ACTA ARITHMETICA
LXVIII.4 (1994)

On the continued fractions of quadratic surds

by

David G. Cantor (San Diego, Cal.)

1. Introduction. Call a formal Laurent series $\Gamma(X) = \sum_{h=-h_0}^{\infty} \gamma_h/X^h$, with coefficients in a field K, *normal* if its continued fraction is not finite and all of the partial quotients, except perhaps the first, are linear. In [1], Allouche, Mendès France, and van der Poorten show that the formal Laurent series

$$F(X) = \prod_{h=0}^{\infty}(1 + 1/X^{3^h}) \tag{1.1}$$

defined over the field of rational numbers $\mathbb{Q}$ is normal. They do this by noting that, over a field of characteristic 3, $F(X)$ equals $1/\sqrt{1+1/X}$. The latter has a periodic continued fraction and, as a consequence, they are able to explicitly verify that $F(X)$ is normal. They then use an "automatic" proof to show that the Laurent series of $F(X)$, defined over $\mathbb{Q}$, is normal.

Here we shall give a different proof of the latter result (Theorem 4, below) and show, more generally, that if a formal Laurent series $\Gamma(X)$ defined over $\mathbb{Q}$ is defined and normal $(\mathrm{mod}\, p)$ for any prime p, then it is also normal over $\mathbb{Q}$.

We shall also consider the continued fraction of the more general surd $1/\sqrt{1+u/X+v/X^2}$ over any field not of characteristic 2. Put $\delta = u^2/4 - v$ and note that $\sqrt{1+u/X+v/X^2} = 1 + u/(2X)$ when $\delta = 0$. Hence, when $\delta = 0$, the continued fraction expansion is trivial and is not normal. Define

$$\alpha_n = \frac{(u/2 - \sqrt{v})^n + (u/2 + \sqrt{v})^n}{2}, \tag{1.2}$$

so that, in particular,

$$\alpha_0 = 1, \quad \alpha_1 = u/2, \quad \alpha_{n+1} = u\alpha_n - \delta\alpha_{n-1} \quad (n \geq 1). \tag{1.3}$$

1991 *Mathematics Subject Classification*: 14H40, 14H45.
Key words and phrases: continued fractions, surds, automata.
The author would like to thank A. J. van der Poorten for several helpful suggestions.

We will prove

THEOREM 1. *Suppose that K is a field not of characteristic 2, that $u, v \in K$, and that $\delta = u^2/4 - v$ is not 0. Then the continued fraction of $1/\sqrt{1 + u/X + v/X^2}$, defined over the field K, is normal if and only if $\alpha_n \neq 0$ for all $n \geq 1$.*

Before giving the proof we make some comments, give more details concerning the definition of the continued fraction expansion and review the definition of continued fractions over fields of formal Laurent series. As a corollary of the proof we shall obtain explicit formulas for the convergents and partial quotients of the continued fraction of $1/\sqrt{1 + u/X + v/X^2}$.

Of course, the cited theorem is the special case of our theorem over a field of characteristic 3 when $u = 1$ and $v = 0$. In that case, $\delta = 1$ is not 0 and $\alpha_n = (1/2)^{n+1}$ which is never 0. As another example, consider the continued fraction of

$$F_1(X) = 1/\sqrt{1 + 1/X + 1/X^2} \tag{1.4}$$

over the field $\mathbb{Q}$. For this function, $\delta = -3/4$ is not 0 and $2\alpha_n = (-1/2)^n + (3/2)^n$ is never 0. By Theorem 1 the series (1.4) is normal. However, over a field of characteristic 3,

$$F_1(X) = 1/(1 - X)$$

and is certainly not normal.

Our theorem does not apply in characteristic 2. In [8], Mesirov and Sweet consider a related problem over characteristic 2.

Note that if $u = 0$ in Theorem 1, then the partial quotients cannot be linear. Since $\alpha_1 = u$, this condition is included in the statement of the theorem.

