Finite Fields and Their Applications 18 (2012) 26–34

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the continued fraction expansion of the unique root in $\mathbb{F}(p)$ of the equation $x^4 + x^2 - Tx - 1/12 = 0$ and other related hyperquadratic expansions

A. Lasjaunias

Institut de Mathématiques de Bordeaux – CNRS UMR 5251, Université Bordeaux 1, 351 Cours de la Libération, F-33405 Talence Cedex, France

ARTICLE INFO

Article history:
Received 29 September 2010
Revised 1 June 2011
Accepted 3 June 2011
Available online 12 June 2011
Communicated by Arne Winterhof

MSC:
11J70
11T55

Keywords:
Continued fractions
Fields of power series
Finite fields

ABSTRACT

In 1986, Mills and Robbins observed by computer the continued fraction expansion of certain algebraic power series over a finite field. Incidentally, they came across a particular equation of degree four in characteristic $p = 13$. This equation has an analogue for all primes $p \geqslant 5$. There are two patterns for the continued fraction of the solution of this equation, according to the residue of p modulo 3. We describe this pattern in the first case. In the second case we only give indications.

1. Introduction

Throughout this note p is an odd prime number, $\mathbb{F}_p$ is the finite field with p elements and $\mathbb{F}(p)$ denotes the field of power series in $1/T$ with coefficients in $\mathbb{F}_p$, where T is an indeterminate. These fields of power series are known to be analogues of the field of real numbers. A non-zero element of $\mathbb{F}(p)$ is represented by a power series expansion

$$\alpha = \sum_{k \leqslant k_0} u_k T^k \quad \text{where } k_0 \in \mathbb{Z},\ u_k \in \mathbb{F}_p \text{ and } u_{k_0} \neq 0.$$

E-mail address: Alain.Lasjaunias@math.u-bordeaux1.fr.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.06.001

We define $|\alpha| = |T|^{k_0}$ where $|T| > 1$ is a fixed real number. The field $\mathbb{F}(p)$ is the completion of the field $\mathbb{F}_p(T)$, of rational elements, for this absolute value. We will also denote by $\mathbb{F}(p)^+$ the subset of power series α with $|\alpha| \geqslant |T|$.

Like in the case of real numbers, we recall that each irrational element $\alpha \in \mathbb{F}(p)^+$ can be expanded in an infinite continued fraction

$$\alpha = [a_1, a_2, \ldots, a_n, \ldots] \quad \text{where } a_i \in \mathbb{F}_p[T] \text{ and } \deg(a_i) > 0 \text{ for } i \geqslant 1.$$

The polynomials a_i are called the partial quotients of the expansion. For $n \geqslant 1$, we denote $\alpha_{n+1} = [a_{n+1}, a_{n+2}, \ldots]$, called the complete quotient, and we have

$$\alpha = [a_1, a_2, \ldots, a_n, \alpha_{n+1}] = f_n(\alpha_{n+1})$$

where f_n is a fractional linear transformation with coefficients in $\mathbb{F}_p[T]$. Indeed, for $n \geqslant 1$, we have $f_n(x) = (x_n x + x_{n-1})/(y_n x + y_{n-1})$, where the sequences of polynomials $(x_n)_{n\geqslant 0}$ and $(y_n)_{n\geqslant 0}$ are both defined by the same recursive relation: $K_n = a_n K_{n-1} + K_{n-2}$ for $n \geqslant 2$, with the initial conditions $x_0 = 1$ and $x_1 = a_1$ or $y_0 = 0$ and $y_1 = 1$. Moreover, for $n \geqslant 1$, we have $x_n/y_n = [a_1, \ldots, a_n]$ and also $x_n y_{n-1} - x_{n-1} y_n = (-1)^n$. In the definition of x_n or y_n, appear polynomials in several variables which are the partial quotients. These polynomials, $K(u_1, u_2, \ldots, u_n)$, called continuants, will simply be denoted by $\langle u_1, u_2, \ldots, u_n\rangle$. With this notation, we write $x_n = \langle a_1, a_2, \ldots, a_n\rangle$ and $y_n = \langle a_2, a_3, \ldots, a_n\rangle$. For more information on continuants, the reader may consult [8] or the introduction of [3].

