ACTA ARITHMETICA
LIX.4 (1991)

Legendre symbols and continued fractions

by

CHRISTIAN FRIESEN (Toronto)

Introduction. In the paper by P. Chowla and S. Chowla, [1], there are several conjectures concerning continued fractions and Legendre symbols. In particular, if we denote the periodic continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ then Chowla and Chowla hypthothesized the relationship

$$\left(\frac{p}{q}\right) = (-1)^{\Sigma} \quad \text{where } \Sigma = \sum_{i=1}^{k} (-1)^{k-i} a_i$$

and when the N in question is the product of the two primes $p \equiv 3 \pmod 4$ and $q \equiv 5 \pmod 8$. This was proved a short time later by A. Schinzel [4].

That result was not, however, an isolated one and this author was led to examine other cases where it was possible to prove relationships between the alternating sum Σ, the Legendre symbol $(\frac{p}{q})$, and the period of the continued fraction expansions of $\sqrt{pq}$ and $\sqrt{2pq}$. The results are outlined in the following tables. It was found necessary, in some of the cases, to include the relative size of p and q in the formula.

Table 1. $N = pq$ with p, q distinct odd primes. Σ, a_0 and k refer to the continued fraction expansion of $\sqrt{N}$; $\varepsilon = 1$ if $p < q$ and $\varepsilon = -1$ if $p > q$.

	$p \equiv 1$ (8)	$p \equiv 3$ (8)	$p \equiv 5$ (8)	$p \equiv 7$ (8)
$q \equiv 1$ (8)	$\Sigma \equiv 2a_0 k$ (4)		$\Sigma \equiv 2a_0 k$ (4)	
$q \equiv 3$ (8)		$(\frac{p}{q}) = \varepsilon(-1)^{k/2}$	$*(\frac{p}{q}) = (-1)^{\Sigma}$	$(\frac{p}{q}) = \varepsilon(-1)^{k/2}$
$q \equiv 5$ (8)	$\Sigma \equiv 2a_0 k$ (4)	$*(\frac{p}{q}) = (-1)^{\Sigma}$	$\Sigma \equiv 2a_0 k$ (4)	$*(\frac{p}{q}) = (-1)^{\Sigma}$
$q \equiv 7$ (8)		$(\frac{p}{q}) = \varepsilon(-1)^{k/2}$	$*(\frac{p}{q}) = (-1)^{\Sigma}$	$(\frac{p}{q}) = \varepsilon(-1)^{k/2}$

* These formulas were first proved by A. Schinzel [4].

The author would like to acknowledge the support of a Toronto University grant and an NSERC Canada research grant.

Table 2. $N = 2pq$ with p, q distinct odd primes. Σ, a_0 and k refer to the continued fraction expansion of $\sqrt{N}$; $\varepsilon_1 = 1$ if $2q > p$ and $\varepsilon_1 = -1$ if $2q < p$; $\varepsilon_2 = 1$ if $2p < q$ and $\varepsilon_2 = -1$ if $2p > q$.

	$p \equiv 1$ (8)	$p \equiv 3$ (8)	$p \equiv 5$ (8)	$p \equiv 7$ (8)
$q \equiv 1$ (8)	$\Sigma \equiv 2a_0k$ (4)		$\Sigma \equiv 2a_0k$ (4)	
$q \equiv 3$ (8)			$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2}$	$\left(\frac{p}{q}\right) = \varepsilon_1(-1)^{k/2}$
$q \equiv 5$ (8)	$\Sigma \equiv 2a_0k$ (4)	$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2}$	$\Sigma \equiv 2a_0k$ (4)	$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2}$
$q \equiv 7$ (8)		$\left(\frac{p}{q}\right) = \varepsilon_2(-1)^{k/2}$	$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2}$	

The formulas in the above tables, several of which were suggested by computational results, are proved in Sections 5 and 6. The absences in the tables correspond to the lack of a simple relationship between the Σ, $\left(\frac{p}{q}\right)$ and k. There are several identities that we will make use of throughout the later sections and their statement and proof will occupy us for the first part of the paper.

1. Continued fractions: Some elementary results. We begin with some simple facts about continued fraction expansions of quadratic irrationals and use this opportunity to fix our notation. Let x be a positive irrational. We define $F_0(x) = x$ and

$$F_{n+1}(x) = \frac{1}{F_n(x) - [F_n(x)]} \quad \text{for all } n \geqslant 0$$

where the square brackets denote the greatest integer function. Let us fix our irrational x to be the square root of a positive non-square integer N and from here on we will be dropping the explicit dependence on x in our notation. It is possible to write each $F_n(\sqrt{N})$ uniquely in the form

$$F_n = (p_n + \sqrt{N})/q_n$$

where the p_n and q_n are non-negative integers [3, Chapter 3]. We shall use the above as our definition of the quantities p_n and q_n, for $n \geqslant 0$. We now define the *partial denominators*

$$a_n = [(p_n + \sqrt{N})/q_n]$$

and we can write the periodic continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ where k is the period of the expansion. We will also find use for the following two series, written as functions of the partial denominators, where we have again dropped the explicit dependence on $\sqrt{N}$.