2. Background. We use the same continued fraction setup as is used in Artin [2], Baum and Sweet [3, 4], Cantor [5], or France and van der Poorten [7] (note that in [5] the roles of X and $1/X$ are interchanged). We give a brief description of it here. For proofs see these references and the survey paper by Shallit [10].

We work in the field of formal Laurent series of the form

$$\Gamma(X) = \sum_{h=-h_0}^{\infty} \gamma_h / X^h, \tag{2.5}$$

where the $\gamma_h \in K$ and h_0 is an integer. If γ_{-h_0} is not 0 then we say that $\Gamma(X)$ has *degree* h_0. In the special case when $\Gamma(X)$ is a polynomial this agrees with the usual definition of degree. A *continued fraction* is then an

expression of the form

$$c_0(X) + \cfrac{1}{c_1(X) + \cfrac{1}{c_2(X) + \cfrac{1}{\ddots}}},$$

where $c_0(X)$ is a finite formal Laurent series and where, when $i \geq 1$, the $c_i(X)$ are polynomials in X of degree ≥ 1. The $c_i(X)$ are called the *partial quotients* of the continued fraction. We define the *integer part* of the series $\Gamma(X)$, given in (2.5), to be the polynomial

$$[\Gamma(X)] = \sum_{h=-h_0}^{0} \gamma_h X^h. \tag{2.6}$$

The continued fraction algorithm for $\Gamma(X)$ is obtained by putting $\Gamma_0(X) = \Gamma(X)$ and, inductively for $n \geq 0$, putting

$$c_n(X) = [\Gamma_n(X)], \quad \Gamma_{n+1}(X) = 1/(\Gamma_n(X) - c_n(X)). \tag{2.7}$$

The algorithm terminates if, for some n, $\Gamma_n(X) = c_n(X)$. This happens if and only if $\Gamma(X)$ is a rational function.

We define two sequences of polynomials $\{p_n(X) \mid n \geq -2\}$ and $\{q_n(X) \mid n \geq -2\}$ by putting

$$p_{-2}(X) = 0,\ p_{-1}(X) = 1, \quad q_{-2}(X) = 1,\ q_{-1}(X) = 0, \tag{2.8}$$

and, for $n \geq 0$,

$$\begin{aligned} p_n(X) &= c_n(X)p_{n-1}(X) + p_{n-2}(X), \\ q_n(X) &= c_n(X)q_{n-1}(X) + q_{n-2}(X). \end{aligned} \tag{2.9}$$

The pairs $(p_n(X), q_n(X))$ are called *convergents* to the continued fraction. It follows by induction from their definition that

$$p_n(X)q_{n-1}(X) - p_{n-1}(X)q_n(X) = (-1)^{n+1}. \tag{2.10}$$

It is immediate from (2.8) and (2.9) that when $n \geq 1$, then

$$\deg q_n(X) = \sum_{i=1}^{n} \deg c_i(X). \tag{2.11}$$

It is easy to verify that

$$\Gamma_n(X) = -\frac{p_{n-1}(X) - q_{n-1}(X)\Gamma(X)}{p_{n-2}(X) - q_{n-2}(X)\Gamma(X)}$$

and hence that

$$c_n(X) = \left[-\frac{p_{n-1}(X) - q_{n-1}(X)\Gamma(X)}{p_{n-2}(X) - q_{n-2}(X)\Gamma(X)} \right]. \tag{2.12}$$

From (2.7) and (2.12) we obtain the basic approximation property of the convergents which is

$$\deg(p_n(X) - q_n(X)\Gamma(X)) = -\deg c_{n+1}(X) - \deg q_n(X) < -\deg q_n(X). \tag{2.13}$$

