Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae, 24. (1997) pp. 23–28

Remark on Ankeny, Artin and Chowla conjecture

ALEKSANDER GRYTCZUK

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 $K = Q(\sqrt{p})$ then $p \nmid U$. 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 $p \mid U$ if and only if $p \nmid B_{\frac{p-1}{2}}$, 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

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

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 $\sqrt{p} = [q_0; \overline{q_1, q_2, \ldots, q_s}]$ 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 $p \mid y_0$ if and only if $p \mid cQ_r + bQ_{r-1}$ and $p \mid Q_r - cQ_{r-1}$, 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 $p \mid y_0$ if and only if $p \mid 4bQ_rQ_{r-1} - (-1)^{r+1}$, where $r = \frac{s-1}{2}$ and P_n/Q_n is n-th convergent of $\sqrt{p}$.*

Basic Lemmas

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

$$q_n = \left[\frac{q_0 + b_n}{c_n}\right], \quad b_n + b_{n+1} = c_n q_n, \quad d = b_{n+1}^2 + c_n c_{n+1} \tag{2}$$

(3) *if* $s = 2r + 1$ *then minimal number* k*, for which* $c_{k+1} = c_k$ *is* $k = \frac{s-1}{2}$,

$$dQ_{n-1} = b_n P_{n-1} + c_n P_{n-2}, \tag{4}$$

$$P_{n-1} = b_n Q_{n-1} + c_n Q_{n-2}, \tag{6}$$

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

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* $\sqrt{p} = [q_0; \overline{q_1, \ldots, q_s}]$*, where* $s = 2r + 1$ *then*

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

$$pQ_r = bP_r + cP_{r-1} \tag{9}$$

$$P_r = bQ_r + cQ_{r-1} \tag{10}$$

$$P_{r-1} = cQ_r - bQ_{r-1} \tag{11}$$

$$P_r Q_{r-1} - Q_r P_{r-1} = (-1)^{r+1} \tag{12}$$

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

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

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

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

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

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.

$$Q_{s-1} = Q_m Q_{s-(m+1)} + Q_{m-1} Q_{s-(m+2)}. \tag{17}$$

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 $Q_{s-1} = Q_{m+1}Q_{s-m-2} + Q_mQ_{s-m-3}$ and inductive proof of (16) is finished. Putting $k = \frac{s-1}{2}$ and ovbserving that $s-k-1 = \frac{s-1}{2}$, $s-k-2 = \frac{s-1}{2}-1$, we obatin $Q_{s-1} = Q^2_{\frac{s-1}{2}-1} + Q^2_{\frac{s-1}{2}}$. 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

$$c = (-1)^{r+1}(P_r^2 - pQ_r^2). \tag{18}$$

From Lemma 2 we also obtain

$$b = (-1)^{r+1}(pQ_rQ_{r-1} - P_rP_{r-1}). \tag{19}$$

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

$$L = (-1)^{r+1}\big(P_r(P_rQ_r - P_{r-1}Q_{r-1}) - pQ_r(Q_r^2 - Q_{r-1}^2)\big). \tag{20}$$

On the other hand from Lemma 2 we have

$$P_rQ_r - P_{r-1}Q_{r-1} = b(Q_r^2 + Q_{r-1}^2). \tag{21}$$

Substituting (21) to (20) we obtain

$$L = (-1)^{r+1}\big(bP_r(Q_r^2 + Q_{r-1}^2) - pQ_r(Q_r^2 - Q_{r-1}^2)\big). \tag{22}$$

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

$$P_r^2 + P_{r-1}^2 = (bQ_r + cQ_{r-1})^2 + (cQ_r - bQ_{r-1})^2. \tag{23}$$

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

$$(bQ_r + cQ_{r-1})^2 + (cQ_r - bQ_{r-1})^2 = (cQ_r + bQ_{r-1})^2 + (bQ_r - cQ_{r-1})^2. \tag{24}$$