$$P_{-1} = 1, \quad P_0 = a_0, \quad P_n = a_nP_{n-1} + P_{n-2} \quad \forall\ 1 \leqslant n \leqslant k,$$
$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_n = a_nQ_{n-1} + Q_{n-2} \quad \forall\ 1 \leqslant n \leqslant k.$$

For the remainder of the paper we fix $N > 2$ to be a non-square integer. The following elementary facts about the continued fraction expansion of $\sqrt{N}$ will be useful.

$$1 < q_n < 2\sqrt{N} \quad \forall\ 1 \leqslant n \leqslant k-1, \quad q_0 = q_k = 1, \tag{1.1}$$

$$0 \leqslant p_n < \sqrt{N} \quad \forall\ n \geqslant 0, \tag{1.2}$$

$$a_n = a_{k-n} \quad \forall\ 1 \leqslant n \leqslant k-1, \quad a_0 = [\sqrt{N}], \quad a_k = 2a_0, \tag{1.3}$$

$$q_n = q_{k-n} \quad \forall\ 0 \leqslant n \leqslant k, \tag{1.4}$$

$$p_n = p_{k+1-n} \quad \forall\ 1 \leqslant n \leqslant k, \tag{1.5}$$

$$Q_nP_{n-1} - P_nQ_{n-1} = (-1)^n \quad \forall\ n \geqslant 0, \tag{1.6}$$

$$P_{n-1}^2 - NQ_{n-1}^2 = (-1)^n q_n \quad \forall\ n \geqslant 0, \tag{1.7}$$

$$p_{n+1} = a_nq_n - p_n \quad \forall\ n \geqslant 0, \tag{1.8}$$

$$q_{n+1} = (N - p_{n+1}^2)/q_n \quad \forall\ n \geqslant 0. \tag{1.9}$$

The first two relations bound the size of the continued fraction quantities q_n and p_n and the next three deal with the symmetry that occurs inside the period. The proofs of all of these results are well known and straightforward. Readers are directed to Perron [3, Chapter 3] for details.

2. Continued fractions: Mid-period results. Our interest in the alternating sum Σ leads us to distinguish between the continued fractions of odd period and those of even period. If the period, k, of the continued fraction is odd then the symmetry result together with the fact that $a_k = 2a_0$ (1.3) leads to the conclusion that $\Sigma = 2a_0$. If, on the other hand, the period is even then the symmetry (1.3) of the continued fraction expansion gives rise to the congruence

$$\Sigma \equiv 2a_0 + a_m + 2\sum_{i=1}^{m-1} a_i \pmod 4 \tag{2.1}$$

where $m = k/2$.

LEMMA. *Let N be a non-square integer greater than 2. Let k be the period of the continued fraction expansion of $\sqrt{N}$. If $k \equiv 0 \pmod 2$ then*

$$a_m = 2\frac{p_m}{q_m}, \tag{2.2}$$

$$q_m | 2N \tag{2.3}$$

where $m = k/2$. If, in addition, we know that N is even then we have

$$q_m | N. \tag{2.4}$$

If the N under consideration is congruent to 2 modulo 4 then we have

$$q_m | p_m \quad \text{and} \quad a_m \equiv 0 \pmod 2. \tag{2.5}$$

Proof. $a_m q_m - p_m = p_{m+1}$ by (1.8). Then we use the symmetry (1.5) to see that $p_{m+1} = p_m$ to arrive at equation (2.2). Using this equation together with the fact (1.9) that $q_m | (N - p_m^2)$ we see that $q_m | 2N$ as required for the second equation. For the proof of the third equation we assume that N is even. If q_m is odd then we obtain $q_m | N$, as desired. For the case where q_m is even we use the fact that q_m divides $N - p_m^2$ together with the fact that N is even to see that p_m must be even. From $q_m | 2p_m$ it must then follow that $q_m | p_m^2$ and we see from this that $q_m | N$, thus finishing the proof of (2.3). We begin the proof of the last equation by noting that if q_m is odd then $q_m | 2p_m$ implies that $q_m | p_m$. If, on the other hand, q_m is even then from $q_m | N - p_m^2$ (1.9) it must follow that p_m is even. Furthermore, since $q_m | N$ we deduce that $q_m \equiv 2 \pmod 4$. Recalling that p_m is even and that $q_m | 2p_m$ we are now able to conclude that $q_m | p_m$.