The uniqueness of these convergents is the statement that if $p(X)$ and $q(X)$ are relatively prime polynomials such that

$$\deg(p(X) - q(X)\Gamma(X)) < -\deg q(X), \tag{2.14}$$

then there exists an integer n and a constant λ such that $p(X) = \lambda p_n(X)$ and $q(X) = \lambda q_n(X)$. By (2.13), $c_{n+1}(X)$ has degree 1 if and only if

$$\deg(p_n(X) - q_n(X)\Gamma(X)) = -1 - \deg q_n(X). \tag{2.15}$$

It will be convenient to let $[1/X^h]$ denote an unspecified formal Laurent series of degree $\le -h$ (there will be no confusion between this definition and the definition of $[\Gamma(X)]$ in (2.6)). As stated at the beginning, we shall call a formal Laurent series $\Gamma(X) = \sum_{h=-h_0}^{\infty} \gamma_h X^h$ normal if its continued fraction is infinite (equivalently, $\Gamma(X)$ is not a rational function) and all, except perhaps the first, of the partial quotients of its continued fraction are linear. It follows from (2.11) that this is equivalent to the statement that for all $n \ge 1$, the denominator $q_n(X)$ of the nth convergent to $\Gamma(X)$ has degree n. We obtain the following remark from (2.13) and the sentence preceding (2.15):

Remark 2.16. A continued fraction is normal if and only if, for all $n \ge 0$, the "error term" $p_n(X) - q_n(X)\Gamma(X)$ has the form $d_n/X^{n+1} + [1/X^{n+2}]$ with $d_n \ne 0$.

3. Main results. In this section we give the proof of Theorem 1 and the statement and proof of the other theorems of this paper.

Proof of Theorem 1. Define

$$\begin{aligned} C(X) &= (X + u/2) - \sqrt{X^2 + uX + v}, \\ \overline{C}(X) &= (X + u/2) + \sqrt{X^2 + uX + v}, \end{aligned} \tag{3.17}$$

where $\sqrt{X^2 + uX + v}$ denotes the formal Laurent series

$$X(1 + u/X + v/X^2)^{1/2} = X \sum_{n=0}^{\infty} \binom{1/2}{n} (u/X + v/X^2)^n. \tag{3.18}$$

Then

$$C(X)\overline{C}(X) = (X + u/2)^2 - (X^2 + uX + v) = u^2/4 - v = \delta. \tag{3.19}$$

Substituting the expansion (3.18) in the definition of $\overline{C}(X)$ shows that

$$\overline{C}(X) = 2X + u + [1/X]. \tag{3.20}$$

It follows that

$$C(X)^n = \frac{\delta^n}{\overline{C}(X)^n} = \frac{(\delta/2)^n}{X^n} + \left[\frac{1}{X^{n+1}}\right]. \tag{3.21}$$

Expanding $C(X)$, as given in (3.17), by the binomial theorem, we obtain, when $n \geq 0$,

$$\begin{aligned} C(X)^n &= \sum_{k=0}^{n} \binom{n}{k} (-1)^k (X + u/2)^{n-k} (X^2 + uX + v)^{k/2} \\ &= A_n(X) - B_n(X)\sqrt{X^2 + uX + v}, \end{aligned} \tag{3.22}$$

where

$$\begin{aligned} A_n(X) &= \frac{\overline{C}(X)^n + C(X)^n}{2} \\ &= \sum_{k \text{ even}} \binom{n}{k} (X + u/2)^{n-k} (X^2 + uX + v)^{k/2} \end{aligned} \tag{3.23}$$

and

$$\begin{aligned} B_n(X) &= \frac{\overline{C}(X)^n - C(X)^n}{2\sqrt{X^2 + uX + v}} \\ &= \sum_{k \text{ odd}} \binom{n}{k} (X + u/2)^{n-k} (X^2 + uX + v)^{(k-1)/2} \end{aligned} \tag{3.24}$$

are polynomials in X. In particular,

$$\begin{aligned} A_0(X) &= 1, & B_0(X) &= 0, \\ A_1(X) &= X + u/2, & B_1(X) &= 1, \\ A_2(X) &= 2X^2 + 2uX + u^2/4 + v, & B_2(X) &= 2X + u. \end{aligned} \tag{3.25}$$

