-1} \)

(12) \( P_rQ_{r-1} - Q_rP_{r-1} = (-1)^{r+1} \)

(13) \( P_r^2 - pQ_r^2 = (-1)^{r+1} c \)

(14) \( P_{r-1}^2 - pQ_{r-1}^2 = (-1)^{r} c \)

(15) \( P_{r-1}^2 + P_r^2 = p(Q_{r-1}^2 + Q_r^2). \)

**Lemma 3.** Let \( \sqrt{d} = [q_0; q_1, \ldots, q_s] \) and \( s = 2r + 1 \), then \( Q_{s-1} = Q_{s-1}^2 - 1 + Q_{s-2}^2 \) and

\( P_{s-1} = P_r Q_r + P_{r-1} Q_{r-1}. \)

**Proof.** First we prove that for \( k = 1, 2, \ldots, \frac{s-1}{2} \) we have

(16) \( Q_{s-1} = Q_k Q_{s-(k+1)} + Q_{k-1} Q_{s-(k+2)}. \)

Really, since \( q_{s-1} = q_1, Q_1 = q_1, Q_0 = 1 \) then we obtain \( Q_{s-1} = q_{s-1} Q_{s-2} + Q_{s-3} = Q_1 Q_{s-2} + Q_0 Q_{s-3} \) and (16) is true for \( k = 1 \). Suppose that (16) is true for \( k = m \), i.e.

(17) \( Q_{s-1} = Q_m Q_{s-(m+1)} + Q_{m-1} Q_{s-(m+2)}. \)
Then, for $k = m + 1$ in virtue of $Q_{s-(m+1)} = q_{s-(m+1)}Q_{s-m-2} + Q_{s-m-3}$ and $q_{s-(m+1)} = q_{m+1}$ we get $Q_{s-(m+1)} = q_{m+1}Q_{s-m-2} + Q_{s-m-3}$. By (17) and the last equality it follows that $Q_{s-1} = Q_{m+1}Q_{s-m-2} + Q_{m}Q_{s-m-3}$ and inductive proof of (16) is finished. Putting $k = \frac{s-1}{2}$ and observing that $s-k-1 = \frac{s-1}{2}$, $s-k-2 = \frac{s-1}{2} - 1$, we obtain $Q_{s-1} = Q_{s-1}^2 + Q_{s-1}^2$. In similar way we obtain that $P_{s-1} = P_rQ_r + P_{r-1}Q_{r-1}$ and the proof of Lemma 3 is complete.

**Proof of Theorems**

**Proof of Theorem 1.** Suppose that $p \mid y_0$. Then by (13) of Lemma 2 we have

\begin{align}
(18) \quad c &= (-1)^{r+1}(P_r^2 - pQ_r^2).
\end{align}

From Lemma 2 we also obtain

\begin{align}
(19) \quad b &= (-1)^{r+1}(pQ_rQ_{r-1} - P_rP_{r-1}).
\end{align}

Let $L = cQ_r + bQ_{r-1}$. Then by (18) and (19) it follows that

\begin{align}
(20) \quad L &= (-1)^{r+1}(P_r(P_rQ_r - P_{r-1}Q_{r-1}) - pQ_r(Q_r^2 - Q_{r-1}^2)).
\end{align}

On the other hand from Lemma 2 we have

\begin{align}
(21) \quad P_rQ_r - P_{r-1}Q_{r-1} &= b(Q_r^2 + Q_{r-1}^2).
\end{align}

Substituting (21) to (20) we obtain

\begin{align}
(22) \quad L &= (-1)^{r+1}(bP_r(Q_r^2 + Q_{r-1}^2) - pQ_r(Q_r^2 - Q_{r-1}^2)).
\end{align}

By Lemma 3 it follows that $y_0 = Q_{s-1} = Q_r^2 + Q_{r-1}^2$ and therefore from (22) we get $p \mid L$. From (10) and (11) of Lemma 2 we have

\begin{align}
(23) \quad P_r^2 + P_{r-1}^2 &= (bQ_r + cQ_{r-1})^2 + (cQ_r - bQ_{r-1})^2.
\end{align}

On the other hand it is well-known the following indentity:

\begin{align}
(24) \quad (bQ_r + cQ_{r-1})^2 + (cQ_r - bQ_{r-1})^2 &= (cQ_r + bQ_{r-1})^2 + (bQ_r - cQ_{r-1})^2.
\end{align}

From (23) and (24) we obtain

\begin{align}
(25) \quad P_r^2 + P_{r-1}^2 &= (cQ_r + bQ_{r-1})^2 + (bQ_r - cQ_{r-1})^2.
\end{align}
From (15) of Lemma 2 and the assumption that \( p \mid y_0 \) we obtain

\[(26)\quad p^2 \mid P_r^2 + P_{r-1}^2.\]

By (25), (26) and the fact that \( p \mid L, L = cQ_r + bQ_{r-1} \) it follows that \( p \mid bQ_r - cQ_{r-1} \). Now, we can prove the converse of the theorem. Assume that

\[(27)\quad p \mid cQ_r + bQ_{r-1}, \quad p \mid bQ_r - cQ_{r-1}.\]

From (15) of Lemma 2 and Lemma 3 we obtain

\[(28)\quad P_r^2 + P_{r-1}^2 = p(Q_r^2 + Q_{r-1}^2) = pQ_{s-1} = py_0.\]

By (27) and (25) it follows that \( p^2 \mid P_r^2 + P_{r-1}^2 \) and therefore from (28) we get \( p \mid y_0 \). The proof of the Theorem 1 is complete.

