Reprinted from:
The American Mathematical Monthly
Volume 106, Number 1, pp 52–56
January, 1999

A Note on Jacobi Symbols and Continued Fractions

A. J. van der Poorten and P. G. Walsh

1. INTRODUCTION. It is well known that the continued fraction expansion of a real quadratic irrational is periodic. Here we relate the expansion for $\sqrt{rs}$, under the assumption that $rX^2 - sY^2 = \pm 1$ has a solution in integers X and Y, to that of $\sqrt{r/s}$ and to the Jacobi symbols $\left(\frac{r}{s}\right)$ which appear in the theory of quadratic residues.

We have endeavoured to make our remarks self-contained to the extent of providing a brief reminder of the background theory together with a cursory sketch of the proofs of the critical assertions. For extensive detail the reader can refer to [5], the bible of the subject. The introductory remarks following in §§2–3 below are *inter alia* detailed in [1].

Let p and q denote distinct odd primes. In [3], Friesen proved connections between the value of the Legendre symbol $\left(\frac{p}{q}\right)$ and the length of the period of the continued fraction expansion of $\sqrt{pq}$. These results, together with those of Schinzel in [6], provided a solution to a conjecture of Chowla and Chowla in [2].

We report a generalization of those results to the evaluation of Jacobi symbols $\left(\frac{r}{s}\right)$, and, in the context of there being a solution in integers X, Y to the equation $rX^2 - sY^2 = \pm 1$, to remark on the continued fraction expansion of $\sqrt{r/s}$ *vis à vis* that of $\sqrt{rs}$.

Theorem 1. *Let r and s be squarefree positive integers with $r > s > 1$, such that the equation $rX^2 - sY^2 = \pm 1$ has a solution in positive integers X, Y. Suppose the continued fraction expansion of $\sqrt{rs}$ is $[\, a_0\,, \overline{a_1\,, a_2\,, \ldots, a_l}\,]$. Then both the length of the period $l = 2h$, and the 'central' partial quotient a_h, are even, and the continued fraction expansion of $\sqrt{r/s}$ is*

$$[\, \tfrac{1}{2}a_h\,, \overline{a_{h+1}\,, \ldots, a_l\,, a_1\,, \ldots, a_h}\,] = [\, \tfrac{1}{2}a_h\,, \overline{a_{h-1}\,, \ldots, a_1\,, a_l\,, a_1\,, \ldots, a_{h-1}\,, a_h}\,].$$

Theorem 2. *Let r and s be squarefree positive integers with $r > s > 1$, such that the equation $rX^2 - sY^2 = \pm 1$ has a solution in positive integers X, Y. Denote by l the length of the period of the continued fraction expansion of $\sqrt{rs}$. Then the following Jacobi symbol equalities hold:*

$$\left(\frac{r}{s}\right) = \left(\frac{-1}{s}\right)^{\frac{1}{2}l+1}, \qquad \left(\frac{s}{r}\right) = \left(\frac{-1}{r}\right)^{\frac{1}{2}l}.$$

As an immediate consequence we obtain the following results which respectively appeared as Theorem 2 and Theorem 5 in [3].

Corollary 1. *Let $p \equiv q \equiv 3 \pmod 4$ be distinct primes and set $N = pq$. Denote by l the length of the period of the continued fraction expansion of $\sqrt{N}$. Then l is even, and*

$$\left(\frac{p}{q}\right) = \epsilon(-1)^{\frac{1}{2}l},$$

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

Corollary 2. *Let* $p \equiv 3 \pmod 8$ *and* $q \equiv 7 \pmod 8$ *be primes and set* $N = 2pq$. *Denote by* l *the length of the period of the continued fraction expansion of* $\sqrt{N}$. *Then* l *is even, and*

$$\left(\frac{p}{q}\right) = \epsilon(-1)^{\frac{1}{2}l},$$

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

2. CONTINUED FRACTIONS. In this section we recall some basic facts about continued fractions that will be appealed to in the proof of our results.

Given an irrational number α, define its sequence $(\alpha_i)_{i\geq 0}$ of *complete quotients* by setting $\alpha_0 = \alpha$, and $\alpha_{i+1} = 1/(\alpha_i - a_i)$. Here, the sequence $(a_i)_{i\geq 0}$ of *partial quotients* of α is given by $a_i = \lfloor \alpha_i \rfloor$ where $\lfloor\ \rfloor$ denotes the integer part of its argument. Plainly we have

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

It is only the partial quotients that matter, so such a continued fraction expansion may be conveniently denoted just by $[\,a_0\,,\,a_1\,,\,a_2\,,\,a_3\,,\,\ldots]$.