It is clear that $A_n(X)$ is a polynomial of degree n whose leading coefficient, when $n \geq 1$, is 2^{n-1}, and that, when $n \geq 1$, $B_n(X)$ is a polynomial of degree $n-1$ with leading coefficient 2^{n-1}. We can obtain $A_n(0)$ and $B_n(0)$ by substituting $X = 0$ in (3.23) and (3.24). We find that

$$A_n(0) = \frac{(u/2 - \sqrt{v})^n + (u/2 + \sqrt{v})^n}{2} = \alpha_n$$

and that

$$B_n(0) = \begin{cases} \dfrac{(u/2 - \sqrt{v})^n - (u/2 + \sqrt{v})^n}{2\sqrt{v}} & \text{when } v \neq 0, \\ n(u/2)^{n-1} & \text{when } v = 0. \end{cases}$$

Now define

$$
\begin{aligned}
Q_n(X) &= \frac{1}{X}\det\begin{pmatrix} \alpha_n & \alpha_{n+1} \\ A_n(X) & A_{n+1}(X)\end{pmatrix},\\
P_n(X) &= \det\begin{pmatrix} \alpha_n & \alpha_{n+1} \\ B_n(X) & B_{n+1}(X)\end{pmatrix}.
\end{aligned}
\tag{3.26}
$$

Then $P_n(X)$ and $Q_n(X)$ are both polynomials of degree $\le n$. In particular, by (3.25),

$$
\begin{aligned}
&P_0(X) = 1, && Q_0(X) = 1,\\
&P_1(X) = uX + u^2/4 - v, && Q_1(X) = uX + 3u^2/4 - v.
\end{aligned}
\tag{3.27}
$$

The coefficient of X^n is the same in both $P_n(X)$ and $Q_n(X)$ and equals $2^n\alpha_n$. Substituting $X = 0$ in the definition of $P_n(X)$ shows that if $v \neq 0$, then

$$
\begin{aligned}
&4\sqrt{v}P_n(0)\\
&\quad= \det\begin{pmatrix} (u/2-\sqrt{v})^n + (u/2+\sqrt{v})^n & (u/2-\sqrt{v})^{n+1} + (u/2+\sqrt{v})^{n+1} \\ (u/2-\sqrt{v})^n - (u/2+\sqrt{v})^n & (u/2-\sqrt{v})^{n+1} - (u/2+\sqrt{v})^{n+1}\end{pmatrix}\\
&\quad= \det\begin{pmatrix} 1 & 1 \\ 1 & -1\end{pmatrix}\cdot\det\begin{pmatrix} (u/2-\sqrt{v})^n & (u/2-\sqrt{v})^{n+1} \\ (u/2+\sqrt{v})^n & (u/2+\sqrt{v})^{n+1}\end{pmatrix}\\
&\quad= -2(u/2-\sqrt{v})^n(u/2+\sqrt{v})^n\det\begin{pmatrix} 1 & u/2-\sqrt{v} \\ 1 & u/2+\sqrt{v}\end{pmatrix} = -4\delta^n\sqrt{v},
\end{aligned}
$$

so that

$$
P_n(0) = -\delta^n. \tag{3.28}
$$

It is easy to verify that this is also true when $v = 0$, so that, in particular, $P_n(0)$ is never 0. Next, using (3.21), (3.22), and (3.26), we obtain

$$
\begin{aligned}
XQ_n(X) - P_n(X)\sqrt{X^2+uX+v} &= \det\begin{pmatrix} \alpha_n & \alpha_{n+1} \\ C(X)^n & C(X)^{n+1}\end{pmatrix}\\
&= \alpha_n C(X)^{n+1} - \alpha_{n+1}C(X)^n\\
&= -\frac{(\delta/2)^n\alpha_{n+1}}{X^n} + \left[\frac{1}{X^{n+1}}\right].
\end{aligned}
$$

Thus, dividing by X yields

$$
Q_n(X) - P_n(X)\sqrt{1+u/X+v/X^2} = \frac{-(\delta/2)^n\alpha_{n+1}}{X^{n+1}} + \left[\frac{1}{X^{n+2}}\right]
$$

or, equivalently,

$$
P_n(X) - Q_n(X)/\sqrt{1+u/X+v/X^2} = \frac{(\delta/2)^n\alpha_{n+1}}{X^{n+1}} + \left[\frac{1}{X^{n+2}}\right]. \tag{3.29}
$$