From (23) and (24) we obtain

$$P_r^2 + P_{r-1}^2 = (cQ_r + bQ_{r-1})^2 + (bQ_r - cQ_{r-1})^2. \tag{25}$$

From (15) of Lemma 2 and the assumption that $p \mid y_0$ we obtain

$$p^2 \mid P_r^2 + P_{r-1}^2. \tag{26}$$

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

$$p \mid cQ_r + bQ_{r-1}, \qquad p \mid bQ_r - cQ_{r-1}. \tag{27}$$

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

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

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 $P_{s-1} = P_rQ_r + P_{r-1}Q_{r-1}$. Substituting (10) and (11) of Lemma 2 to this equality we obtain

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

By (29) easily follows that

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

On the other hand from Lemma 2 we can deduce that

$$c(Q_r^2 - Q_{r-1}^2) + (-1)^{r+1} = 2bQ_rQ_{r-1}. \tag{31}$$

From (30) and (31) we obtain

$$c^2(P_{s-1}^2 + 1) = (b^2 + c^2)\left(4(b^2 + c^2)Q_r^2Q_{r-1}^2 - 4b(-1)^{r+1}Q_rQ_{r-1} + 1\right). \tag{32}$$

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

$$p^3 \mid P_{s-1}^2 + 1. \tag{33}$$

By (33) and (32) it follows that

$$p \mid 4bQ_rQ_{r-1} - (-1)^{r+1}, \tag{34}$$

because $p = b^2 + c^2$. Now, we can assume that the relation (34) is satisfied. Using (32) we obtain

$$p^2 \mid c^2(P_{s-1}^2 + 1). \tag{35}$$

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

$$p^2 \mid P_{s-1}^2 + 1. \tag{36}$$

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 fundamtental 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* $\sqrt{p} = [q_0; \overline{q_1, q_2, \ldots, q_s}]$, $s = 2r + 1$ *be the representation of* $\sqrt{p}$ *as a simple continued fraction. If* $p \mid y_0$ *then* $\operatorname{ord}_p(cQ_r - bQ_{r-1}) = 1$ *or* $\operatorname{ord}_p(bQ_r - cQ_{r-1}) = 1$.

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

$$p^2 \mid cQ_r + bQ_{r-1}, \qquad p^2 \mid bQ_r - cQ_{r-1}. \tag{37}$$

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

$$p^2 \mid (b^2 + c^2)Q_r. \tag{38}$$

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 $d \nmid y_0$, 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

$$y_0 = Q_0^2 + Q_1^2 = 1 + q_1^2. \tag{39}$$

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:

$$d\left(\left(q_1^2+1\right)k+\frac{q_1}{2}\right)^2+2q_1k+1, \tag{40}$$

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

[1] T. Agoh, A note on unit and class number of real quadratic fields *Acta Math. Sinica* **5** (1989), 281–288.

[2] N. C. Ankeny, E. Artin and S. Chowla, The class number of real quadratic number fields *Annals of Math.* **51** (1952), 479–483.

[3] N. C. Ankeny and S. Chowla, A note on the class number of real quadratic fields, *Acta Arith.* VI. (1960), 145–147.

[4] B. D. Beach, H. C. Willims and C. R. Zarnke, Some computer results on units in quadratic and cubic fields, *Proc. 25 Summer Mitting Canad. Math. Congr.* (1971), 609–649.

[5] L. J. Mordell, On a Pellian equation conjecture, *Acta Arith.* VI. (1960), 137–144.

[6] M. Sheingorn, Hyperbolic reflections on Pell's equation, Theory 33. (1989), 267–285.

[7] M. Sheingorn, The $\sqrt{p}$ Riemann surface, *Acta. Arith.* LXIII. 3. (1993), 255–266.

[8] W. Sierpinski, Elementary Thory of Numbers, PWN-Warszawa, (1987)

Aleksander Grytczuk
Intitute of Mathematics
Department of Algebra and Number Theory
T. Kotarbiński Pedagogical University
Pl. Słowiański 9, 65-069 Zielona Góra
Poland