MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 351-354

CONTINUED FRACTIONS AND LINEAR RECURRENCES

H. W. LENSTRA, JR. AND J. O. SHALLIT

Dedicated to the memory of D. H. Lehmer

ABSTRACT. We prove that the numerators and denominators of the convergents to a real irrational number θ satisfy a linear recurrence with constant coefficients if and only if θ is a quadratic irrational. The proof uses the Hadamard Quotient Theorem of A. van der Poorten.

Let θ be an irrational real number with simple continued fraction expansion $[a_0, a_1, a_2, \dots]$. Define the numerators and denominators of the *convergents* to θ as follows:

$$p_{-2} = 0; \quad p_{-1} = 1; \quad p_n = a_n p_{n-1} + p_{n-2} \quad \text{for } n \geq 0; \tag{1}$$

$$q_{-2} = 1; \quad q_{-1} = 0; \quad q_n = a_n q_{n-1} + q_{n-2} \quad \text{for } n \geq 0. \tag{2}$$

By the classical theory of continued fractions (see, for example, [2, Chapter X]), we have

$$\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n].$$

In this note, we consider the question of when the sequences $(p_n)_{n\geq 0}$ and $(q_n)_{n\geq 0}$ can satisfy a linear recurrence with constant coefficients. If, for example, $\theta = \sqrt{3}$, then $\theta = [1, 1, 2, 1, 2, 1, 2, \dots]$, and it is easy to verify that $q_{n+4} = 4q_{n+2} - q_n$ for all $n \geq 0$. Our main result shows that this exemplifies the situation in general.

Theorem 1. *Let θ be an irrational real number. Let its simple continued fraction expansion be $\theta = [a_0, a_1, \dots]$, and let (p_n) and (q_n) be the sequence of numerators and denominators of the convergents to θ, as defined above. Then the following four conditions are equivalent:*

(a) $(p_n)_{n\geq 0}$ *satisfies a linear recurrence with constant complex coefficients;*
(b) $(q_n)_{n\geq 0}$ *satisfies a linear recurrence with constant complex coefficients;*
(c) $(a_n)_{n\geq 0}$ *is an ultimately periodic sequence;*
(d) θ *is a quadratic irrational.*

Received by the editor July 2, 1992 and, in revised form, October 19, 1992.
1991 *Mathematics Subject Classification.* Primary 11A55; Secondary 11B37.
Key words and phrases. Continued fractions; linear recurrences.
The first author is supported by the National Science Foundation under Grant No. DMS-9002939. The hospitality and support of the Institute for Computer Research (Waterloo) are gratefully acknowledged. The second author is supported in part by a grant from NSERC Canada.

Our proof is simple, but uses a deep result of van der Poorten known as the Hadamard Quotient Theorem. We do not know how to give a short proof of the implication (b) $\Longrightarrow$ (c) from first principles.

Proof. The equivalence (c) $\Longleftrightarrow$ (d) is classical. We will prove the equivalence (b) $\Longleftrightarrow$ (c); the equivalence (a) $\Longleftrightarrow$ (c) will follow in a similar fashion.

(c) $\Longrightarrow$ (b): It is easy to see (cf. Frame [1]) that

$$\begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}. \tag{3}$$

Now if the sequence $(a_n)_{n\geq 0}$ is ultimately periodic, then there exists an integer $r \geq 0$, and r integers $b_0, b_1, \dots, b_{r-1}$, and an integer $s \geq 1$ and s positive integers $c_0, c_1, \dots, c_{s-1}$ such that

$$\theta = [b_0, b_1, \dots, b_{r-1}, c_0, c_1, \dots, c_{s-1}, c_0, c_1, \dots, c_{s-1}, \dots].$$