LEMMA. *Let N be a non-square integer greater than 2. Let k be the period of the continued fraction expansion of $\sqrt{N}$. If N has a prime divisor congruent to 3 modulo 4 then*

$$k \equiv 0 \pmod 2. \tag{2.6}$$

Proof. Let $p \equiv 3 \pmod 4$ be a prime dividing N. Combining the fact that $q_k = 1$ (1.1) with the formula (1.7) gives rise to $P_{k-1}^2 - NQ_{k-1}^2 = (-1)^k$. Looking at this equation modulo p results in the relation

$$1 = \left(\frac{P_{k-1}^2}{p}\right) = \left(\frac{(-1)^k}{p}\right) = (-1)^k,$$

which leads to the desired conclusion that k is even.

3. A modulo 4 identity for Σ. We shall require a number of results relating the parities of the P_n and the Q_n from the continued fraction expansion with our sum Σ. As has been the practice throughout this paper we let N be a non-square integer greater than 2 and we consider the continued fraction expansion of $\sqrt{N}$ with period k. We then have the following

LEMMA. *For all $n \geqslant 1$ we have*

$$a_n + 1 \equiv Q_n + Q_{n-2} + P_n + P_{n-2} + P_n Q_{n-1} + P_{n-1} Q_{n-2} \pmod 2. \tag{3.1}$$

Proof. From the equation $Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n$ (1.6) it follows that not both P_{n-1} and Q_{n-1} can be even. We may encode this fact in a modulo two congruence. Namely, we have

$$P_{n-1} + Q_{n-1} + P_{n-1} Q_{n-1} + 1 \equiv 0 \pmod 2.$$

By multiplying the above identity by a_n and noting that $a_n P_{n-1} = P_n - P_{n-2}$ and $a_n Q_{n-1} = Q_n - Q_{n-2}$ we obtain

$$P_n - P_{n-2} + Q_n - Q_{n-2} + (P_n - P_{n-2}) Q_{n-1} \equiv -a_n \pmod 2.$$

Since we are operating modulo 2 we may replace all subtractions by additions. It only remains to remark that we may use (1.6) to determine that $P_{n-2} Q_{n-1} \equiv P_{n-1} Q_{n-2} + 1 \pmod 2$ and with this substitution we arrive at the desired congruence

$$a_n + 1 \equiv Q_n + Q_{n-2} + P_n + P_{n-2} + P_n Q_{n-1} + P_{n-1} Q_{n-2} \pmod 2.$$

The above identity has a particular form (out of many that it could take) whose usefulness is made clear in the following application.

LEMMA. *Let N be a non-square integer greater than 2. Let k be the period of the continued fraction expansion of $\sqrt{N}$. Then*

$$\sum_{i=1}^{n} (a_i + 1) \equiv a_0 + Q_{n-1} + Q_n + P_{n-1} + P_n + P_n Q_{n-1} \pmod 2 \tag{3.2}$$

for all $n \geqslant 1$.

Proof. The proof is by induction. It is easy to verify that the result is true for $n = 1$. To show that the equation holds for n whenever it holds for $n-1$ we write

$$\begin{aligned} \sum_{i=1}^{n} (a_i + 1) &= \sum_{i=1}^{n-1} (a_i + 1) + (a_n + 1) \\ &\equiv a_0 + Q_{n-2} + Q_{n-1} + P_{n-2} + P_{n-1} + P_{n-1} Q_{n-2} + a_n + 1 \pmod 2. \end{aligned}$$

Replacing $a_n + 1$ with the aid of expression (3.1) and disposing of duplicates (since we are working modulo 2) leaves us with

$$\sum_{i=1}^{n} (a_i + 1) \equiv Q_n + P_n + P_n Q_{n-1} + a_0 + Q_{n-1} + P_{n-1} \pmod 2,$$

which is the identity that we wanted to prove. It follows that equation (3.2) holds for all $n \geqslant 1$.

Combining the above result with the formula (2.1) for Σ modulo 4 gives us the following identity for the case where the continued fraction expansion of $\sqrt{N}$ has even period $= 2m$:

$$\begin{aligned} \Sigma \equiv 2m + 2 + a_m + 2Q_{m-2} + 2Q_{m-1} + 2P_{m-2} + 2P_{m-1} \\ + 2P_{m-1} Q_{m-2} \pmod 4 \end{aligned} \tag{3.3}$$

where the a_n, P_n and Q_n arise out of the continued fraction expansion of $\sqrt{N}$.

4. Some preparatory lemmas. This section provides the proofs of several lemmas that will find frequent application in the theorems to come. The first result of importance to us is the following

LEMMA. *Let $N > 2$ be a non-square integer. Let k denote the period of the continued fraction expansion of $\sqrt{N}$. If k is even then*

$$(-1)^m a_m q_m + 2(P_{m-1}P_{m-2} - NQ_{m-1}Q_{m-2}) = 0 \tag{4.1}$$

where $m = k/2$.