The truncations $[\,a_0\,,\,a_1\,,\,\ldots\,,\,a_i\,]$ plainly are rational numbers p_i/q_i. Here, the pairs of relatively prime integers p_i, q_i are given by the matrix identities

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix}$$

and the remark that the empty matrix product is the identity matrix. The alleged correspondence, whereby matrix products provide the *convergents* p_i/q_i, may be confirmed by induction on the number of matrices on noticing the definition

$$[\,a_0\,,\,a_1\,,\,\ldots\,,\,a_i\,] = a_0 + 1/[\,a_1\,,\,\ldots\,,\,a_i\,], \qquad [\,a_0\,] = a_0\,.$$

Incidentally, it clearly follows from transposing the matrix correspondence that

$$(1) \qquad [\,a_i\,,\,a_{i-1}\,,\,\ldots\,,\,a_1\,] = q_i/q_{i-1}, \quad \text{for} \quad i = 1, 2, \ \ldots\ .$$

The matrix correspondence entails $p_i/q_i = p_{i-1}/q_{i-1} + (-1)^{i-1}/q_{i-1}q_i$ whence, by induction, $\alpha = a_0 + \sum_{i=1}^{\infty}(-1)^{i-1}/q_{i-1}q_i$, and so

$$0 < (-1)^{i-1}(q_i\alpha - p_i) < 1/q_{i+1}\,,$$

displaying the excellent quality of approximation to α provided by its convergents. Conversely, if

$$(2) \qquad |q\alpha - p| < 1/2q\,,$$

then the rational p/q must be a convergent to α.

3. CONTINUED FRACTIONS OF SQUARE ROOTS OF RATIONALS. In the case $\alpha = \sqrt{N}$, for positive integer N not a square, it is well known and easy to confirm by induction that its complete quotients α_i are all of the shape

$$\alpha_i = (P_i + \sqrt{N})/Q_i\,,$$

with the sequences of integers (P_i) and (Q_i) given sequentially by

$$P_{i+1} + P_i = a_i Q_i, \quad \text{and} \quad Q_{i+1}Q_i = N - P_{i+1}^2\,,$$

where $\alpha_0 = \sqrt{N}$ entails $P_0 = 0$ and $Q_0 = 1$. Plainly, always $P_i^2 \equiv N \pmod{Q_i}$. Moreover, it is easy to see that the integers P_i all satisfy $0 \le P_i < \sqrt{N}$ and the positive integers Q_i are all less than $2\sqrt{N}$. It follows by the box principle that the continued fraction expansion of $\sqrt{N}$ must be periodic. Much more is fairly clear.

First, note that the generic step in the continued fraction algorithm for $\alpha = \sqrt{N}$ is

$$\alpha_i = (P_i + \sqrt{N})/Q_i = a_i - (P_{i+1} - \sqrt{N})/Q_i\,.$$

Under conjugation $\sqrt{N} \mapsto -\sqrt{N}$, this step transforms to

$$(P_{i+1} + \sqrt{N})/Q_i = a_i - (P_i - \sqrt{N})/Q_i\,. \tag{3}$$

But the 0-th step, ingeniously adjusted by adding $a_0 = P_1$,

$$a_0 + \sqrt{N} = 2a_0 - (a_0 - \sqrt{N})$$

is plainly invariant under conjugation. Moreover, because $-1 < P_1 - \sqrt{N} < 0$ we have $(P_1 + \sqrt{N})/Q_1 > 1$. On the other hand $P_1 + \sqrt{N} > 1$ of course entails $-1 < (P_1 - \sqrt{N})/Q_1 < 0$. It's now easy to see, by induction on i, that in (3) $-1 < (P_i - \sqrt{N})/Q_i < 0$. So a_i is the integer part of $(P_{i+1} + \sqrt{N})/Q_i$ and (3) is a step in the continued fraction expansion of $a_0 + \sqrt{N}$, and thus of $\sqrt{N}$.

It follows that the sequence of steps detailing the continued fraction expansion of $a_0 + \sqrt{N}$ is inverted by conjugation, that since it has a fixed point the entire tableaux must be periodic, and that, with l the length of the period, we must have

$$a_0 + \sqrt{N} = [\,\overline{2a_0\,,\, a_1\,,\, a_2\,,\, \ldots\,,\, a_{l-1}}\,], \tag{4}$$

moreover with the *word* $a_1 a_2 \ldots a_{l-1}$ a palindrome.