Thus the fraction $P_n(X)/Q_n(X)$ is a convergent to the continued fraction of $1/\sqrt{1+u/X+v/X^2}$. It is now immediate from (3.29) and Remark 2.16 that $1/\sqrt{1+u/X+v/X^2}$ is normal, in the sense defined above, if and only if $\alpha_n \neq 0$ for all $n \geq 1$. ∎

We have proved somewhat more than stated. In fact, we have

COROLLARY. *If $\delta = u^2/4 - v$ is not 0, then the sequence of fractions $\{P_n(X)/Q_n(X) \mid \alpha_n \neq 0\}$ is the sequence of convergents to the continued fraction of $1/\sqrt{1+u/X+v/X^2}$.*

Proof. By the above proof, this is a sequence of distinct convergents to $1/\sqrt{1+u/X+v/X^2}$. We must show that it includes all convergents. By (1.3) no two successive α_n can be 0. The leading coefficient of both $P_n(X)$ and $Q_n(X)$ is $2^n\alpha_n$. Hence, when $\alpha_n = 0$, then the degree of both $P_n(X)$ and $Q_n(X)$ is $\leq n-1$. Since $P_{n-1}(X)$ and $Q_{n-1}(X)$ both have degree $n-1$ and are convergents, it must be that

$$P_n(X)/Q_n(X) = P_{n-1}(X)/Q_{n-1}(X)$$

and this convergent is in the sequence defined in the statement of this corollary. ∎

THEOREM 2. *Using the notation of the proof of Theorem 1 and still assuming that K is a field whose characteristic is not 2 we have, for all $n \geq 1$,*

$$\begin{aligned} \alpha_{n-1}^2 P_n(X) &= (2\alpha_{n-1}\alpha_n X + \alpha_{n-1}^2\delta + \alpha_n^2)P_{n-1}(X) - \alpha_n^2\delta P_{n-2}(X), \\ \alpha_{n-1}^2 Q_n(X) &= (2\alpha_{n-1}\alpha_n X + \alpha_{n-1}^2\delta + \alpha_n^2)Q_{n-1}(X) - \alpha_n^2\delta Q_{n-2}(X). \end{aligned} \tag{3.30}$$

Proof. The element δ, the elements α_n, the coefficients of the $P_n(X)$ and of the $Q_n(X)$ are all polynomials with rational coefficients in u and v. The denominators of the rational coefficients (when expressed in lowest form) are powers of 2 only. Thus the statement of this theorem amounts to certain formal identities between polynomials with rational coefficients in u and v. It therefore suffices to prove this when the ground field has characteristic 0. We shall prove it when the ground field is $\mathbb{Q}$. If $\delta \neq 0$, $v > 0$ and $u > 2\sqrt{v}$, then by (1.2) all of the α_n are non-zero. In that case, by Theorem 1, $p_i(X)/q_i(X) = P_i(X)/Q_i(X)$, for all $i \geq 0$. Under these assumptions it follows from (2.9) that recurrences of the form

$$\begin{aligned} P_n(X) &= (U_n X + V_n)P_{n-1}(X) + W_n P_{n-2}(X), \\ Q_n(X) &= (U_n X + V_n)Q_{n-1}(X) + W_n Q_{n-2}(X), \end{aligned} \tag{3.31}$$

where the U_n, V_n, W_n are elements of K, exist. We need three conditions to determine U_n, V_n, W_n. These will be obtained by examining (1) the coefficient of X^n in either of the recurrences (3.31), (2) the constant term

in the first such recurrence, and (3) the coefficient of $1/X^{n-1}$ in the derived recurrence,

$$\begin{aligned} P_n(X) - Q_n(X)/\sqrt{1+u/X+v/X^2} \\ = (U_nX+V_n)(P_{n-1}(X) - Q_{n-1}(X)/\sqrt{1+u/X+v/X^2}) \\ + W_n(P_{n-2}(X) - Q_{n-2}(X)/\sqrt{1+u/X+v/X^2}). \end{aligned}$$