Proof. From the symmetry of the continued fraction, (1.4), we have $q_{m+1} = q_{m-1}$ and we can use formula (1.7) to see that this leads to $P_m^2 - NQ_m^2 = P_{m-2}^2 - NQ_{m-2}^2$. We use the iterative definition to reduce P_m and Q_m to $a_m P_{m-1} + P_{m-2}$ and $a_m Q_{m-1} + Q_{m-2}$, respectively, and we arrive at

$$a_m^2 P_{m-1}^2 + 2a_m P_{m-1}P_{m-2} + P_{m-2}^2 - Na_m^2 Q_{m-1}^2 - 2Na_m Q_{m-1}Q_{m-2} - NQ_{m-2}^2 = P_{m-2}^2 - NQ_{m-2}^2.$$

Rearranging and cancelling provides us with the following equation:

$$a_m^2(P_{m-1}^2 - NQ_{m-1}^2) + 2a_m P_{m-1}P_{m-2} - 2Na_m Q_{m-1}Q_{m-2} = 0.$$

Now we invoke identity (1.7) and then divide the entire equation by a_m to get the desired identity.

We conclude this section with the following

LEMMA. *If $N = 2pq$ where p and q are distinct odd primes and if the continued fraction expansion of $\sqrt{N}$ has even period $= 2m$ then we have the identities:*

$$\Sigma \equiv 2m + P_{m-1} + 2 \pmod 4 \quad \text{if } q_m \text{ even}, \tag{4.2}$$

$$\Sigma \equiv 2m + 2Q_{m-1} \pmod 4 \quad \text{if } q_m \text{ odd}. \tag{4.3}$$

Proof. We should preface this proof by remarking that it is possible to arrive at this result via some stronger (modulo 8) congruences proved by Heinrich Lang in [2]. But such a proof would take us out of our way in establishing the connections between the three quantities of interest to us, namely m, Q_{m-1} and P_{m-1}, and the fundamental unit parameters that were used in his paper (which can be easily converted to Q_{2m-1} and P_{2m-1}). It is possible to use the results of Lang to determine Σ modulo 4 in terms of Q_{2m-1} and P_{2m-1} with very little effort and if our only goal were to determine Σ modulo 4 then we would be well-advised to take the above approach. The relationships of Σ with the Legendre symbols and parity of m would not, however, be apparent and it is our interest in precisely this interplay that prompts the following proof which proceeds independent of the results of Lang.

To begin the proof we take formula (1.7) with $n = m$ and, after making note of the fact (2.4) that $q_m | N$, we arrive at

$$q_m X^2 - \frac{N}{q_m} Q_{m-1}^2 = (-1)^m \tag{4.4}$$

where $X = P_{m-1}/q_m$.

Proof of formula (4.2). If $q_m \equiv 0 \pmod 2$ then $q_m | N$ implies that $q_m \equiv 2 \pmod 4$. Considering the above equation modulo 4 shows that Q_{m-1} is odd and that P_{m-1} is even and we use this in equation (1.6) to see that P_{m-2} must be odd. Equation (2.5) implies that a_m is even and using this along with $q_m \equiv 2 \pmod 4$ in (4.1) leads to the congruence $2a_m + 2P_{m-1} - 4Q_{m-2} \equiv 0 \pmod 8$ which in turn gives rise to

$$a_m + P_{m-1} + 2Q_{m-2} \equiv 0 \pmod 4.$$

We use our knowledge of the parities of Q_{m-1} and P_{m-2} together with this most recent equation and formula (3.3) to obtain the desired identity of (4.2).

For the proof of formula (4.3) we look at equation (4.4) and conclude from q_m being odd that P_{m-1} must be odd as well. From (2.5) we see that, since N is even, a_m is even. We now consider (4.1) modulo 4 to arrive at $a_m + 2P_{m-2} \equiv 0 \pmod 4$. We use the previous equation, together with the fact that P_{m-1} is odd, in the formula (3.3) to obtain

$$\begin{aligned}\Sigma &\equiv a_m + 2Q_{m-1} + 2Q_{m-2} + 2P_{m-1} + 2P_{m-2} + 2P_{m-1}Q_{m-2} + 2m + 2 \pmod 4\\ &\equiv 2Q_{m-1} + 2Q_{m-2} + 2P_{m-1} + 2P_{m-1}Q_{m-2} + 2m + 2 \pmod 4\\ &\equiv 2Q_{m-1} + 2Q_{m-2} + 2 + 2Q_{m-2} + 2m + 2 \pmod 4\\ &\equiv 2Q_{m-1} + 2m \pmod 4\end{aligned}$$

as required.

We are now prepared to state and prove our major theorems.