Lemma. *The symmetry just mentioned entails that for even period length l there is a 'central' step, at $h = \frac{1}{2}l$,*

$$\alpha_h = (P_h + \sqrt{N})/Q_h = a_h - (P_{h+1} - \sqrt{N})/Q_h\,,$$

invariant under conjugation. So $P_{h+1} = P_h$, and $a_h = 2P_h/Q_h$. It follows that $Q_h \big| 2N$. Conversely, if N is squarefree and $Q_j \big| 2N$, where $j \ne 0$, then l is even and $2j = l$.

Proof. Plainly $Q_h \big| N - P_h^2$ and $Q_h \big| 2P_h$ entails $Q_h \big| 2N$. As regards the converse, it suffices to notice that $Q_j \big| N - P_j^2$ and $Q_j \big| 2N$ implies $Q_j \big| 2P_j^2$. The only possible square factor of Q_j is 4, since N is squarefree and $Q_j \big| 2N$, so it follows that $Q_j \big| 2P_j$; say $2P_j/Q_j = a_j$. Thus

$$\alpha_j = (P_j + \sqrt{N})/Q_j = a_j - (P_j - \sqrt{N})/Q_j$$

is a step in the continued fraction expansion of $\sqrt{N}$ invariant under conjugation. It therefore must be the central such step, and this is what we were to show. ∎

Again by induction, or otherwise, one can confirm that

$$\begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} \begin{pmatrix} 1 & P_{i+1} \\ 0 & Q_{i+1} \end{pmatrix} = \begin{pmatrix} p_i & Nq_i \\ q_i & p_i \end{pmatrix};$$

which entails in particular that $p_i^2 - Nq_i^2 = (-1)^{i+1}Q_{i+1}$. In other words, the Q_{i+1} arise from the convergents as just indicated.

Conversely, one sees that when $x^2 - Ny^2 = t$ with $|t| < \sqrt{N}$ then, if $t > 0$, $|x/y - \sqrt{N}| < 1/2y^2$, whilst if $t < 0$ then $|y/x - 1/\sqrt{N}| < 1/2x^2$. In either case it follows from the remark following (2) that x/y is a convergent to $\sqrt{N}$, whence t is $(-1)^{i+1}Q_{i+1}$, some i.

4. PROOF OF THE THEOREMS.

Proof of Theorem 1. Set $N = rs$. By the definitions of the sequences (P_i) and (Q_i) we have

$$(P_h + \sqrt{N})/Q_h = [\, a_h \,, a_{h+1} \,, a_{h+2} \,, \ldots] = [\, a_h \,, \overline{a_{h+1} \,, \ldots \,, a_l \,, a_1 \,, a_2 \,, \ldots \,, a_h}\,].$$

Let (X, Y) be a positive integer solution to $rX^2 - sY^2 = \pm 1$. Then $(sY)^2 - NX^2 = \mp s$, so because $s < \sqrt{N}$ it follows that sY/X is a convergent to $\sqrt{rs}$, and, more to the point, s is some Q_i for $\sqrt{N}$. Since, trivially, $s \big| N = rs$, we see that the lemma entails that $i = \frac{1}{2}l = h$, whence $sY/X = p_{h-1}/q_{h-1}$.

Here $Q_h = s$ is squarefree by hypothesis and, since now it divides N, the argument given at the lemma entails that $Q_h \big| P_h$. Thus $P_h/Q_h = \frac{1}{2}a_h$ is an integer, and so

$$\sqrt{rs}/Q_h = \sqrt{r/s} = [\, \tfrac{1}{2}a_h \,, \overline{a_{h+1} \,, \ldots \,, a_l \,, a_1 \,, \ldots \,, a_h}\,].$$

Finally, our remark at (1), or, if one prefers, the observation at (4) that the word $a_1a_2\ldots a_{l-1}$ is a palindrome, provides the given formulation of the expansion. ∎

Proof of Theorem 2. We saw above that the data entails $sY/X = p_{h-1}/q_{h-1}$. Thus

$$p_{h-1}^2 - Nq_{h-1}^2 = (-1)^hQ_h \quad \text{is} \quad (sY)^2 - rsX^2 = (-1)^hs,$$

and so

$$sY^2 - rX^2 = (-1)^h,$$

from which the desired conclusions follow. ∎

We now establish the proofs of the corollaries.

Proof of Corollary 1. With $N = pq$ divisible by a prime congruent to 3 modulo 4, it is plain that $U^2 - NV^2 = -1$ has no solution in nonzero integers U, V. Thus the period of $\sqrt{pq}$ has even length $l = 2h$, say. Hence there is a solution in relatively prime integers x, y for $x^2 - pqy^2 = \pm Q_h$ with some Q_h dividing $2pq$, and $1 < Q_h < 2\sqrt{pq}$.