We are interested in describing the sequence of partial quotients for certain algebraic power series over $\mathbb{F}_p(T)$. In the real case, an explicit description of the sequence of partial quotients for algebraic numbers is only known for quadratic elements. We will see that in the power series case over a finite field, such a description is possible for many elements belonging to a large class of algebraic power series containing the quadratic ones. Our study is based on a particularly simple algebraic equation of degree 4.

Let p be a prime number with $p \geqslant 5$. Let us consider the following quartic equation with coefficients in $\mathbb{F}_p(T)$:

$$x^4 + x^2 - Tx - 1/12 = 0. \qquad (Eq.1)$$

It is easy to see that $(Eq.1)$ has a unique root in $\mathbb{F}(p)$. We denote it by u and we have $u = -1/(12T) + 1/(12^2T^3) + \cdots$. We put $\alpha = 1/u$ and we consider the continued fraction expansion of α in $\mathbb{F}(p)^+$. We have

$$\alpha = [a_1, a_2, \ldots, a_n, \ldots] \quad \text{with } a_1 = -12T.$$

A simple and general fact about this continued fraction expansion can be observed. The root of $(Eq.1)$ is an odd function of T, since $-u(-T)$ is also solution, and consequently all partial quotients are odd polynomials in $\mathbb{F}_p[T]$.

This quartic equation $(Eq.1)$ appeared for the first time in [6]. There the authors considered the case $p = 13$, hence $-1/12 = 1$. A partial conjecture on the continued fraction for the solution of $(Eq.1)$ in $\mathbb{F}(13)$, observed by computer, was given in [6] and later this conjecture was improved in [2]. The proof of this conjecture was given in [4].

The origin of the generalization for arbitrary $p \geqslant 5$, changing 1 into $-1/12$, is to be found in [1]. If the continued fraction for the root of $(Eq.1)$ is peculiar and can be explicitly described, this is due to the following result [1, Theorem 3.1, p. 263].

Let $p \geqslant 5$ be a prime number and $P(X) = X^4 + X^2 - TX - 1/12 \in \mathbb{F}_p(T)[X]$. Then P divides a nontrivial polynomial $AX^{r+1} + BX^r + CX + D$ where $(A, B, C, D) \in (\mathbb{F}_p[T])^4$ and where

$$r = p \quad \text{if } p = 1 \mod 3 \quad \text{and} \quad r = p^2 \quad \text{if } p = 2 \mod 3.$$

An irrational element $\alpha \in \mathbb{F}(p)$ is called hyperquadratic if it satisfies an algebraic equation of the form $A\alpha^{r+1} + B\alpha^r + C\alpha + D = 0$, where A, B, C and D are in $\mathbb{F}_p[T]$ and r is a power of p. The continued fraction expansion for many hyperquadratic elements can be explicitly described. The reader may consult [9] for various examples and also more references.

According to the result stated above, the solution in $\mathbb{F}(p)$ of $(Eq.1)$ is hyperquadratic. It appears that there are two different structures for the pattern of the continued fraction expansion of this solution, corresponding to both cases: p congruent to 1 or 2 modulo 3. In the second section, we describe a large family of hyperquadratic continued fractions, and we show how some of them can be explicitly described. In the third section if $p = 1 \mod 3$, we show that the solution of $(Eq.1)$, up to a transformation, belongs to the previous family and this allows us to obtain an explicit description of its expansion. In the second case, $p = 2 \mod 3$, we will only give indications which might lead to an explicit description of the continued fraction. In the last section, we make a remark on programming which is based on a result established by Mkaouar [7].

2. Continued fraction expansions of type (p, l, k)

In this section p is an odd prime number and k an integer with $1 \leqslant k < p/2$. We introduce a pair of polynomials which play a fundamental role in the expression of the continued fraction of the solution of $(Eq.1)$ and of many other hyperquadratic power series. These polynomials in $\mathbb{F}_p[T]$ are defined by

$$P_k(T) = \left(T^2 - 1\right)^k \quad \text{and} \quad Q_k(T) = \int_0^T P_{k-1}(x)\,dx.$$

We have $Q_1(T) = T$. Note that the definition of Q_k, for $k > 1$, is made possible by the condition $2k < p$: by formal integration an antiderivative of T^n in $\mathbb{F}_p[T]$ is $T^{n+1}/(n+1)$ if p does not divide $n+1$.