Now for each integer i modulo s, define

$$M_i = \prod_{0\leq j<s} \begin{bmatrix} c_{i+j} & 1 \\ 1 & 0 \end{bmatrix}.$$

Then for all $n \geq r$, we have, by equation (3),

$$\begin{bmatrix} p_{n+s} & p_{n+s-1} \\ q_{n+s} & q_{n+s-1} \end{bmatrix} = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} M_{n-r}. \tag{4}$$

Since for all pairs (i, j) it is possible to find matrices A, B such that $M_i = AB$ and $M_j = BA$, and since $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, it readily follows that $t = \mathrm{Tr}(M_i)$ does not depend on i. Hence the characteristic polynomial of each M_i is $X^2 - tX + (-1)^s$. Since every matrix satisfies its own characteristic polynomial, we see that $M_{n-r}^2 - tM_{n-r} + (-1)^s I$ is the zero matrix. Combining this observation with equation (4), we get

$$\begin{bmatrix} p_{n+2s} & p_{n+2s-1} \\ q_{n+2s} & q_{n+2s-1} \end{bmatrix} - t \begin{bmatrix} p_{n+s} & p_{n+s-1} \\ q_{n+s} & q_{n+s-1} \end{bmatrix} + (-1)^s \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} = 0.$$

Therefore, $q_{n+2s} - tq_{n+s} + (-1)^s q_n = 0$ for all $n \geq r$, and hence the sequence $(q_n)_{n\geq 0}$ satisfies a linear recurrence with constant integral coefficients.

(b) $\Longrightarrow$ (c): The proof proceeds in two stages. First we show, by means of a theorem of van der Poorten, that if $(q_n)_{n\geq 0}$ satisfies a linear recurrence, then so does $(a_n)_{n\geq 0}$. Next we show that the a_n are bounded because otherwise the q_n would grow too rapidly. The periodicity of $(a_n)_{n\geq 0}$ then follows immediately.

Let us recall a familiar definition: if the sequence of complex numbers $(u_n)_{n\geq 0}$ satisfies a linear recurrence with constant complex coefficients

$$u_n = \sum_{1\leq i\leq d} e_i u_{n-i}$$

for all n sufficiently large, and d is chosen to be as small as possible, then $X^d - \sum_{1\leq i\leq d} e_i X^{d-i}$ is said to be the *minimal polynomial* for the linear recurrence. Also recall that a sequence of complex numbers $(u_n)_{n\geq 0}$ satisfies a linear recurrence with constant coefficients if and only if the formal series $\sum_{n\geq 0} u_n X^n$ represents a rational function of X.

Define the two formal series $F = \sum_{n\geq 0}(q_{n+2} - q_n)X^n$ and $G = \sum_{n\geq 0} q_{n+1}X^n$. Clearly F and G represent rational functions. We now use the following theorem of van der Poorten [4, 5, 6]:

Theorem 2 (Hadamard Quotient Theorem). *Let* $F = \sum_{i\geq 0} f_i X^i$ *and* $G = \sum_{i\geq 0} g_i X^i$ *be formal series representing rational functions in* $\mathbf{C}(X)$. *Suppose that the* f_i *and* g_i *are complex numbers such that* $g_i \neq 0$ *and* f_i/g_i *is an integer for all* $i \geq 0$. *Then* $\sum_{i\geq 0}(f_i/g_i)X^i$ *also represents a rational function.*

Since $q_{n+2} = a_{n+2}q_{n+1} + q_n$ for all $n \geq 0$, it follows from this theorem that $\sum_{n\geq 0} a_{n+2}X^n$ represents a rational function, and hence the sequence of partial quotients $(a_n)_{n\geq 0}$ also satisfies a linear recurrence with constant coefficients.