The first condition yields $2^n\alpha_n = 2^{n-1}\alpha_{n-1}U_n$ or

$$U_n = 2\frac{\alpha_n}{\alpha_{n-1}}.$$

By (3.29), the third condition yields $U_n\alpha_n(\delta/2)^{n-1} + W_n\alpha_{n-1}(\delta/2)^{n-2} = 0$, or

$$W_n = -\frac{\alpha_n\delta U_n}{2\alpha_{n-1}} = -\delta\frac{\alpha_n^2}{\alpha_{n-1}^2}. \tag{3.32}$$

Using (3.28), the second condition yields $\delta^n = V_n\delta^{n-1} + W_n\delta^{n-2}$ or

$$V_n = \delta - W_n/\delta = \delta + \alpha_n^2/\alpha_{n-1}^2.$$

Simplifying yields the formula in the statement of the theorem.

Since, as stated above, δ, the α_n, all of the coefficients of P_n, and all of the coefficients of Q_n are polynomials in u and v with rational coefficients, with only powers of 2 in the denominator, the statement of this theorem amounts to certain polynomial relations between u and v. Since these hold for infinitely many u, and for each such u, for infinitely many v, they are formal identities holding for all u and v, valid over any field not of characteristic 2. ∎

An alternative proof of Theorem 2 can be obtained by defining

$$R_n(X) = XQ_n(X) - P_n(X)\sqrt{X^2+uX+v} = \det\begin{pmatrix} \alpha_n & \alpha_{n+1} \\ C(X)^n & C(X)^{n+1} \end{pmatrix}$$

and then showing directly that, for all $n \geq 1$,

$$\alpha_{n-1}^2R_n(X) - (2\alpha_{n-1}\alpha_nX + \alpha_{n-1}^2\delta + \alpha_n^2)R_n(X) + \alpha_n^2\delta R_{n-1}(X) = 0. \tag{3.33}$$

To do this we note that the left-hand side of (3.33) is divisible by $C(X)^{n-1}$ and, after dividing by it, we are left with the expression

$$\begin{aligned} \alpha_{n-1}^2(\alpha_nC(X)^3 - \alpha_{n+1}C(X)^2) \\ - (2\alpha_{n-1}\alpha_nX + \alpha_{n-1}^2\delta + \alpha_n^2)(\alpha_{n-1}C(X)^2 - \alpha_{n+1}C(X)) \\ + \alpha_n^2\delta(\alpha_{n-2}C(X) - \alpha_{n-1}), \end{aligned}$$

which, with some difficulty, can be directly verified to be identically 0.

We now derive the partial quotients of the continued fraction of $1/\sqrt{1+u/X+v/X^2}$. To this purpose define, for $n \geq 0$,

$$\lambda_n = \begin{cases} (-\delta)^m \prod_{j=1}^{m} (\alpha_{2j}/\alpha_{2j-1})^2 & \text{if } n \text{ is even and } n = 2m, \\ -2(-\delta)^m / \prod_{j=0}^{m} (\alpha_{2j+1}/\alpha_{2j})^2 & \text{if } n \text{ is odd and } n = 2m+1. \end{cases}$$

Note that when $n \geq 2$,

$$\lambda_n/\lambda_{n-2} = -\delta\alpha_n^2/\alpha_{n-1}^2, \quad \lambda_n\lambda_{n-1} = -2(-\delta)^{n-1}\alpha_n^2. \tag{3.34}$$

Further, define

$$c_0(X) = 1, \quad c_1(X) = -2X/u + 2v/u^2 - 3/2,$$

and for $n \geq 2$, define

$$\begin{aligned} c_n(X) &= \frac{\lambda_{n-1}(2\alpha_{n-1}\alpha_n X + \alpha_{n-1}^2\delta + \alpha_n^2)}{\lambda_n \alpha_{n-1}^2} \\ &= \frac{\lambda_{n-1}}{\lambda_n}\left(2\frac{\alpha_n}{\alpha_{n-1}}X + \delta + \left(\frac{\alpha_n}{\alpha_{n-1}}\right)^2\right). \end{aligned}$$