Further we introduce a sequence of polynomials in $\mathbb{F}_p[T]$, based on the polynomial P_k. For a fixed k with $1 \leqslant k < p/2$, we set

$$A_{0,k} = T \quad \text{and} \quad A_{i+1,k} = \left[A_{i,k}^p / P_k\right] \quad \text{for } i \geqslant 0.$$

Here the brackets denote the integral (i.e. polynomial) part of the rational function. We observe that the polynomials $A_{i,k}$ are odd polynomials in $\mathbb{F}_p[T]$. Moreover, it is important to notice that in the extremal case, if $k = (p-1)/2$ then $A_{i,k} = T$ for $i \geqslant 0$.

In [3] (see p. 333 and p. 342), we showed the existence of continued fractions in $\mathbb{F}(p)^+$ generated by the pair (P_k, Q_k). To be more precise we state the following definition.

Definition 2.1. Let $l \geqslant 1$ and $1 \leqslant k < p/2$. A continued fraction expansion $\alpha = [a_1, a_2, \ldots, a_n, \ldots] \in \mathbb{F}(p)$ is of type (p, l, k) if there are an l-tuple $(i(1), \ldots, i(l)) \in \mathbb{N}^l$ and an $(l+2)$-tuple $(\lambda_1, \ldots, \lambda_l, \epsilon_1, \epsilon_2) \in (\mathbb{F}_p^*)^{l+2}$ such that

$$a_j = \lambda_j A_{i(j),k} \quad \text{for } 1 \leqslant j \leqslant l \quad \text{and} \quad \alpha^p = \epsilon_1 P_k \alpha_{l+1} + \epsilon_2 Q_k.$$

Note that all power series defined by a continued fraction of type (p,l,k) are hyperquadratic and they satisfy an algebraic equation of degree less than or equal to $p+1$ (see [3, Theorem 1, p. 332]).

For certain expansions of type (p,l,k), we observed that all the partial quotients, obtained by computer, belong to the sequence $(A_{i,k})_{i\geqslant 1}$ up to a multiplicative constant in $\mathbb{F}_p^*$. In general the partial quotients are proportional to $A_{i,k}$ only up to a certain rank depending on the choice of the $(l+2)$-tuple $(\lambda_1,\ldots,\lambda_l,\epsilon_1,\epsilon_2)\in(\mathbb{F}_p^*)^{l+2}$ (see [3, Proposition 4.6, p. 347]). Consequently, we will introduce another definition. First we define a sequence $(i(n))_{n\geqslant 1}$ based on (l,k). Given $(l,k)\in(\mathbb{N}^*)^2$, we define the sequence of integers $(f(n))_{n\geqslant 1}$ by $f(n)=(2k+1)n+l-2k$. Then the sequence of integers $(i(n))_{n\geqslant 1}$ is defined in the following way:

$$\big(i(1),\ldots,i(l)\big)\in\mathbb{N}^l \text{ is given,}\quad i(n)=0 \quad \text{if } n\notin f\big(\mathbb{N}^*\big) \text{ and } n>l$$
$$\text{and}\quad i\big(f(n)\big)=i(n)+1 \quad \text{for } n\geqslant 1.$$

Definition 2.2. A continued fraction expansion of type (p,l,k) is said to be perfect if there exists a sequence $(\lambda_n)_{n\geqslant 1}$ in $\mathbb{F}_p^*$ such that we have

$$a_n=\lambda_n A_{i(n),k}\quad \text{for } n\geqslant 1.$$

Note that, when the l-tuple $(i(1),\ldots,i(l))$ is fixed, there are $(p-1)^{l+2}$ expansions of type (p,l,k) and only a small proportion of them (less than $1/p$) are perfect. We shall see below that if the expansion is perfect, then the sequence $(\lambda_n)_{n\geqslant 1}$ in $\mathbb{F}_p^*$ is explicitly given and therefore the continued fraction itself is explicitly known. If the expansion is not perfect, its explicit description is yet out of reach in general. Finally, we observe that if $k=(p-1)/2$, in a perfect expansion, all the partial quotients are proportional to T: amazingly such an example also exists in [6] (see the introduction of [3]).

The structure of expansions of type (p,l,k) is based upon certain properties of the pair (P_k, Q_k) which are given in the following proposition, the proof of which is to be found in [3].