**Proof of the Theorem 2.** From Lemma 3 we have \( P_{s-1} = P_r Q_r + P_{r-1}Q_{r-1} \). Substituting (10) and (11) of Lemma 2 to this equality we obtain

\[(29)\quad P_{s-1} = b(Q_r^2 - Q_{r-1}^2) + 2cQ_rQ_{r-1}.\]

By (29) easily follows that

\[(30)\quad P_{s-1}^2 + 1 = b^2(Q_r^2 - Q_{r-1}^2)^2 + 4bcQ_rQ_{r-1}(Q_r^2 - Q_{r-1}^2) + 4c^2Q_r^2Q_{r-1}^2 + 1.\]

On the other hand from Lemma 2 we can deduce that

\[(31)\quad c(Q_r^2 - Q_{r-1}^2) + (-1)^{r+1} = 2bQ_rQ_{r-1}.\]

From (30) and (31) we obtain

\[(32)\quad c^2(P_{s-1}^2 + 1) = (b^2 + c^2)(4(b^2 + c^2)Q_r^2Q_{r-1}^2 - 4b(-1)^{r+1}Q_rQ_{r-1}^2 + 1).\]

Since \( \langle x_0, y_0 \rangle = \langle P_{s-1}, Q_{s-1} \rangle \) then \( P_{s-1}^2 + 1 = pQ_{q-1}^2 \). Suppose that \( p \mid y_0 \). Then we have

\[(33)\quad p^3 \mid P_{s-1}^2 + 1.\]

By (33) and (32) it follows that

\[(34)\quad p \mid 4bQ_rQ_{r-1} - (-1)^{r+1},\]
because \( p = b^2 + c^2 \). Now, we can assume that the relation (34) is satisfied. Using (32) we obtain

\[
(35) \quad p^2 \mid c^2(P_{s-1}^2 + 1).
\]

Since \( p = b^2 + c^2 \) and \((p, c) = 1\), by (35) it follows that

\[
(36) \quad p^2 \mid P_{s-1}^2 + 1.
\]

But \( P_{s-1}^2 + 1 = pQ_{s-1}^2 \) and consequently from (36) we obtain \( p \mid Q_{s-1} \), \( Q_{s-1} = y_0 \). The proof of the Theorem 2 is complete.

From Theorem 1 we obtain the following:

**Corollary.** Let \( \langle x_0, y_0 \rangle \) be fundamental solution of the equation \( x^2 - py^2 = -1 \), where \( p \equiv 1 \pmod{4} \) is a prime such that \( p = b^2 + c^2 \) and let \( \sqrt{p} = [q_0; q_1, q_2, \ldots, q_s] \), \( s = 2r + 1 \) be the representation of \( \sqrt{p} \) as a simple continued fraction. If \( p \mid y_0 \) then \( \text{ord}_p(cQ_r - bQ_{r-1}) = 1 \) or \( \text{ord}_p(bQ_r - cQ_{r-1}) = 1 \).

**Proof.** If \( p \mid y_0 \) then by the Theorem 1 it follows that \( \alpha = \text{ord}_p(cQ_r + bQ_{r-1}) \geq 1 \) and \( \beta = \text{ord}_p(bQ_r - cQ_{r-1}) \geq 1 \). Suppose that \( \alpha \geq 2 \) and \( \beta \geq 2 \). Then we have

\[
(37) \quad p^2 \mid cQ_r + bQ_{r-1}, \quad p^2 \mid bQ_r - cQ_{r-1}.
\]

From (37) we obtain \( p^2 \mid c^2Q_r + bcQ_{r-1} \) and \( p^2 \mid b^2Q_r - bcQ_{r-1} \). Hence

\[
(38) \quad p^2 \mid (b^2 + c^2)Q_r.
\]

Since \( p = b^2 + c^2 \) then by (38) it follows that \( p \mid Q_r \). By \( y_0 = Q_{s-1} = Q_r^2 + Q_{r-1}^2 \) and virtue of \( p \mid y_0, p \mid Q_r \) we get \( p \mid Q_{r-1} \). On the other hand from Lemma 2 we have \( P_r = bQ_r + cQ_{r-1} \) and therefore we obtain \( p \mid P_r \).

Hence we have \( p \mid P_r \) and \( p \mid Q_r \), which is impossible because \( (P_r, Q_r) = 1 \).

The proof is complete.

**Remark.** If the representation of \( \sqrt{d} \) as a simple continued fraction has the period \( s = 3 \) then \( d \mid y_0 \), where \( \langle x_0, y_0 \rangle \) is the fundamental solution of the non-Pellian equation \( x^2 - dy^2 = -1 \). Really, putting \( s = 3 \) in Lemma 3 we obtain

\[
(39) \quad y_0 = Q_0^2 + Q_1^2 = 1 + q_1^2.
\]
On the other hand it is well-known (see, [8]; Thm. 4, p. 323) that all natural numbers \( d \), for which the representation of \( \sqrt{d} \) as a simple continued fraction has the period \( s = 3 \) are given by the formula:

\[
(40) \quad d \left( (q_1^2 + 1) k + \frac{q_1}{2} \right)^2 + 2q_1 k + 1,
\]

where \( q_1 \) is an even natural number and \( k = 1, 2, 3, \ldots \) Suppose that \( d \mid y_0 \), then we have \( d \leq y_0 \). By (39) and (40) it follows that \( d > y_0 \) and we get a contradiction.

From this observation follows that A-A-C conjecture is true for all primes \( p \equiv 1 \pmod{4} \), having the representation in the form (40).

References


