

On some connections between Legendre symbols and continued fractions

ALEKSANDER GRZYTCZUK

Abstract. In this note we give a complement of some results of Friesen given in [2] about some connections between Legendre symbols and continued fractions.

1. Introduction

In the paper [1] P. Chowla and S. Chowla gave several conjectures concerning continued fractions and Legendre symbols. Let $d = pq$, where p, q are primes such that $p \equiv 3 \pmod{4}$, $q \equiv 5 \pmod{8}$ and let $\sqrt{d} = [q_0; \overline{q_1, \dots, q_s}]$ be the representation of \sqrt{d} as a simple continued fraction. Denote by $S = \sum_{i=1}^s (-1)^{s-i} q_i$. Then P. Chowla and S. Chowla conjectured the following relationship: $\left(\frac{p}{q}\right) = (-1)^s$, where $\left(\frac{p}{q}\right)$ is the Legendre's symbol. This conjecture has been proved by A. Schinzel in [3]. Further interesting results for $d = pq \equiv 1 \pmod{4}$ and for $d = 2pq$ was given by C. Friesen in [2]. From his results summarized in the Table 1 on page 365 of [2] it follows that in the following cases: $p \equiv 3 \pmod{8}, q \equiv 1 \pmod{8}$ or $p \equiv 7 \pmod{8}, q \equiv 1 \pmod{8}$ or $p \equiv 1 \pmod{8}, q \equiv 3 \pmod{8}$ or $p \equiv 1 \pmod{8}, q \equiv 7 \pmod{8}$ are not known a connection between Legendre's symbol and the representation of \sqrt{pq} as a simple continued fraction. In this connection we prove the following Theorem:

Theorem. Let $d = pq \equiv 3 \pmod{4}$ and $\sqrt{pq} = [q_0; \overline{q_1, \dots, q_s}]$, then $s = 2m$; $c_m = 2, p, q$; and

$$\begin{aligned} \left(\frac{p}{q}\right) &= (-1)^{m \frac{q-1}{2}}, & \text{if } c_m = p \\ \left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2} \cdot \frac{s+q-1}{2}}, & \text{if } c_m = q \\ \left(\frac{2}{p}\right) \left(\frac{2}{q}\right) &= (-1)^m, & \text{if } c_m = 2 \end{aligned}$$

where c_m is defined by the following recurrent formulas:

$$q_m = \left[\frac{q_0 + b_m}{c_m} \right], \quad b_m + b_{m+1} = c_m q_m, \quad d = pq = b_{m+1}^2 + c_m c_{m+1}.$$

2. Proof of the Theorem

In the proof of the Theorem we use the following lemmas:

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

- (1) $q_n \left[\frac{q_0 + b_n}{c_n} \right]$, $b_n + b_{n+1} = c_n q_n$, $d = b_{n+1}^2 + c_n c_{n+1}$, for any integer $n \geq 0$
- (2) if $s = 2r + 1$ then minimal number k , for which $c_k = c_{k+1}$ is $k = \frac{s-1}{2}$
- (3) if $s = 2r$ then minimal number k , for which $b_k = b_{k+1}$ is $k = \frac{s}{2}$
- (4) $1 < c_n < 2\sqrt{d}$, for $1 \leq n \leq s - 1$
- (5) $P_{n-1}^2 - dQ_{n-1}^2 = (-1)^n c_n$, where P_n/Q_n is n -th convergent of \sqrt{d} .

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

Lemma 2. Let $\sqrt{d} = [q_0; \overline{q_1, \dots, q_s}]$. The equation $x^2 - dy^2 = -1$ is solvable if and only if the period s is odd. Moreover, if $p \equiv 3 \pmod{4}$ and p is a divisor of d then this equation is unsolvable.

This Lemma is well-known result given by Legendre in 1785.

For the proof of the Theorem we remark that by the condition $d = pq \equiv 3 \pmod{4}$ it follows that $p \equiv 3 \pmod{4}$ or $q \equiv 3 \pmod{4}$ and consequently from Lemma 2 we obtain that the period $s = 2m$. From (5) of Lemma 1 we get

$$(6) \quad P_{m-1}^2 - pqQ_{m-1}^2 = (-1)^m c_m.$$

On the other hand by (1) and (3) of Lemma 1 it follows that

$$(7) \quad 2b_{m+1} = q_m c_m, \quad d = pq = b_{m+1}^2 + c_m c_{m+1}.$$

From (7) we obtain

$$(8) \quad 4pq = c_m(q_m^2 c_m + 4c_{m+1}).$$

By (8) it follows that $c_m = 1, 2, 4, p, q, pq, 2pq, 4pq$. Using (4) of Lemma 1 we get that $c_m = 1, 2, 4, p, q$. If $c_m = 1$ then it is easy to see that (6) is impossible. If $c_m = 4$ then from (6) we obtain

$$(9) \quad P_{m-1}^2 - pqQ_{m-1}^2 = (-1)^m 4.$$

Since $(P_{m-1}, Q_{m-1}) = 1$ then by (9) it follows that P_{m-1} and Q_{m-1} are odd and consequently we obtain $P_{m-1}^2 \equiv Q_{m-1}^2 \equiv 1 \pmod{4}$. Since $pq \equiv 3 \pmod{4}$ then by (9) it follows that $1 \equiv P_{m-1}^2 = pqQ_{m-1}^2 + (-1)^m 4 \equiv 3 \pmod{4}$ and we get a contradiction. Therefore, we have $c_m = p, q, 2$. Let $c_m = p$ then from (6) we obtain

$$(10) \quad pX^2 - qQ_{m-1}^2 = (-1)^m, \quad \text{where } P_{m-1} = pX.$$

From (10) and the well-known properties of Legendre's symbol we obtain

$$(11) \quad \left(\frac{p}{q}\right) = \left(\frac{(-1)^m}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}m}.$$

In similar way, for the case $c_m = q$ we get

$$(12) \quad \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}m}.$$

By (12) and the reciprocity law of Gauss we obtain

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{s+q-1}{2}}.$$

If $c_m = 2$ then by (6) it follows that $\left(\frac{2(-1)^m}{p}\right) = \left(\frac{2(-1)^m}{q}\right) = 1$. Hence, in virtue of $pq \equiv 3 \pmod{4}$ we obtain $\left(\frac{2}{p}\right)\left(\frac{2}{q}\right) = (-1)^m$ and the proof is complete.

References

- [1] P. CHOWLA AND S. CHOWLA, Problems on periodic simple continued fractions, *Proc. Nat. Acad. Sci. USA* **69** (1972), 37–45.
- [2] C. FRIESEN, Legendre symbols and continued fractions, *Acta Arith.* **59** 4. (1991), 365–379.
- [3] A. SCHINZEL, On two conjectures of P. Chowla and S. Chowla concerning continued fractions, *Ann. Math. Pure Appl.* **98** (1974), 111–117.

INSTITUTE OF MATHEMATICS
 DEPARTMENT OF ALGEBRA AND NUMBER THEORY
 T. KOTARBIŃSKI PEDAGOGICAL UNIVERSITY
 PL. SŁOWIAŃSKI 9, 65-069 ZIELONA GÓRA
 POLAND