5. Theorems for the case $N = pq$.

THEOREM 1. *Let $p \equiv q \equiv 1 \pmod 4$ be distinct primes and let $N = pq$. Write the continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ with period k and define $\Sigma = \sum_{i=1}^{k} (-1)^{k-i} a_i$. Then*

$$\Sigma \equiv 2a_0 k \pmod 4.$$

Proof. It is easy to see from the symmetry of the continued fraction expansion (1.3) that when k is odd we obtain the result $\Sigma = 2a_0$ which satisfies the above congruence. It remains to show that $k \equiv 0 \pmod 2$ implies that $\Sigma \equiv 0 \pmod 4$. Let $k = 2m$. From (1.7) we have

$$P_{m-1}^2 - pqQ_{m-1}^2 = (-1)^m q_m. \tag{5.1}$$

Taking this equation modulo 4 shows that q_m cannot be congruent to 2 modulo 4. From (2.3) we know that $q_m|2pq$ and since $q_m \not\equiv 2 \pmod 4$ it follows that $q_m \equiv 1 \pmod 4$. Using equation (2.2) with q_m odd shows that a_m is even. We now consider two cases, depending on the parity of the half-period, m.

Case 1. Let $m \equiv 0 \pmod 2$. From (5.1) it follows that $P_{m-1} \equiv 1 \pmod 2$ and $Q_{m-1} \equiv 0 \pmod 2$. This latter congruence, together with (1.6), shows that Q_{m-2} must be odd. Using the fact that a_m is even and q_m is odd in equation (4.1) leads to the congruence

$$a_m \equiv 2P_{m-2} \pmod 4.$$

We combine the above congruences in equation (3.3) to see that $\Sigma \equiv 0 \pmod 4$.

Case 2. Let $m \equiv 1 \pmod 2$. From (5.1) we have $P_{m-1} \equiv 0 \pmod 2$ and $Q_{m-1} \equiv 1 \pmod 2$. The former congruence implies (from (1.6)) that $P_{m-2} \equiv 1 \pmod 2$. Using the fact that a_m is even and q_m is odd in equation (4.1) leads to the congruence

$$a_m \equiv 2Q_{m-2} \pmod 4.$$

Combining the above results in the congruence (3.3) leads to the desired conclusion that $\Sigma \equiv 0 \pmod 4$ and this finishes the proof of Theorem 1.

THEOREM 2. *Let $p \equiv q \equiv 3 \pmod 4$ be distinct primes and let $N = pq$. Let k denote the period of the continued fraction expansion of $\sqrt{N}$. Then k is even and*

$$\left(\frac{p}{q}\right) = \varepsilon(-1)^{k/2}$$

where $\varepsilon = 1$ if $p < q$ and $\varepsilon = -1$ if $p > q$.

Proof. Since N is divisible by a prime congruent to 3 modulo 4 it follows, from (2.6), that k is even. We may write $m = k/2$. From (1.7) we have

$$P_{m-1}^2 - pqQ_{m-1}^2 = (-1)^m q_m.$$

As in the previous proof, looking at this equation modulo 4 shows that q_m cannot be congruent to 2 modulo 4. It follows from $q_m|2N$ (2.3) that q_m is odd. Since $q_m|2p_m$ (2.2) and $p_m < \sqrt{N}$ (1.2) we see that $q_m < \sqrt{N}$. Together with $q_m > 1$ (1.1) the preceding restricts q_m to one possible value, namely the smaller of p and q. If $p < q$ then $q_m = p$ and we rewrite the above equation to get

$$pX^2 - qQ_{m-1}^2 = (-1)^m$$

where $X = P_{m-1}/p$. Considering this equation modulo q leads to the desired result

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

If, on the other hand, $p > q$ then q_m must equal q and we obtain

$$qX^2 - pQ_{m-1}^2 = (-1)^m$$

where $X = P_{m-1}/q$. Considering this equation modulo q leads to the desired result

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{m+1}}{q}\right) = -(-1)^m,$$

which completes the proof of Theorem 2.

THEOREM 3. *Let $p \equiv 3 \pmod 4$ and $q \equiv 5 \pmod 8$ be primes and let $N = pq$. Write the continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ with period k and define $\Sigma = \sum_{i=1}^{k} (-1)^{k-i} a_i$. Then $k \equiv 0 \pmod 2$ and*

$$\left(\frac{p}{q}\right) = (-1)^{\Sigma}.$$

Proof. A proof of this theorem, using the same techniques as found throughout this paper, has been omitted in the interest of brevity. Interested readers may find a proof in [4].