Proposition 2.3. *Let p be an odd prime and k an integer with $1\leqslant k<p/2$. We have in $\mathbb{F}_p(T)$ the following continued fraction expansion*:

$$P_k/Q_k=[v_1T,\ldots,v_iT,\ldots,v_{2k}T],$$

where the numbers $v_i\in\mathbb{F}_p^*$ are defined by $v_1=2k-1$ and recursively, for $1\leqslant i\leqslant 2k-1$, by

$$v_{i+1}v_i=(2k-2i-1)(2k-2i+1)\big(i(2k-i)\big)^{-1}.$$

Moreover, if we set $\theta_k=(-1)^k2^{-2k}\binom{2k}{k}\in\mathbb{F}_p^*$, we also have

$$v_{2k-i+1}=\big(-4k^2\theta_k^2\big)^{(-1)^i}v_i\quad \text{for } 1\leqslant i\leqslant 2k.$$

Our goal was to understand under which condition an expansion of type (p,l,k) is perfect. A general theorem on this question in a larger context is given in [5, Theorem B, p. 256], and a weaker version in [4, Theorem 1, p. 1111]. In our previous works, we assumed that $i(j)=0$ for $1\leqslant j\leqslant l$. This hypothesis was not natural and the proof of the theorems mentioned above is unchanged with the larger hypothesis made here, the condition is only slightly modified. Therefore we state below a short version of these theorems in our context.

Theorem 2.4. *Let p be an odd prime, k and l be given as above. Let $\alpha \in \mathbb{F}(p)$ be a continued fraction of type (p, l, k) defined by $(\lambda_1, \ldots, \lambda_l, \epsilon_1, \epsilon_2)$ in $(\mathbb{F}_p^*)^{l+2}$ and $(i(1), \ldots, i(l))$ in $\mathbb{N}^l$. Let $\theta_k \in \mathbb{F}_p^*$ be defined as in Proposition* 2.3. *Define*

$$\delta_n = \left[\theta_k^{i(n)}\lambda_n, \ldots, \theta_k^{i(1)}\lambda_1, 2k\theta_k/\epsilon_2\right] \in \mathbb{F}_p \quad \text{for } 1 \leqslant n \leqslant l.$$

If $\delta_n \neq 0$ for $1 \leqslant n \leqslant l$ and $\delta_l = 2k\epsilon_1/\epsilon_2$ then the expansion of α is perfect.

It is an open question whether the condition stated in Theorem 2.4 is necessary to have a perfect expansion. We expect it to be so, but a difficulty arises when the base field is not prime because in this context the sequence $(\lambda_n)_{n\geqslant 1}$ in $\mathbb{F}_q^*$ may exist without the condition $\delta_l = 2k\epsilon_1/\epsilon_2$. However in all cases when the sequence $(\lambda_n)_{n\geqslant 1}$ in $\mathbb{F}_p^*$ does exist it is explicitly described. We do not report here the complicated formulas giving this sequence from the first values $(\lambda_1, \ldots, \lambda_l)$ and the pair (ϵ_1, ϵ_2), but the reader can find them in [5].

3. The case $p = 1 \bmod 3$

In this section p is an odd prime number with $p = 1 \bmod 3$. In order to obtain the explicit continued fraction for the solution of $(Eq.1)$, we need to make a transformation. The inverse of the root of $(Eq.1)$ is denoted by α. We introduce $\beta \in \mathbb{F}(p)$ defined by $\beta(T) = v\alpha(vT)$ where $v^2 = -8/27$. Note that, as α is an odd function of T, we know that β belongs to $\mathbb{F}(p)$ even though v is in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$, according to the value of p. Moreover, since $-\alpha^4/12 - T\alpha^3 + \alpha^2 + 1 = 0$, we obtain $\beta^4 + 12v^2(T\beta^3 - \beta^2 - v^2) = 0$. Consequently β is the unique root in $\mathbb{F}(p)$ of the polynomial $G(X) = X^4 - 32/9(TX^3 - X^2 + 8/27)$.

Concerning the value $-8/27$, a comment must be made. In a first approach, the author realized that the solution needed to be transformed as above with $v^2 = a$ for some $a \in \mathbb{F}_p^*$ (see [4, p. 1112], where $a = 5$ for $p = 13$). When we prepared paper [1], A. Bluher, interested in the Galois group of Eq. $(Eq.1)$, could obtain some complementary results. At the fall of 2006, at a workshop in Banff, she presented some of this work in progress. The author realized, from Bluher's formulas, that we should have $a = -8/27$ in all characteristics.