However, it is plain that $x^2 - pqy^2 \equiv 2 \pmod 4$ is impossible so we must have Q_h is one of p or q; say $Q_h = q$. But $x^2 - pqy^2 = \mp q$ implies $x = qY$, $y = X$, giving a solution in integers X, Y to $pX^2 - qY^2 = \pm 1$, satisfying the conditions of Theorem 2. ∎

Proof of Corollary 2. As above, $U^2 - 2pqV^2 = -1$ is impossible in nonzero integers U, V, so there is a solution in relatively prime integers x, y for $x^2 - 2pqy^2 = \pm Q_h$, for some Q_h dividing $4pq$, and $1 < Q_h < 2\sqrt{2pq}$.

It's easy to see that the possibilities modulo 8 are $x^2 - 2pqy^2 = \pm 2p$ or $x^2 - 2pqy^2 = \pm q$ and that either yields integers X, Y satisfying $2pX^2 - qY^2 = \pm 1$. Thus again the hypotheses of Theorem 2 are satisfied, and the result follows by noticing that the Jacobi symbol $\left(\frac{2}{q}\right) = 1$ for $q \equiv 7 \pmod 8$. ∎

5. CLOSING REMARKS.

Suppose we know both that

$$\sqrt{r/s} = [\,\tfrac{1}{2}a_h\,,\,\overline{a_{h+1}\,,\,\ldots\,,\,a_l\,,\,a_1\,,\,\ldots\,,\,a_h}\,] \text{ and } \sqrt{rs} = [\,a_0\,,\,\overline{a_1\,,\,\ldots\,,\,a_h\,,\,a_{h+1}\,,\,\ldots\,,\,a_l}\,].$$

The two expansions have the same 'tail', that is, they differ only in a finite number of initial partial quotients. Thus the numbers $\sqrt{rs}$ and $\sqrt{r/s}$ are *equivalent* and one sees, for example from the matrix correspondence, that there are integers X, Y, U, and V satisfying $VX - UY = \pm 1$ and so that $(U\sqrt{r/s}+B)(X\sqrt{r/s}+Y) = \sqrt{rs}$. But, removing the surd from the denominator yields

$$\frac{(rUX - sVY) + (VX - UY)\sqrt{rs}}{rX^2 - sY^2} = \sqrt{rs}.$$

It follows that $rUX - sVY = 0$ and, this is the point, $rX^2 - sY^2 = \pm 1$. So the shape of the two continued fraction expansions, and first principles, shows that there is a solution in integers X, Y to $rX^2 - sY^2 = \pm 1$.

We might also recall a cute result mentioned by Nagell [4]. Namely, given an integer N, consider the collection of all equations $aX^2 - bY^2 = \pm 1$ with integers a and b so that $ab = N$. Nagell's remark is that at most two of that collection of diophantine equations can have a solution. One of us happened to have been reminded of this fine fact by Dmitri Mit'kin at a meeting at Minsk, Belarus in 1996.

Proof. The cases N less than zero or N a square are uninteresting and trivial, so we suppose that $N > 0$ and is not a square. Then we have at least one equation with a solution, namely $1 \cdot X^2 - NY^2 = 1$. Further, if the length l of the period of $\sqrt{N}$ is odd then also $NX^2 - 1 \cdot Y^2 = 1$ has a solution. If there is some other one of the equations with a solution, say $aX^2 - bY^2 = \pm 1$ with $a > b > 1$, then, as we saw above, $(bY)^2 - NX^2 = \mp b$ so $l = 2h$, $b = Q_h$, and $\mp 1 = (-1)^{h+1}$. Thus there is at most one 'other' equation, and if it has a solution then l is not odd. ∎

REFERENCES

[1] Enrico Bombieri and A. J. van der Poorten, 'Continued fractions of algebraic numbers', in *Computational Algebra and Number Theory, Sydney* 1992, Wieb Bosma and Alf van der Poorten eds., Kluwer 1995, 138–154.

[2] P. Chowla and S. Chowla, 'Problems on periodic simple continued fractions', *Proc. Nat. Acad. Sci. USA* **69** (1972), 37-45.

[3] C. Friesen, 'Legendre Symbols and continued fractions', *Acta Arith.* **59** (1991), 365-379.

[4] T. Nagell, 'On a special class of Diophantine equations of the second degree', *Ark. Mat.* **3** (1954), 51–65.

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

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

Centre for Number Theory Research, Macquarie University, Sydney 2109, Australia
alf@maths.mq.edu.au

University of Ottawa, 585 King Edward St., Ottawa, Ontario, Canada K1N 6N5
gwalsh@mathstat.uottawa.ca