6. Theorems for the case $N = 2pq$.

THEOREM 4. *Let $p \equiv q \equiv 1 \pmod 4$ be two distinct primes and let $N = 2pq$. Write the continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ with period k and define $\Sigma = \sum_{i=1}^{k} (-1)^{k-i} a_i$. Then*

$$\Sigma \equiv 2a_0 k \pmod 4.$$

Proof. We begin by noting that this is obvious if k is odd as then we have $\Sigma = 2a_0$, which trivially gives us the desired result. From this point in the proof onwards we shall assume that k is even and we let $m = k/2$. We know, from (2.4), that $q_m|N$ and we proceed by looking at the two cases $q_m \equiv 2 \pmod 8$ and $q_m \equiv 1 \pmod 4$. In both cases we will be examining the equation

$$P_{m-1}^2 - 2pqQ_{m-1}^2 = (-1)^m q_m,$$

which we get by letting $n = m$ in (1.7).

Case 1. Let $q_m \equiv 2 \pmod 8$. The above equation, considered modulo 8, gives rise to the following congruence modulo 4:

$$2X^2 - Q_{m-1}^2 \equiv (-1)^m \pmod 4$$

where $X = P_{m-1}/2$. Since we must have Q_{m-1} odd we derive the relationship

$$P_{m-1} \equiv 2X \equiv 2m+2 \pmod 4.$$

We now apply (4.2) to obtain the desired equivalence $\Sigma \equiv 0 \equiv 2a_0 k \pmod 4$.

Case 2. Let $q_m \equiv 1 \pmod 4$. It follows from $P_{m-1}^2 - 2pqQ_{m-1}^2 = (-1)^m q_m$ that P_{m-1} is odd and that $Q_{m-1} \equiv m \pmod 2$. Applying (4.3) shows that

$\Sigma \equiv 0 \equiv 2a_0 k \pmod 4$ in this last case as well. This finishes the proof of Theorem 4.

THEOREM 5. *Let $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ be primes and let $N = 2pq$. Let k denote the period of the continued fraction expansion of $\sqrt{N}$. Then k is even and*

$$\left(\frac{p}{q}\right) = \varepsilon(-1)^{k/2}$$

where $\varepsilon = 1$ if $2p < q$ and $\varepsilon = -1$ if $2p > q$.

Proof. Since N has a prime divisor congruent to 3 modulo 4 it follows that k must be even. We will make repeated use of equation (4.4) which we shall duplicate here:

$$q_m X^2 - \frac{N}{q_m} Q_{m-1}^2 = (-1)^m \tag{6.1}$$

where $X = P_{m-1}/q_m$. From $q_m | N$ (2.4) we see that q_m is restricted to divisors of N. The fact that $q_m | p_m$ (2.5) and $p_m < \sqrt{N}$ (1.2) taken together with the restriction that $q_m > 1$ (1.1) forces $1 < q_m < \sqrt{N}$. This limits q_m to the following cases:

Case 1. Let $q_m = 2$. Taking (6.1) modulo p we see that

$$-1 = \left(\frac{2}{p}\right) = \left(\frac{2X^2}{p}\right) = \left(\frac{(-1)^m}{p}\right) = (-1)^m,$$

which implies that m must be odd. Using this fact when we take (6.1) modulo q results in the contradiction that

$$1 = \left(\frac{2}{q}\right) = \left(\frac{2X^2}{q}\right) = \left(\frac{(-1)^m}{q}\right) = (-1)^m = -1$$

and we are forced to conclude that this case does not occur.

Case 2. Let $q_m = p$. Here (6.1) gives rise to

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

and

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

We now notice that both p and q are congruent to 3 modulo 4 and, by the law of quadratic reciprocity, we must have

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

This results in a contradiction and shows that this case fails to arise.

Case 3. Let $q_m = 2q$. The analysis for this case is similar to that of the previous one and we arrive at a contradiction that eliminates this case.

Case 4. Let $q_m = 2p$. We begin by noting that $q_m < \sqrt{N}$ implies that we must have $2p < q$ for this case to occur. From (6.1) we have

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

as required.

Case 5. Let $q_m = q$. We note that this case can arise only if $2p > q$ as q_m must be smaller than $\sqrt{N}$. Again we consider (6.1) to arrive at the conclusion that

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

This is the required result and the proof of the theorem is complete.

THEOREM 6. *Let $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$ be primes and let $N = 2pq$. Write the continued fraction expansion of $\sqrt{N}$ as $(a_0; \overline{a_1, a_2, \ldots, a_k})$ with period k and define $\Sigma = \sum_{i=1}^{k} (-1)^{k-i} a_i$. Then*

$$\Sigma \equiv \left(\frac{p}{q}\right) + 1 \pmod 4. \tag{6.2}$$

Proof. Since N is divisible by a prime congruent to 3 modulo 4 it follows from (2.6) that we may write $k = 2m$ for some integer m. We also have equation (2.4) restricting q_m to divisors of N. From $q_m | p_m$ (2.5) and $p_m < \sqrt{N}$ (1.2) we see that $q_m < \sqrt{N}$. A consequence of this, and the fact that $q_m > 1$ (1.1), is that we can eliminate $q_m = 1$, pq and $2pq$ from consideration. We now examine the remaining positive divisors of $2pq$ as values for q_m and consider, in each case, equation (6.1).