Our goal is to describe explicitly the continued fraction expansion for β. Of course if $\beta = [b_1, \ldots, b_n \ldots]$ and $\alpha = [a_1, \ldots, a_n \ldots]$, we have $a_n(T) = v^{(-1)^n} b_n(T/v)$ for $n \geqslant 1$ and the continued fraction for α is explicitly known.

Throughout this section we set $j = (p-1)/6$. We consider the $4j$-tuple $(v_1, v_2, \ldots, v_{4j})$ in $(\mathbb{F}_p^*)^{4j}$ and $\theta_{2j} \in \mathbb{F}_p^*$, introduced in Proposition 2.3. We shall make use of the continuants, linked to the continued fraction algorithm as we recalled in the introduction. We will use the following notations:

$$K_{n,m} = \langle v_n T, v_{n+1}T, \ldots, v_m T\rangle \quad \text{for } 1 \leqslant n \leqslant m \leqslant 4j \quad \text{and} \quad K_{n,n-1} = 1.$$

We shall make use of the following general formula for continuants (see [8])

$$K_{n,m}K_{t,m-1} - K_{n,m-1}K_{t,m} = (-1)^{m-t}K_{n,t-2} \quad \text{for } n < t \leqslant m. \tag{1}$$

Moreover, for $\epsilon \in \mathbb{F}_p^*$, we define

$$K_{n,m}^{\epsilon} = \left\langle \epsilon v_n T, \epsilon^{-1} v_{n+1}T, \ldots, \epsilon^{(-1)^{m-n}} v_m T\right\rangle \quad \text{for } n \leqslant m.$$

By basic properties of the continuants, we have the following equalities:

$$K_{n,m}^{\epsilon} = K_{n,m}, \quad \text{if } m-n \text{ is odd} \quad \text{and} \quad K_{n,m}^{\epsilon} = \epsilon K_{n,m}, \quad \text{if } m-n \text{ is even.} \tag{2}$$

With these notations, we have the following theorem.

Theorem 3.1. *Let p be a prime number with $p = 1 \bmod 3$ and $p < 200$. Let $G \in \mathbb{F}_p[T][X]$ be defined by*

$$G(X) = X^4 - 32/9\big(TX^3 - X^2 + 8/27\big).$$

We set $\epsilon = 32/(9v_{j+1})$ and $\lambda = (-1)^{j+1}3\epsilon/(2\theta_{2j})$. Then there exists $\mu \in \mathbb{F}_p^*$, defined by

$$\mu = \lambda[v_{j+1}, v_{j+2}, \ldots, v_{4j-1}, 3v_{4j}/5],$$

such that G divides H in $\mathbb{F}_p[T][X]$, where H is defined by

$$H(X) = K_{j+2,4j}X^{p+1} - \epsilon K_{j+1,4j}X^p + \mu(K_{1,j}X + \epsilon K_{1,j-1}).$$

One must explain the bound given on the size of the prime p. Clearly, for a given prime p, with $p = 1 \bmod 3$, it is easy to compute the v_i and therefrom to compute the $K_{n,m}$ which appear as the coefficients of H. Once H and G are given, we only have to check by computer the divisibility property. We have done so for all primes up to 199 and we obviously expect it to be true for all primes congruent to 1 modulo 3.

With the notations of Theorem 3.1, we have the following:

Theorem 3.2. *Let p be an odd prime with $p = 1 \bmod 3$ and $p < 200$. Let β be the unique root in $\mathbb{F}(p)$ of G. Then the continued fraction expansion for β is of type $(p, 3j, 2j)$. This expansion is perfect and defined by*

$$b_i(T) = \epsilon^{(-1)^{i+1}} v_{j+i}T \quad \text{for } 1 \leqslant i \leqslant 3j,$$
$$\epsilon_1 = (-1)^j \epsilon^{(-1)^{j+1}}\mu \quad \text{and} \quad \epsilon_2 = (-1)^{j+1}4\theta_{2j}^2\mu/9.$$