We now require the following lemma:

Lemma 3. *Suppose that* $(y_n)_{n\geq 0}$ *and* $(z_n)_{n\geq 0}$ *are sequences of complex numbers, each satisfying a linear recurrence, with the property that the minimal polynomial of* $(z_n)_{n\geq 0}$ *divides the minimal polynomial of* $(y_n)_{n\geq 0}$. *Let* d *denote the degree of the minimal polynomial of* $(y_n)_{n\geq 0}$. *Then there exist constants* $c > 0$ *and* n_0 *such that for all* $n \geq n_0$ *we have*

$$\max(|y_{n-d+1}|, |y_{n-d+2}|, \ldots, |y_n|) > c|z_n|.$$

Proof. Put $Y = \sum_{n\geq 0} y_n X^n = f/g$ with $\gcd(f, g) = 1$ and $\deg g = d$, and $Z = \sum_{n\geq 0} z_n X^n = h/g$; here $f, g, h \in \mathbf{C}[X]$. Since $\gcd(f, g) = 1$, we can find a polynomial $k = \sum_{0\leq i<d} k_i X^i$ of degree $< d$ such that $kf \equiv h \pmod{g}$. Then $Z = kY + m$, for a polynomial m, and $z_n = \sum_{0\leq i<d} k_i y_{n-i}$ for $n > n_0 = \deg m$. It follows that

$$|z_n| \leq \left(\sum_{0\leq i<d} |k_i|\right) \max(|y_{n-d+1}|, |y_{n-d+2}|, \ldots, |y_n|),$$

and the lemma follows, with $c = (1 + \sum_{0\leq i<d} |k_i|)^{-1}$. □

Since $(a_n)_{n\geq 0}$ satisfies a linear recurrence, we may express a_n as a generalized power sum

$$a_n = \sum_{1\leq i\leq d} A_i(n)\alpha_i^n,$$

for all n sufficiently large. Here the α_i are distinct nonzero complex numbers (the "characteristic roots") and the $A_i(n)$ are polynomials in n.

Now take $y_n = a_n$ and $z_n = n^l\alpha^n$, where $\alpha = \alpha_i$ and $l = \deg A_i$ for some i. Then the hypothesis of Lemma 3 holds, and we conclude that at least one of $a_{n-d+1}, a_{n-d+2}, \ldots, a_n$ is greater than $cn^l|\alpha|^n$, for all n sufficiently large. Then, using equation (2), we have

$$q_{dm} \geq \prod_{1\leq j\leq dm} a_j > c' \cdot c^m \cdot d^{lm} \cdot (m!)^l \cdot (|\alpha|^d)^{m(m+1)/2}$$

for some positive constant c' and all $m \geq 1$. But $(q_n)_{n\geq 0}$ satisfies a linear recurrence, and therefore $\log q_{dm} = O(dm)$. It follows that $|\alpha_i| \leq 1$ for all i, and further that $\deg A_i = 0$ for those i with $|\alpha_i| = 1$. Hence the sequence $(a_n)_{n\geq 0}$ is bounded. But a simple argument using the pigeonhole principle (see, for example, [3, Part VIII, Problem 158]) shows that any bounded integer sequence satisfying a linear recurrence is ultimately periodic. This completes the proof. □

Bibliography

1. J. S. Frame, *Continued fractions and matrices*, Amer. Math. Monthly **56** (1949), 98–103.
2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1989, Fifth edition, reprinting.
3. G. Pólya and G. Szegö, *Problems and theorems in analysis* II, Springer-Verlag, Berlin and New York, 1976.
4. A. J. van der Poorten, *p-adic methods in the study of Taylor coefficients of rational functions*, Bull. Austral. Math. Soc. **29** (1984), 109–117.
5. ———, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris **306** (1988), 97–102.
6. R. Rumely, *Notes on van der Poorten's proof of the Hadamard quotient theorem*: *Parts* I–II, Séminaire de Théorie des Nombres Paris 1986-87 (C. Goldstein, ed.), Progress in Mathematics, vol. 75, Birkhäuser, Boston, 1989, pp. 349–382; 383–409.

Department of Mathematics, University of California, Berkeley, California 94720
E-mail address: hwl@math.berkeley.edu

Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail address: shallit@graceland.uwaterloo.ca