Then we have

THEOREM 3. *Suppose all α_n are non-zero. Then the partial quotients of the continued fraction of $1/\sqrt{1+u/X+v/X^2}$ are the $c_n(X)$. For $n \geq 0$, the convergents are given by $p_n(X) = P_n(X)/\lambda_n$ and $q_n(X) = Q_n(X)/\lambda_n$.*

Proof. Clearly $p_n(X)/q_n(X) = P_n(X)/Q_n(X)$. It therefore suffices to show that $p_n(X)$ and $q_n(X)$ satisfy the recurrences of the shape of (2.9) when $n \geq 0$. Since $p_0(X) = q_0(X) = c_0(X) = 1$, (2.9) holds when $n = 0$. When $n = 1$ then $\lambda_1 = -2\alpha_1^2/\alpha_0^2 = -u^2/2$ so that, by (3.27),

$$p_1(X) = P_1(X)/\lambda_1 = (uX + u^2/4 - v)/(-u^2/2) = -2X/u + 2v/u^2 - 1/2,$$
$$q_1(X) = Q_1(X)/\lambda_1 = (uX + 3u^2/4 - v)/(-u^2/2) = -2X/u + 2v/u^2 - 3/2.$$

Thus $p_1(X) = 1 + c_1(X)$ and $q_1(X) = c_1(X)$, as required. When $n \geq 2$, we have, by Theorem 2,

$$\alpha_{n-1}^2\lambda_n p_n(X) = (2\alpha_{n-1}\alpha_n X + \alpha_{n-1}^2\delta + \alpha_n^2)\lambda_{n-1}p_{n-1}(X) - \alpha_n^2\delta\lambda_{n-2}p_{n-2}(X).$$

Hence, using (3.34),

$$\begin{aligned} p_n(X) &= (2\alpha_{n-1}\alpha_n X + \alpha_{n-1}^2\delta + \alpha_n^2)\frac{\lambda_{n-1}}{\alpha_{n-1}^2\lambda_n}p_{n-1}(X) - \frac{\alpha_n^2\delta\lambda_{n-2}}{\alpha_{n-1}^2\lambda_n}p_{n-2}(X) \\ &= c_n(X)p_{n-1}(X) + p_{n-2}(X). \end{aligned}$$

Similarly, $q_n(X) = c_n(X)q_{n-1}(X) + q_{n-2}(X)$. ∎

THEOREM 4. *Suppose that the formal Laurent series $\Gamma(X)$ is defined over $\mathbb{Q}$ and suppose further that for some prime p, $\Gamma(X)$ is defined and normal when read* (mod p). *Then $\Gamma(X)$ is normal over $\mathbb{Q}$.*

P r o o f. We denote the partial quotients and convergents to the continued fraction of $\Gamma(X)$ in characteristic 0 by $c_n(X)$, $p_n(X)$, and $q_n(X)$, respectively. We denote the corresponding quantities for the continued fraction in characteristic p by $\overline{c}_n(X)$, $\overline{p}_n(X)$, and $\overline{q}_n(X)$, respectively. We shall also write $\overline{\Gamma}(X)$ for the formal Laurent series $\Gamma(X)$ when read $(\mathrm{mod}\, p)$. Put $\varepsilon_n(X) = p_n(X) - q_n(X)\Gamma(X)$ and $\overline{\varepsilon}_n(X) = \overline{p}_n(X) - \overline{q}_n(X)\overline{\Gamma}(X)$. The barred quantities $\overline{c}_n(X)$, $\overline{p}_n(X)$, $\overline{q}_n(X)$, and $\overline{\varepsilon}_n(X)$ are obtained by applying the algorithm described in (2.7), (2.8), and (2.9) to $\overline{\Gamma}(X)$ working $(\mathrm{mod}\, p)$, and by the definition in the preceding sentence. They are *not* obtained by reducing the corresponding unbarred quantities $c_n(X)$, $p_n(X)$, $q_n(X)$, and $\varepsilon_n(X) \pmod p$. Thus (3.35) below is not simply a restatement of the definition of the barred quantities. We shall show by induction that, under the hypotheses of this theorem, the barred quantities are congruent to the corresponding unbarred quantities $(\mathrm{mod}\, p)$. That is,