Proof. Let $\gamma \in \mathbb{F}(p)$ be the infinite continued fraction, of type $(p, 3j, 2j)$, defined by $(b_1, \ldots, b_{3j})$ and (ϵ_1, ϵ_2) as they are given in this corollary. First we shall prove that $\gamma = \beta$. We know (see [3, pp. 332–333]) that γ is the unique root in $\mathbb{F}(p)^+$ of the algebraic equation,

$$y_{3j}X^{p+1} - x_{3j}X^p + UX + V = 0, \tag{3}$$

where we have

$$U = \epsilon_1 P_{2j}y_{3j-1} - \epsilon_2 Q_{2j}y_{3j} \quad \text{and} \quad V = \epsilon_2 Q_{2j}x_{3j} - \epsilon_1 P_{2j}x_{3j-1}. \tag{4}$$

From the values of the first partial quotients, we get

$$x_{3j} = \langle b_1, \ldots, b_{3j}\rangle = \big\langle \epsilon v_{j+1}T, \ldots, \epsilon^{(-1)^{3j+1}} v_{4j}T\big\rangle = K^{\epsilon}_{j+1,4j}. \tag{5}$$

In the same way we have

$$y_{3j} = K^{\epsilon^{-1}}_{j+2,4j}, \qquad x_{3j-1} = K^{\epsilon}_{j+1,4j-1} \quad \text{and} \quad y_{3j-1} = K^{\epsilon^{-1}}_{j+2,4j-1}. \tag{6}$$

From Proposition 2.3, we have $P_{2j}/Q_{2j} = K_{1,4j}/K_{2,4j}$. Since both polynomials P_{2j} and $K_{1,4j}$ have the same degree and the same constant term equal to 1, we have

$$P_{2j} = K_{1,4j} \quad \text{and} \quad Q_{2j} = K_{2,4j}.$$

Using the symmetry property of the sequence $(v_i)_{1\leqslant i\leqslant 4j}$, stated in Proposition 2.3, we have $v_i = (v_{4j}/v_1)^{(-1)^i} v_{4j-i+1}$. Hence, according to (2), we can write

$$K_{2,4j} = \big\langle (v_{4j}/v_1)v_{4j-1}T, \ldots, (v_{4j}/v_1)v_1T \big\rangle = (v_{4j}/v_1)K_{1,4j-1}.$$

Consequently we have

$$K_{1,4j} = P_{2j}, \qquad K_{1,4j-1} = (v_1/v_{4j})Q_{2j}. \tag{7}$$

Combining (4), (5), (6) and (7), we obtain

$$U = \epsilon_1 K_{1,4j} K^{\epsilon^{-1}}_{j+2,4j-1} - \epsilon_2 (v_{4j}/v_1) K_{1,4j-1} K^{\epsilon^{-1}}_{j+2,4j} \tag{8}$$

and

$$V = \epsilon_2 (v_{4j}/v_1) K_{1,4j-1} K^{\epsilon}_{j+1,4j} - \epsilon_1 K_{1,4j} K^{\epsilon}_{j+1,4j-1}. \tag{9}$$

Note that we have $v_1/v_{4j} = -16j^2\theta_{2j}^2 = -4\theta_{2j}^2/9$, since $j = -1/6$ in $\mathbb{F}_p^*$. Hence, introducing the values for ϵ_1 and ϵ_2, (8) becomes

$$U = (-1)^j \mu \big(\epsilon^{(-1)^{j+1}} K_{1,4j} K^{\epsilon^{-1}}_{j+2,4j-1} - K_{1,4j-1} K^{\epsilon^{-1}}_{j+2,4j} \big) \tag{10}$$

and, in the same way, (9) becomes

$$V = (-1)^j \mu \big(K_{1,4j-1} K^{\epsilon}_{j+1,4j} - \epsilon^{(-1)^{j+1}} K_{1,4j} K^{\epsilon}_{j+1,4j-1} \big). \tag{11}$$

From (1), we obtain

$$K_{1,4j} K_{j+2,4j-1} - K_{1,4j-1} K_{j+2,4j} = (-1)^j K_{1,j}, \tag{12}$$

$$K_{1,4j} K_{j+1,4j-1} - K_{1,4j-1} K_{j+1,4j} = (-1)^{j-1} K_{1,j-1}. \tag{13}$$