Case 1. If $q_m = 2$ then we consider equation (6.1) modulo p and make use of the fact that -1 is a quadratic residue modulo p and that 2 is not. This leads to the contradiction that

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

It follows that this case does not occur.

Case 2. If $q_m = 2q$ then (6.1) becomes

$$2qX^2 - pQ_{m-1}^2 = (-1)^m.$$

Since the right-hand side is odd we must have Q_{m-1} odd as well. Reducing this equation modulo 8 gives

$$6X^2 - 5 \equiv (-1)^m \pmod 8,$$

which forces X odd and m even. Since m is even and $P_{m-1} = 2qX \equiv 2 \pmod 4$ it follows from (4.2) that $\Sigma \equiv 0 \pmod 4$. It remains necessary to show that $\left(\frac{p}{q}\right) = -1$. Once again we consider equation (6.1), this time modulo q, to see that

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

Recalling that m is even leads to the desired congruence $\Sigma \equiv \left(\frac{p}{q}\right)+1 \pmod 4$.

Case 3. If $q_m = p$ then taking (6.1) modulo 8 gives us

$$5X^2 - 6Q_{m-1}^2 \equiv (-1)^m \pmod 8$$

and the only possible solutions to this are when m, X and Q_{m-1} are all odd. Since q_m, Q_{m-1} and m are all odd it follows from (4.3) that $\Sigma \equiv 0 \pmod 4$. Looking at (6.1) modulo q gives

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

and therefore the desired relationship between Σ and $\left(\frac{p}{q}\right)$ holds for this case.

Case 4. $q_m = 2p$. Parity considerations applied to (6.1) force Q_{m-1} to be odd and we then take (6.1) modulo 4 to get $2X^2+1 \equiv (-1)^m \pmod 4$. It is easy to see that X and m must have the same parity. This leads us to the congruence $P_{m-1} = 2pX \equiv 2X \equiv 2m \pmod 4$. Applying equation (4.2) gives us the result $\Sigma \equiv 2 \pmod 4$. Using the law of quadratic reciprocity and considering (6.1) modulo p we see that

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

as required.

Case 5. $q_m = q$. From (6.1) it is clear that both X and P_{m-1} must be odd. If we consider equation (6.1) modulo 4 we see that $Q_{m-1} \equiv m+1 \pmod 2$. Applying (4.3) we come to the conclusion that $\Sigma \equiv 2 \pmod 4$. We evaluate the Legendre symbol by using equation (6.1) together with the law of quadratic reciprocity to obtain

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

which satisfies the desired relation, thus finishing the proof of Theorem 6.

We use these results in Table 2 by recognizing that

$$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2} \Leftrightarrow \Sigma \equiv \left(\frac{p}{q}\right)+1 \pmod 4.$$

For the case where the roles of p and q are reversed we note that $\Sigma = \left(\frac{q}{p}\right)+1 \pmod 4$ taken together with $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ (from quadratic reciprocity)

shows, as needed, that

$$\left(\frac{p}{q}\right) = -(-1)^{\Sigma/2}$$

in this case as well.

7. Concluding comments. The cases considered in this paper, namely where N is the product of two distinct odd primes or where N is twice such a product, are, in some sense, both the most general cases and also the simplest ones, for which we can hope to arrive at relationships between the Legendre symbols, the alternating sum, Σ, and the period of the continued fraction expansion of $\sqrt{N}$. One can expect more complications (and many more separate cases to examine) when N has 3 or more odd prime factors.

With the exception of those results of the form $\Sigma \equiv 2a_0k \pmod 4$ the theorems proved in this paper were all of a similar nature. After noting that k, the period of the continued fraction expansion of $\sqrt{N}$, was even we began an examination of the equation

$$P_{m-1}^2 - NQ_{m-1}^2 = (-1)^m q_m$$

where $m = k/2$. This mid-period identity was useful precisely because of the fact that we could limit q_m to positive factors of $2N$ (and, if N was even, to factors of N itself). Eliminating some cases by the size restrictions ($q_m > 1$, $q_m | 2p_m$, and $p_m < \sqrt{N}$) and others by modulo 8 congruences or by quadratic residuacity results left us with sufficiently few possibilities that a governing relationship could be deduced.