$$\begin{aligned} &p_n(X) \equiv \overline{p}_n(X) \pmod p, \quad && q_n(X) \equiv \overline{q}_n(X) \pmod p, \\ &c_n(X) \equiv \overline{c}_n(X) \pmod p, \quad && \varepsilon_n(X) \equiv \overline{\varepsilon}_n(X) \pmod p, \end{aligned} \tag{3.35}$$

and

$$\deg c_n(X) = \deg \overline{c}_n(X) = 1, \quad \deg \varepsilon_n(X) = \deg \overline{\varepsilon}_n(X) = -n - 1. \tag{3.36}$$

By the definitions of the quantities involved, (3.35) and (3.36) are true for $n \le 0$. Suppose, inductively, that we have proved them for $n < N$. By (2.12), $c_N(X) = [-\varepsilon_{N-1}(X)/\varepsilon_{N-2}(X)]$ and $\overline{c}_N(X) = [-\overline{\varepsilon}_{N-1}(X)/\overline{\varepsilon}_{N-2}(X)]$. It is immediate that $c_N(X) \equiv \overline{c}_N(X) \pmod p$ and that $\deg c_N(X) = \deg \overline{c}_N(X) = 1$. By (2.9), equation (3.35) holds for $n = N$. By Remark 2.16, $\deg \varepsilon_n(X) = -n - 1$ and now (3.36) follows from (3.35). ∎

References

[1] J.-P. Allouche, M. Mendès France and A. J. van der Poorten, *An infinite product with bounded partial quotients*, Acta Arith. 59 (1991), 171–182.

[2] E. Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen I, II*, in: The Collected Papers of Emil Artin, Addison-Wesley, 1965 (originally published in Math. Z. 19 (1924), 153–246).

[3] L. E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic* 2, Ann. of Math. 103 (1976), 593–610.

[4] —, —, *Badly approximable power series in characteristic* 2, ibid. 105 (1977), 573–580.

[5] D. G. Cantor, *Investigations of T-numbers and E-sequences*, in: Computers in Number Theory, A. O. L. Atkin and B. J. Birch (eds.), Academic Press, 1971, 137–140.

[6] —, *On the analogue of the division polynomials for hyperelliptic curves*, J. Reine Angew. Math. 447 (1994), 91–145.

[7] M. Mendès France and A. J. van der Poorten, *Some explicit continued fraction expansions*, Mathematika 38 (1991), 1–9.

[8] J. P. Mesirov and M. M. Sweet, *Continued fraction expansions of rational expressions with irreducible denominators in characteristic* 2, J. Number Theory 27 (1987), 144–148.

[9] W. H. Mills and D. P. Robbins, *Continued fractions for certain algebraic power series*, ibid. 23 (1986), 388–404.

[10] J. Shallit, *Real numbers with bounded partial quotients: A survey*, Enseign. Math. 38 (1992), 151–187.

[11] A. J. van der Poorten, *Fractions of the period of the continued fraction expansion of quadratic integers*, Bull. Austral. Math. Soc. 44 (1991), 155–169.

[12] A. J. van der Poorten and J. Shallit, *Folded continued fractions*, J. Number Theory 40 (1992), 237–250.

CENTER FOR COMMUNICATIONS RESEARCH
4320 WESTERRA COURT
SAN DIEGO, CALIFORNIA 92121
U.S.A.
E-mail: DGC@MATH.UCLA.EDU

Received on 20.4.1993
and in revised form on 31.1.1994 (2417)