Therefrom, combining (10), (11), (12) and (13), and considering alternatively both cases j odd or even, we can write Eq. (3) as

$$K_{j+2,4j} X^{p+1} - \epsilon K_{j+1,4j} X^p + \mu (K_{1,j} X + \epsilon K_{1,j-1}) = 0. \tag{14}$$

Thus we have $H(\gamma) = 0$. Since $G(\beta) = 0$, we also have, by Theorem 3.1, $H(\beta) = 0$. But Eq. (14) has only one root in $\mathbb{F}(p)^+$ and therefore $\gamma = \beta$. Now we prove that the continued fraction for β is perfect. We have the following equivalence, which is easily verified by induction:

$$[t_n, \ldots, t_2, t_1 + u] = v \quad \Longleftrightarrow \quad [t_1, \ldots, t_{n-1}, t_n - v] = -u.$$

Consequently, using the definition of μ, we see that the equality

$$[v_{j+1}, \ldots, v_{4j-21}, v_{4j} - 2v_{4j}/5] = \mu\lambda^{-1}$$

is equivalent to

$$\left[v_{4j}, \ldots, v_{j+1} - \mu\lambda^{-1}\right] = 2v_{4j}/5.$$

Multiplying both sides by $\epsilon^{(-1)^{j+1}}$, this last equality becomes

$$\left[\lambda_{3j}, \ldots, \lambda_1, -\lambda/(\mu\epsilon)\right] = \epsilon^{(-1)^{j+1}} 2v_{4j}/5.$$

So the conclusion follows from Theorem 2.4, by checking that the pair (ϵ_1, ϵ_2) satisfies the equalities

$$4j\theta_{2j}/\epsilon_2 = -\lambda/(\mu\epsilon) \quad \text{and} \quad 4j\epsilon_1/\epsilon_2 = \epsilon^{(-1)^{j+1}} 2v_{4j}/5. \qquad \square$$

4. Indications in the case $p = 2 \bmod 3$

In this second case, the pattern for the continued fraction of the solution of $(Eq.1)$ appears to be very different from the one we have described in the first case. Here again there seems to be a general pattern for all primes p with $p = 2 \bmod 3$. The reader may use the few lines of a program, which is given in the last section, to observe the beginning of this expansion on a computer screen. This pattern is not understood but we can indicate some observations which are somehow parallel to what has been presented above. We do not know whether a similar method can be developed from these indications to obtain an explicit description of this continued fraction. We have the following conjecture.

Conjecture. *Let p be a prime number with $p = 2 \bmod 3$. Let $\beta \in \mathbb{F}(p)$ be defined by $\beta(T) = v\alpha(vT)$ where $v = \sqrt{-8/27}$ and $1/\alpha$ is the unique root of $(Eq.1)$. Let $\beta = [b_1, b_2, \ldots, b_n, \ldots]$ be its continued fraction expansion. Then there exists a pair $(\epsilon_1, \epsilon_2) \in (\mathbb{F}_p^*)^2$ such that*

$$\beta^{p^2} = \epsilon_1 P_k^{p-1} \beta_{l+1} + \epsilon_2 Q_k^p$$

where

$$l = \frac{(p+1)^2}{3} \quad \text{and} \quad k = \frac{p+1}{3}.$$

This conjecture has been checked by computer for the first primes congruent to 2 modulo 3. We report below, for $p \leqslant 23$, the values of the pair (ϵ_1, ϵ_2).

p	5	11	17	23
ϵ_1	4	1	16	1
ϵ_2	3	9	11	22

5. A remark on programming

Before concluding, we want to discuss a particular way to obtain by computer the beginning of the continued fraction expansion for an algebraic power series. The natural way is to start from a rational approximation, often obtained by truncating the power series expansion, and therefrom transform this rational into a finite continued fraction as this is done for an algebraic real number. However, here in the formal case, it is possible to proceed differently. The origin of this method is based on a result introduced by M. Mkaouar, it can be found in [7] and also in other papers from him. We recall here this result:

Proposition *(Mkaouar). Let P be a polynomial in $\mathbb{F}_q[T][X]$ of degree $n \geqslant 1$ in X. We put $P(X) = \sum_{0\leqslant i\leqslant n} a_i X^i$ where $a_i \in \mathbb{F}_q[T]$. Assume that we have*

$$|a_i| < |a_{n-1}| \quad \text{for } 0 \leqslant i \leqslant n \text{ and } i \neq n-1. \tag{$*$}$$

Then P has a unique root in $\mathbb{F}(q)^+ = \{\alpha \in \mathbb{F}(q) \mid |\alpha| \geqslant |T|\}$. Moreover, if u is this root, we have $[u] = -[a_{n-1}/a_n]$. If $u \neq [u]$ and $u = [u] + 1/v$ then v is the unique root in $\mathbb{F}(q)^+$ of a polynomial $Q(X) = \sum_{0\leqslant i\leqslant n} b_i X^i$, and we have the same property $(*)$ on the coefficients b_i.