As a concluding remark the author would like to point out that it is possible, in some of the cases treated in this paper, to rewrite the results in terms of congruences involving the fundamental unit of $\boldsymbol{Q}(\sqrt{N})$. Witness the following

THEOREM 7. *Let $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ be primes and let $N = 2pq$. Let $T+U\sqrt{N}$ be the fundamental unit of $\boldsymbol{Q}(\sqrt{N})$. Then U is even and*

$$\left(\frac{p}{q}\right) = (-1)^{U/2}.$$

Proof. We begin by remarking that, since $N \equiv 2 \pmod 4$ has a prime factor congruent to 3 modulo 4, the fundamental unit of $\boldsymbol{Q}(\sqrt{N})$ must be equal to $P_{k-1}+Q_{k-1}\sqrt{N}$ where k is the (necessarily even) period of the continued fraction expansion of $\sqrt{N}$ and where P_{k-1} and Q_{k-1} are as defined in Section 1. We define the mid-period $m = k/2$. We state here, without proof, the following identity, valid for the continued fraction expansion of $\sqrt{N}$, where N is a non-square integer greater than 2 with period $= 2m$:

$$Q_{2m-1} = Q_{m-1}(a_mQ_{m-1} + 2Q_{m-2}). \tag{7.1}$$

The proof (not included here) is an inductive argument that hinges on the symmetry of the continued fraction expansion. We will also make use of the fact that $a_m \equiv 0 \pmod 2$ (2.5). We examine the proof of Theorem 5 and see that the only two cases that may occur are $q_m = 2p$ and $q_m = q$.

Case 1. If $q_m = 2p$ then (6.1) becomes $2pX^2 - qQ_{m-1}^2 = (-1)^m$, which gives rise to

$$2X^2 + Q_{m-1}^2 \equiv (-1)^m \pmod 4.$$

Since Q_{m-1} is odd it follows that $X \equiv m \pmod 2$. From $P_{m-1} = 2pX \equiv 0 \pmod 2$ and identity (1.6) it follows that P_{m-2} is odd. Looking at (4.1) modulo 8 gives us $2a_m + 4Q_{m-2} \equiv 2P_{m-1} \pmod 8$, which leads to

$$a_m + 2Q_{m-2} \equiv P_{m-1} \pmod 4.$$

Combining the above identity with the fact that Q_{m-1} is odd and applying (7.1) gives the result

$$Q_{2m-1} \equiv a_m + 2Q_{m-2} \equiv P_{m-1} \pmod 4.$$

Recalling that $U = Q_{2m-1}$ and $P_{m-1} = 2pX$ shows that $U \equiv 2X \equiv 2m \pmod 4$. Now we use the result from Case 4 of Theorem 5 to see that

$$\left(\frac{p}{q}\right) = (-1)^m = (-1)^{U/2}$$

as required.

Case 2. If $q_m = q$ then (6.1) becomes $qX^2 - 2pQ_{m-1}^2 = (-1)^m$, from which we obtain

$$-X^2 + 2Q_{m-1}^2 \equiv (-1)^m \pmod 4.$$

Since X is clearly odd it follows that $Q_{m-1} \equiv m+1 \pmod 2$. Here we must split the remainder of the argument into two pieces, depending on the parity of Q_{m-1}.

If Q_{m-1} is even then m is odd and (7.1) gives $Q_{2m-1} \equiv 0 \pmod 4$. Recalling that $U = Q_{2m-1}$ and using the results of Case 5 in Theorem 5 we see that

$$\left(\frac{p}{q}\right) = (-1)^{m+1} = 1 = (-1)^{U/2}.$$

If Q_{m-1} is odd then m is even. We have $U = Q_{2m-1} \equiv a_m + 2Q_{m-2} \pmod 4$ from (7.1). Since both Q_{m-1} and P_{m-1} $(= qX)$ are odd it follows from (1.6) that $P_{m-2} + Q_{m-2} \equiv 1 \pmod 2$. Substituting this last equation into the former one gives rise to

$$U \equiv a_m + 2P_{m-2} + 2 \pmod 4.$$

We use the fact that q_m and P_{m-1} are odd and that a_m is even together with equation (4.1) to see that $a_m + 2P_{m-2} \equiv 0 \pmod 4$ and this leads to the equality $U \equiv 2 \pmod 4$. We make use of the result of Case 5 in Theorem 5 and it follows that

$$\left(\frac{p}{q}\right) = (-1)^{m+1} = -1 = (-1)^{U/2}$$

as required. This finishes the proof of Theorem 7.

References

[1] P. Chowla and S. Chowla, *Problems on periodic simple continued fractions*, Proc. Nat. Acad. Sci. U.S.A. 69 (1972), 37–45.

[2] H. Lang, *Über einfache periodische Kettenbrüche und Vermutungen von P. Chowla und S. Chowla*, Acta Arith. 28 (1976), 419–428.

[3] O. Perron, *Die Lehre von den Kettenbrüchen*, Chelsea Publishing Company, New York 1950.

[4] A. Schinzel, *On two conjectures of P. Chowla and S. Chowla concerning continued fractions*, Ann. Mat. Pura Appl. 98 (1974), 111–117.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TORONTO
Toronto, Canada, M5S 1A1

Received on 27.9.1990
and in revised form on 6.12.1990 (2084)