In this proposition, it is clear that the coefficients b_i can be deduced from $[u]$ and the a_i's. We have $b_n = P([u])$, so if u is not integer we obtain $[v] = -[b_{n-1}/b_n]$. Consequently the process can be carried on, for a finite number of steps if the solution u is rational or infinitely otherwise. Thus the partial quotients of the solution can all be obtained by induction. This method can be applied to obtain the continued fraction expansion of the solution of our quartic equation, starting from the polynomial $P(X) = -X^4/12 - TX^3 + X^2 + 1$. We have written here below the few lines of a program (using Maple) to obtain the first two hundred partial quotients of this expansion.

```
p:=5:n:=200:u:=-1/12 mod p:
a:=array(1..n):b:=array(1..n):c:=array(1..n):d:=array(1..n):
e:=array(1..n):qp:=array(1..n):a[1]:=u:
b[1]:=-T:c[1]:=1:d[1]:=0:e[1]:=1:qp[1]:=-quo(b[1],a[1],T) mod p:
for i from 2 to n do
a[i]:=simplify(a[i-1]*qp[i-1]^4+b[i-1]*qp[i-1]^3+
c[i-1]*qp[i-1]^2+d[i-1]*qp[i-1]+e[i-1]) mod p:
b[i]:=simplify(4*a[i-1]*qp[i-1]^3+3*b[i-1]*qp[i-1]^2+
2*c[i-1]*qp[i-1]+d[i-1]) mod p:
c[i]:=simplify(6*a[i-1]*qp[i-1]^2+3*b[i-1]*qp[i-1]+c[i-1]) mod p:
d[i]:=simplify(4*a[i-1]*qp[i-1]+b[i-1]) mod p:e[i]:=a[i-1]:
qp[i]:=-quo(b[i],a[i],T) mod p:od:print(qp);
```

This method is easy to use in two cases: if the degree of the initial polynomial is small and also if the initial polynomial has the particular form corresponding to a hyperquadratic solution. Indeed in this second case, in the proposition stated above, the polynomial Q has the same form as P, therefore the recurrence relations between the coefficients of P and those of Q are made simple. In both cases, it seems that the method is of limited practical use because the degrees of the polynomials in T, giving the partial quotients by division, are growing fast.

Acknowledgment

We want to thank warmly the referee for his or her careful reading of the manuscript and for his or her suggestions to improve its presentation.

References

[1] A. Bluher, A. Lasjaunias, Hyperquadratic power series of degree four, Acta Arith. 124 (2006) 257–268.
[2] W. Buck, D. Robbins, The continued fraction of an algebraic power series satisfying a quartic equation, J. Number Theory 50 (1995) 335–344.
[3] A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. 14 (2008) 329–350.
[4] A. Lasjaunias, On Robbins' example of a continued fraction expansion for a quartic power series over $\mathbb{F}_{13}$, J. Number Theory 128 (2008) 1109–1115.
[5] A. Lasjaunias, Algebraic continued fractions in $\mathbb{F}_q((T^{-1}))$ and recurrent sequences in $\mathbb{F}_q$, Acta Arith. 133 (2008) 251–265.
[6] W. Mills, D. Robbins, Continued fractions for certain algebraic power series, J. Number Theory 23 (1986) 388–404.
[7] M. Mkaouar, Sur les fractions continues des séries formelles quadratiques sur $\mathbb{F}_q(X)$, Acta Arith. 97 (3) (2006) 241–251.
[8] O. Perron, Die Lehre von den Kettenbrüchen, 2nd ed., Chelsea Publishing Company, New York, 1950.
[9] W. Schmidt, On continued fractions and diophantine approximation in power series fields, Acta Arith. 95 (2) (2000) 139–166.